THE FEDERAL COMMUNICATIONS COMMISSION'S PROPOSED BROADBAND PRIVACY RULES WOULD VIOLATE THE FIRST AMENDMENT

LAURENCE H. TRIBE
420 Hauser Hall
1575 Massachusetts Ave.
Cambridge, MA 02138
Tel: (617) 495-1767
tribe@law.harvard.edu

JONATHAN S. MASSEY
MASSEY & GAIL, LLP
1325 G St., NW, Ste 500
Washington, D.C. 20005
Tel: (202) 652-4511
jmassey@masseygail.com

May 27, 2016

TABLE OF CONTENTS

Executive Summary **1**

Discussion **9**

A. The Uses Of Customer Data That Would Be Regulated By The Proposed Rules Constitute Protected "Speech" Under The First Amendment. **9**

1. The *U.S. West* Decision Recognizes Fundamental First Amendment Limits On The FCC's Authority To Regulate Customer Information. 9

2. The Supreme Court's Decision in *Sorrell* Reaffirms That The FCC's Proposal Triggers First Amendment Scrutiny. 13

B. The Proposed Rules Fail First Amendment Scrutiny **14**

1. The Burden on Speech Is Substantial: The Proposed Rules Restrict A Great Deal Of Speech. 16

2. The First *Central Hudson* Prong: Whether the FCC Has Asserted A "Substantial" Governmental Interest. 18

3. The Second *Central Hudson* Prong: Whether the Regulation is Tailored To and "Directly Advances" the Asserted Interest. 22

(a) The Under-Inclusiveness Of The Proposed Rules Shows That They Fail The Second Prong. 22

(b) The Commission's Reasons For The Limited Scope Of Its Proposal Do Not Justify the Restrictions On Speech. 24

(c) The Proposed Rules Suffer From Additional Mis-Matches Between The FCC's Asserted Interests and the Restrictions on Speech. 27

(i) The Proposed Rules Are Not Tailored To Any Interest In Restricting The Sharing of Private Information With Third Parties. 27

(ii) The Proposal Draws Impermissible Content-Based Distinctions Based On What a Marketer Says. 30

(iii) The Proposal Provides No Adequate Basis For Distinguishing Between Corporate Affiliates and Third-Party Agents/Vendors. 32

4. The Third *Central Hudson* Prong: A Notice-and-Choice Regulatory Regime Consistent with the FTC's Approach Provides An Obvious Alternative That Is Less Speech-Suppressing. 33

C. The Canon Of Constitutional Avoidance Requires That the FCC Narrowly Construe Its Authority. **38**

D. The 2009 *NCTA* Decision Does Not Support the NPRM. **39**

Conclusion **40**

Executive Summary

The Notice of Proposed Rulemaking ("NPRM") issued by the Federal Communications Commission ("FCC") proposes a tripartite scheme that would create three categories for customer information:[1]

(i) Where consent to the use in question is inherent in a customer's decision to purchase the Internet Service Provider's ("ISP's") services in the first place, ISPs would be permitted to use certain customer information with no additional customer consent, beyond the creation of the customer-ISP relationship. But, as set forth in the FCC's lead proposal, this is a very limited category, covering customer data necessary to provide broadband services, for marketing the type of broadband service purchased by a customer, and for certain other restricted purposes, such as contacting public safety.

(ii) The proposal would impose an opt-out rule for using customer information to market other "communications-related services" and for sharing customer information with ISP affiliates that provide communications-related services. The FCC proposes a narrow interpretation of the term "communications-related services." Hence, this category of activity is a very limited one.

(iii) All other uses and sharing of consumer information would be prohibited unless ISPs obtain "opt-in" consent from customers. For example:

- The FCC's proposal would impose an opt-in consent requirement before ISPs could use customer information to develop and communicate online ads on social media to enable consumers to receive targeted, useful information in a timely manner.
- The proposal would require opt-in consent when the ISP seeks to use customer information to market non-communications-related services (such as home security, music, or energy management services) to that customer.
- Similarly, an opt-in consent requirement would apply to an ISP's use of customer information in conjunction with third parties for any purpose, even if

[1] This White Paper is being filed at the request of NCTA, CTIA, and USTelecom. The views reflected herein are Professor Tribe's own conclusions as a scholar of constitutional law.

> the information is used to market communications-related services, and even if the ISP uses the data to do the marketing itself on behalf of a third party (i.e., the third party never has access to the data).

Importantly, none of the opt-in consent requirements turns on the sensitivity of the customer information at issue; rather, unlike the Federal Trade Commission ("FTC") privacy framework and most other privacy laws, as well as the Obama Administration's Consumer Privacy Bill of Rights, the FCC's proposal makes no distinction between sensitive and non-sensitive data.

In practical terms, the NPRM is a highly burdensome approach to privacy that imposes an affirmative opt-in consent requirement for marketing anything beyond a very narrow category of communications-related services marketed by the ISP and its corporate affiliates. Notably, for example, *the proposal could prohibit a broadband provider from using information about its own customer (including non-sensitive information) to offer a discounted bundle of its own services to that customer or to offer accessories that are compatible with her devices without her prior opt-in consent*. In most circumstances, even efforts to solicit opt-ins from consumers will be infeasible, because the costs of doing so for a small percentage of likely affirmative responses will simply be too great. If the Commission restricts the use of inducements to consumers in exchange for their consent to use their information, the practical import of the NPRM will be even harsher.

Accordingly, the NPRM imposes a substantial burden on speech, because it will effectively prevent ISPs from using customer information to develop and express important communications with consumers. This will preclude the kind of targeted speech that consumers find most valuable and useful, as well as other lawful communications. The proposal thus ignores the important social role of the First Amendment in advancing the *rights of the audience* to receive useful information. The value of speech accrues not just to the speaker but also, as in the commercial marketplace itself, to the *consumer* of speech. The proposed rules violate this principle.

These burdensome and harmful effects on speech are not required by the statute. Section 222 does not by its terms mandate the FCC to adopt an opt-in consent requirement. Instead, Section 222(c)(1) authorizes a carrier to use customer information upon "the approval of the customer," which the Commission itself and the courts have previously determined can be satisfied via either an opt-out procedure or an opt-in procedure, or even via implied consent. Thus, the Obama Administration's 2012 "Consumer Privacy Bill of Rights" took the view that first-party marketing is within the expectations of customers and that consent may be implied. Section 222(f) requires opt-in consent for location information in only two specific situations (certain call location information and automatic crash notifications) – confirming that the Commission has authority to adopt opt-out in other circumstances.

The proposal runs afoul of fundamental First Amendment limits on the FCC's authority to regulate customer information, as recognized in *Sorrell v. IMS Health, Inc*., 564 U.S. 552 (2011), and *U.S. West Communications, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999). *Sorrell* struck down a Vermont law restricting the disclosure of pharmacy records that revealed the prescribing practices of individual doctors, which data miners were using to make drug marketing more targeted and effective. *Sorrell* held that the process of gathering and analyzing data in preparation for speech is protected by the First Amendment. In fact, the Court left open the question whether restrictions on such expression should receive stricter First Amendment scrutiny than the intermediate standard of *Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y.*, 447 U.S. 557, 564 (1980), which is applicable to commercial speech. *See Sorrell*, 564 U.S. at 571 (leaving open whether *Central Hudson* or a "stricter form of judicial scrutiny" should be applied).

In *U.S. West*, the Tenth Circuit invalidated the Commission's Customer Proprietary Network Information ("CPNI") rules for voice communications. The Court of Appeals held that

the analysis and transfer of CPNI among corporate affiliates, in preparation for consumer marketing, was "speech" and that the FCC's opt-in consent requirement failed to satisfy intermediate First Amendment scrutiny. If anything, the proposed rules here are even *more constitutionally problematic* than the CPNI regulations invalidated by the Tenth Circuit. The proposed rules represent a *much larger* burden on speech and are far *less* tailored to any substantial governmental interest. And technological and market developments make it even more implausible that the FCC could meet its burden under any form of First Amendment scrutiny (including under all three prongs of the intermediate standard of *Central Hudson*) of demonstrating that its proposed restrictions on speech are tailored to a substantial governmental interest.

Further, the FCC's proposal fails First Amendment scrutiny because it singles out broadband ISPs for extremely burdensome regulation while ignoring the fact that much of the same information is available to and routinely used by social media companies, web browsers, search engines, data brokers, and other digital platforms. In fact, Google, Amazon, Facebook, and other so-called "edge providers" accumulate, use, and share far more customer data than ISPs and are the biggest players by far in the online advertising market. Importantly, the point is not that the FCC can or should regulate edge providers or that heightened standards are warranted more generally. Rather, the point is that 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. By essentially blocking ISP entry into the online advertising market by singling out new entrants in the online advertising market for heightened standards that do not apply to the established market leaders, the FCC's proposal is anti-competitive, anti-consumer, and anti-First Amendment.

The proposed rules suffer from further profound mis-matches that render them invalid under *Central Hudson*'s tailoring requirement (as well as under undiluted First Amendment scrutiny):

(i) The proposal is not keyed to the sensitivity of consumer information, unlike the FTC's existing regulatory scheme. The FCC's proposal uses the same blunderbuss, speech-suppressing approach for all types of information.

(ii) The FCC's asserted privacy concerns arise from the *sharing* of information between an ISP and unaffiliated third parties, but its proposal also seeks to regulate how an ISP or its affiliates can *use* information – for example, by marketing a non-communications-related service to customers or targeting online advertising to the consumers for whom it is most relevant.

(iii) The proposal would require opt-in by the customer before information about that customer may be shared with an affiliate for marketing non-communications-related services. This imposes a significant burden on broadband ISPs by making it necessary for them to maintain separate databases and extensively track which information can be shared with which affiliates, but it provides little or no additional privacy over a regime that allows broadband ISPs to keep consumer information in a single database and simply confirm appropriate customer consent before using.[2]

In addition, the proposal draws content-based distinctions that trigger still further constitutional concerns. The proposal allows ISPs to use customer data (and to share it with their affiliates) to market *communications-related* services (subject only to an *opt-out* consent

[2] *See FEC v. Massachusetts Citizens for Life*, 479 U.S. 238, 254-55 (1986) (plurality opinion) (treating the burden of keeping track of a separate segregated fund for making expenditures in connection with federal elections as too heavy to meet First Amendment standards, citing "[d]etailed recordkeeping" obligations, "administrative costs," and "the statute's practical effect" of "discourag[ing] protected speech"); *id.* at 266 (O'Connor, J., concurring in part and concurring in the judgment) (agreeing that organizational requirements violated the First Amendment).

requirement), but *not* to market *non-communications-related* services without prior *opt-in* consent. Thus, the restriction on speech turns in significant part on *what the speaker says* – whether the marketing relates to a "communications-related service" (such as voice) or a "non-communications-related service" (such as home security, music, or energy management services).

The proposal also distinguishes between agents/vendors and corporate affiliates, without providing a sufficient basis for that distinction. The proposal would impose an *opt-out* consent requirement for a broadband ISP's sharing of customer data with its *corporate affiliates* for marketing communications-related services, but an *opt-in* requirement if broadband ISPs instead seek to use *third-party agents/vendors* to do exactly the same thing, even if those agents/vendors are bound by exactly the same confidentiality restrictions and protections as the affiliates and despite the fact that, under Section 217 of the Communications Act, they are treated as employees of the ISP itself for enforcement purposes.

The FTC regulatory regime provides an obvious alternative that is less speech-suppressing and demonstrates that the FCC's proposal fails the third prong of *Central Hudson* (let alone full First Amendment scrutiny). Extensive experience with the FTC's privacy protections – which have applied to ISPs for many years – undermines the FCC's assertion that its new rules impose no more restrictions on speech than necessary. In fact, the FTC's well-established and highly successful privacy framework shows that (1) an opt-in consent requirement should be applied very narrowly only to "sensitive data" and (2) there is nothing unique about ISPs' data collection or use practices that would justify the FCC's onerous privacy rules. The FTC has actually brought far more privacy enforcement actions against edge providers than against ISPs. Further, the FTC's 2012 Privacy Report concluded, "[T]he Commission agrees that any privacy framework should be technology neutral. ISPs are just one type of large platform provider that may have access to all

or nearly all of a consumer's online activity."[3] This conclusion was confirmed after a December 2012 FTC workshop, by the Associate Director of the Privacy Division at the FTC, who reinforced the "need for tech neutrality" as an area of consensus among workshop participants because "there are lots of business models . . . that can permit an entity to get a pretty comprehensive window into consumers' browsing behavior," and "we can't be picking winners and losers in this space."[4] And, importantly, the FTC has maintained this core conclusion and this technology-neutral approach to privacy regulation to the present, making no distinction with respect to ISPs in the numerous privacy-related studies, round tables, analyses, and reports the FTC has conducted and produced in this period, including on the Internet of Things, Data Brokers, and Cross-Device Tracking. The FCC's proposed rules violate this important principle of technological neutrality – one that is closely related to the settled requirement of speaker-neutrality.

The D.C. Circuit's decision in *NCTA v. FCC*, 555 F.3d 996 (D.C. Cir. 2009), does not provide support for the FCC's broad proposal. *NCTA* involved "a limited opt-in consent requirement" for the sale of customer information to third-party marketers, which the FCC adopted "in response to the increasing activity of data brokers." *Id.* at 1003. In contrast, the proposed rules here also govern an ISP's own *use* of customer information, as well as its sharing with affiliates and controlled agents/vendors, even to market the ISP's own products and services to its customers. The proposed rules suffer from tailoring flaws and content-based distinctions that were not present in *NCTA*. The record of the two proceedings is also substantially different. And the

[3] "Protecting Consumer Privacy in an Era of Rapid Change," *available at* https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers (March 2012), at 56.

[4] *See* Transcript of Federal Trade Commission Workshop, *The Big Picture: Comprehensive Online Data Collection* (Dec. 6, 2012), https://www.ftc.gov/sites/default/files/documents/public_events/The%20Big%20Picture%3A%20Comprehensive%20Online%20Data%20Collection/bigpicture_transcript_21206ftc.pdf.

force of the *NCTA* decision is substantially weakened not only by the petitioners' concessions in that case, which the D.C. Circuit repeatedly stressed, but also by the Supreme Court's subsequent decision in *Sorrell*.

For all these reasons, the FCC's proposal would violate the First Amendment. The deference ordinarily afforded under *Chevron* is thus inapplicable and instead the Communications Act should be construed as not authorizing the proposed rules. The canon of constitutional avoidance is particularly salient because the NPRM rests on very thin statutory ice. The proposed rules should not be adopted.

Discussion

A. The Uses Of Customer Data That Would Be Regulated By The Proposed Rules Constitute Protected "Speech" Under The First Amendment.

1. The *U.S. West* Decision Recognizes Fundamental First Amendment Limits On The FCC's Authority To Regulate Customer Information.

In *U.S. West Communications, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999), the Tenth Circuit held that the analysis and transfer of CPNI among corporate affiliates, in preparation for consumer marketing, is "speech" and that the FCC's opt-in consent requirement failed to satisfy intermediate First Amendment scrutiny. *Id.* at 1232. The CPNI rules invalidated in *U.S. West* sought to implement Section 222 of the Communications Act by requiring customer opt-in before a carrier could use, disclose, or permit access to CPNI for the purpose of marketing categories of service to which the customer did not already subscribe. The rules treated affiliated entities of a carrier as separate for the purposes of use or disclosure. Absent customer opt-in, for example, a carrier could not use CPNI obtained through the provision of local landline service to market cellular services, nor could it transfer or disclose CPNI between corporate affiliates for that purpose. *Id.* at 1230. In addition, the regulations prevented telecommunications carriers from using (without customer opt-in consent) CPNI to market customer premises equipment or information services (such as call answering, voice mail, or Internet access services). *Id.*

The Court of Appeals warned that "in this age of exploding information," the "rights bestowed by the United States Constitution must be guarded as vigilantly as in the days of handbills on public sidewalks." *Id.* at 1228. "In the name of deference to agency action, important civil liberties, such as the First Amendment's protection of speech, could easily be overlooked." *Id.* The Tenth Circuit held that the deference ordinarily afforded to agency interpretations under *Chevron U.S.A., Inc. v. Natural Resources Defense Council, Inc.*, 467 U.S. 837 (1984), is inapplicable where an interpretation raises serious constitutional questions: "deference to an

agency interpretation is inappropriate not only when it is conclusively unconstitutional, but also when it raises serious constitutional questions." *U.S. West*, 182 F.3d at 1231. "When faced with a statutory interpretation that 'would raise serious constitutional problems, the [c]ourt[s] will construe the statute to avoid such problems unless such construction is plainly contrary to the intent of Congress.'" *Id.* (quoting *Edward J. DeBartolo Corp. v. Fla. Gulf Coast Bldg. & Constr. Trades Council*, 485 U.S. 568, 575 (1988)).[5]

The Tenth Circuit concluded that the FCC's CPNI rules triggered serious constitutional questions. The court observed 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.'" *Id.* at 1232. "[T]he targeted speech in this case fits soundly within the definition of commercial speech." *Id.* at 1233. The court also concluded that the transfer and analysis of CPNI within U.S. West's corporate family constituted protected commercial speech. *Id.* at 1233 n.4.

The Tenth Circuit's holding thus vindicated essential constitutional guarantees. After the Solicitor General's office reviewed the case, the Government decided not to seek certiorari. *U.S. West* applied well-established First Amendment jurisprudence, and the Commission continues to rely on it.[6]

[5] In *NFIB v. Sebelius*, 132 S. Ct. 2566 (2012), for example, the Court construed the Affordable Care Act individual mandate as providing an option to purchase insurance or pay a "tax" penalty rather than as a regulation mandating such purchase, adopting an interpretation of the statute that was concededly less plausible than that insisted upon by the dissent, solely to save the statute from constitutional infirmity.

[6] *See In The Matter Of Ensuring Customer Premises Equipment Backup Power For Continuity Of Communications Technology Transitions*, 29 FCC Rcd. 14,968, 15020 (2014); *In The Matter Of Structure and Practices Of The Video Relay Service Program*, 28 FCC Rcd. 8618 (2013); *In The Matter Of Petition Of USTelecom For Forbearance Under 47 U.S.C. 160(c) From Enforcement Of Certain Legacy Telecommunications Regulations*, 28 FCC Rcd. 7627 (2013); *In The Matter Of Applications Filed For The Acquisition Of Certain Assets Of Cimco Communications, Inc. By Comcast Phone LLC*, 25 FCC Rcd. 3401 (2010); *In The Matter Of Telecommunications Relay Services And Speech-To-Speech Services For Individuals With Hearing And Speech Disabilities E911 Requirements For IP-Enabled Service Providers*, 23 FCC Rcd. 11,591 (2008); *In re Implementation of*

Furthermore, *U.S. West*'s holding that an opt-in consent requirement burdens speech is fully consistent with a long line of Supreme Court precedent. For example, in *Martin v. Struthers*, 319 U.S. 141 (1943), the Supreme Court invalidated a city ordinance that effectively operated as an "opt-in" consent requirement by preventing those distributing religious handbills from reaching audiences that did not affirmatively seek them out. The ordinance banned such speakers from ringing the doorbell, knocking on the door, or otherwise summoning the residents of a house to the door. The Court held that the ordinance burdened speech because it, "in effect, makes a person a criminal trespasser if he enters the property of another for an innocent purpose without an explicit command from the owners to stay away." *Id.* at 148.[7]

Other opt-in laws invalidated by the Supreme Court based upon First Amendment scrutiny include *Lamont v. Postmaster General*, 381 U.S. 301, 307 (1965), which discouraged speech by requiring Americans to make an affirmative request to the post office in order to receive literature from designated foreign sources, and *Denver Area Educational Telecom Consortium, Inc. v. FCC*, 518 U.S. 727, 753-60 (1996), in which the Court struck down a "segregate and block" system for

Telecommunications Act of 1996, 22 FCC Rcd. 6927 (2007); *In The Matters Of Section 272(f)(1) Sunset Of The BOC Separate Affiliate And Related Requirements*, 22 FCC Rcd. 16,440 (2007); *In The Matters Of Appropriate Framework For Broadband Access To The Internet Over Wireline Facilities Universal Service Obligations Of Broadband Providers Computer III Further Remand Proceedings: Bell Operating Company Provision Of Enhanced Services; 1998 Biennial Regulatory Review*, 20 FCC Rcd. 14,853 (2005); *In re Implementation of the Subscriber Carrier Selection Changes Provisions of the Telecommunications Act of 1996*, 18 FCC Rcd. 5099 (2003); *In re BellSouth Petition for Waiver of Computer III*, 17 FCC Rcd. 13,881 (2002); *In re Implementation of Telecommunications Act of 1996*, 17 FCC Rcd. 14,860 (2002); *In re WorldCom, Inc*., 17 FCC Rcd. 27,039 (2002); *In re Appropriate Framework for Broadband Access to Internet over Wireline Facilities,* 17 FCC Rcd. 3019 (2002); *In re Petition of Nevada Bell*, 16 FCC Rcd. 19,255 (2001); *In re Forbearance from Applying Provisions of Communications Act to Wireless Telecommunications Carriers*, 15 FCC Rcd. 17,414, 17414 (2000); *In re Section 257 Report to Congress Identifying and Eliminating Market Entry Barriers for Entrepreneurs and Other Small Businesses*, 15 FCC Rcd. 15,376 (2000); *In re Implementation of Telecommunications Act of 1996*, 14 FCC Rcd. 15,550, 15656 (1999); *MCI Telecommunications Corp. v. Pacific Bell*, 14 FCC Rcd. 15,362 (1999).

[7] *Breard v. City of Alexandria*, 341 U.S. 622 (1951), upheld an ordinance requiring a prior request by a homeowner before a commercial solicitor could approach the house, and distinguished *Martin* largely on the ground that it did not involve commercial speech. *Id.* at 642-43. After *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc.*, 425 U.S. 748 (1976), *Breard* is likely no longer good law.

receiving certain indecent cable shows on the ground that its opt-in system would suppress speech.[8] The *Denver* Court opined that the requirement would "mean that a subscriber cannot decide to watch a single program without considerable advance planning," and would "prevent programmers from broadcasting to viewers who select programs day by day (or, through 'surfing,' minute by minute); to viewers who would like occasionally to watch a few, but not many, of the programs on the 'patently offensive' channel; and to viewers who simply tend to judge a program's value through channel reputation, i.e., by the company it keeps." *Id.* at 754. The Court explained that it "has not been willing to stretch the limits of the plausible, to create hypothetical nonobvious explanations in order to justify laws that impose significant restrictions upon speech." *Id.* at 760.

More broadly, the Supreme Court has recognized that the "distinction between laws burdening and laws banning speech is but a matter of degree." *United States v. Playboy Entm't Grp., Inc*., 529 U.S. 803, 812 (2000). Hence, an opt-in consent requirement that "merely" *burdens* (rather than explicitly prohibits) speech remains subject to heightened constitutional scrutiny. "Lawmakers may no more silence unwanted speech by burdening its utterance than by censoring its content." *Sorrell*, 564 U.S. at 565; *see also United States v. Nat'l Treasury Emps. Union*, 513 U.S. 454, 469 (1995) (striking down a limit on honoraria because it decreased the "incentive" of government employees to speak); *Simon & Schuster, Inc. v. Members of the N.Y. State Crime Victims Bd*., 502 U.S. 105, 109-10, 123 (1991) (striking down law that eliminated financial gain from speech on specified subjects); *Riley v. Nat'l Fed'n of the Blind*, 487 U.S. 781, 789 n.5 (1988) (financial regulation of professional fundraisers could not be defended as a "merely economic" regulation having "only an indirect effect on protected speech").

[8] The Court upheld other aspects of the statutory scheme.

2. The Supreme Court's Decision in *Sorrell* Reaffirms That The FCC's Proposal Triggers First Amendment Scrutiny.

Sorrell likewise makes clear that the FCC's proposed rules trigger First Amendment scrutiny. It explains that the First Amendment not only safeguards the right to "speak" in the abstract but also protects the right to engage in the uninhibited gathering and thorough processing of information – activities that provide the foundation of expression. *Sorrell* struck down a state statute limiting the disclosure of pharmacy records that revealed the prescribing practices of individual doctors. Data miners used those records to make drug marketing more targeted and effective. The Court opined that the challenged restrictions triggered First Amendment scrutiny, because "[a]n individual's right to speak is implicated when information he or she possesses is subjected to 'restraints on the way in which the information might be used' or disseminated." 564 U.S. at 568 (citation omitted). *Sorrell* held that "the creation and dissemination of information are speech within the meaning of the First Amendment. Facts, after all, are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs. There is thus a strong argument that prescriber-identifying information is speech for First Amendment purposes." *Id*. at 570.

Importantly, *Sorrell* left open the possibility that restrictions like those proposed by the FCC here should receive stricter First Amendment protection than the *Central Hudson* test. *See* 564 U.S. at 571 (leaving open whether *Central Hudson* or a "stricter form of judicial scrutiny" should be applied). After all, analysis of customer information that serves as a foundation for expressive activities is a valuable form of fully protected First Amendment speech – not merely commercial speech. As the Court noted in *Sorrell*, "[w]hile the burdened speech results from an economic motive, so too does a great deal of vital expression," such as commercial newspaper publishing. *Id.* at 567. Far from demeaning an economic motive, the Court has recognized that

"compensation provides a significant incentive toward more expression." *United States v. Treasury Employees*, 513 U.S. 454, 469 (1995) (citing *Simon & Schuster, Inc. v. Members of N.Y. State Crime Victims Bd.*, 502 U.S. 105 (1991)); *see also Riley v. Nat'l Fed'n of the Blind*, 487 U.S. 781, 796 (1988) (solicitation does not lose fully protected nature merely because it is "intertwined" with speech possessing commercial characteristics); *Bose Corp. v. Consumers Union of United States, Inc.*, 466 U.S. 485, 513 (1984) (affording full First Amendment protection to opinion concerning commercial product); *Bolger v. Youngs Drug Prod. Corp.*, 463 U.S. 60, 66 (1983) ("The mere fact that these pamphlets are conceded to be advertisements clearly does not compel the conclusion that they are commercial speech. Similarly, the reference to a specific product does not by itself render the pamphlets commercial speech."); *New York Times v. Sullivan*, 376 U.S. 254, 265-66 (1964) (paid newspaper ad designed to raise money entitled to full First Amendment protection).

In the wake of *Sorrell*, some courts have held that the decision requires a higher level of scrutiny than the ordinary *Central Hudson* analysis for this kind of restrictions. *See, e.g., Retail Digital Network, LLC v. Appelsmith*, 810 F.3d 638, 648 (9th Cir. 2016) ("*Sorrell* modified the *Central Hudson* test for laws burdening commercial speech. Under *Sorrell*, courts must first determine whether a challenged law burdening non-misleading commercial speech about legal goods or services is content- or speaker-based. If so, heightened judicial scrutiny is required.").

The FCC's proposed rules here would not survive any form of First Amendment scrutiny – whether the intermediate standard of *Central Hudson* or the stricter scrutiny applied in *Sorrell.*

B. The Proposed Rules Fail First Amendment Scrutiny.

Under intermediate scrutiny, the Government may restrict speech – even if it constitutes purely commercial speech – only if the Government satisfies the burden of proving "a substantial interest to be achieved" by restrictions on such speech and a regulatory technique that is "in

proportion to that interest," i.e., "designed carefully to achieve the State's goal." *Central Hudson*, 447 U.S. at 564. The *Central Hudson* framework thus asks (1) "whether the asserted governmental interest is substantial," (2) "whether the regulation directly advances the governmental interest asserted," and (3) "whether it is not more extensive than is necessary to serve that interest." *Id.* at 566. Under this test, the Supreme Court has invalidated numerous restrictions on speech.[9]

The NPRM recognizes that the opt-in consent requirement imposed by the FCC raises First Amendment questions. The NPRM cites *Central Hudson* (NPRM ¶302), as well as the Tenth Circuit's decision in *U.S. West* (NPRM ¶96 n.469). The NPRM explains that "the Tenth Circuit found an earlier set of rules with fewer opt-out options to be insufficiently supported by the record at the time." (NPRM ¶96.) The NPRM asserts that the proposed rules comply with the requirements of intermediate First Amendment scrutiny, because they "are intended to directly advance both the substantial public interest in consumer privacy as well as Section 222's mandate to protect customer confidentiality, while not being more extensive than necessary to serve those interests, according to the criteria of *Central Hudson*." *Id.*

The NPRM's unsupported assertions do not withstand scrutiny. The broadband context is very different from the voice context governed by Section 222, and intermediate scrutiny bars the FCC from assuming an equivalence and simply transplanting rules from one situation to the other. Moreover, the purported distinctions drawn in the NPRM between *U.S. West* and the instant

[9] *See Thompson v. W. States Med. Ctr.*, 535 U.S. 357, 360 (2002) (striking down law banning advertising and promotion of certain compounded drugs); *Lorillard Tobacco Co. v. Reilly*, 533 U.S. 525, 532, 561-67 (2001) (striking down restrictions on tobacco advertising); *United States v. United Foods, Inc.*, 533 U.S. 405 (2001) (striking down a modest assessment on mushroom growers); *44 Liquormart, Inc. v. Rhode Island*, 517 U.S. 484, 489 (1996) (striking down state ban on price advertising for alcoholic beverages); *Rubin v. Coors Brewing Co.*, 514 U.S. 476, 490-91 (1995) (striking down restrictions on alcohol labeling); *Ibanez v. Fla. Dep't of Bus. & Prof'l Regulation, Bd. of Accountancy*, 512 U.S. 136, 138-39, 143-49 (1994) (overturning reprimand of attorney who used CPA and CFP designations in advertising); *Edenfield v. Fane*, 507 U.S. 761, 763, 770-71 (1993) (overturning ban on in-person solicitation by CPAs); *City of Cincinnati v. Discovery Network, Inc.*, 507 U.S. 410, 412, 424 (1993) (invalidating regulation of newsracks for commercial handbills).

proceeding do not warrant a different result. The reason that the Tenth Circuit invalidated the prior CPNI rules was not simply that there were too "few[] opt-out options," as the proposal asserts (NPRM ¶96); the defects in the prior rules were much more fundamental, and the instant proposed rules are even less warranted or defensible under First Amendment principles and jurisprudence.

The proposed rules cannot meet the *Central Hudson* test, much less the requirements of full First Amendment scrutiny. Contrary to the NPRM's insistence, technological and market developments since the *U.S. West* decision in 1999 make the proposed rules even *more constitutionally problematic* than the CPNI regulations invalidated by the Tenth Circuit. The proposed rules would impose a *much larger* burden on speech and are far *less* tailored to any substantial governmental interest.

1. The Burden on Speech Is Substantial: The Proposed Rules Restrict A Great Deal Of Speech.

The FCC's proposal would not only restrict a company's cross-marketing activities (as did the CPNI rules for telephone carriers in the *U.S. West* case), but would also have an entirely new and very substantial adverse impact on speech not at issue in the voice CPNI case: it could effectively prevent broadband ISPs from entering the online advertising market to supply targeted advertising to consumers. As the NPRM acknowledges, "many consumers want targeted advertising that provides very useful information in a timely (sometimes immediate) manner." (NPRM ¶12.) Yet the sweeping opt-in consent requirements imposed on ISPs' use of customer information would effectively prevent such ISP speech for the vast majority of their customers.

Excluding ISPs from this market represents an enormous restriction on their constitutionally protected communication with consumers. According to some estimates, the

online advertising market is projected to grow to as much as $220.38 billion by 2019.[10] The exclusion of ISPs also makes little sense in terms of the asserted governmental interest. Some 70% of the online ad market is dominated by large Internet companies *other than* ISPs, and no ISP is in the top 10.[11] Two recent industry reports showed Facebook and Google are the "dominant players" in the digital advertising market, accounting for 64% of revenue in 2015.[12] And another recently concluded, "We can't think of any other media marketplace with this level of dominance."[13] Social media advertising revenue increased at a 55% annual rate from 2012 to 2014.[14] Facebook alone had mobile advertising revenues of over $7.39 billion in 2014 and total advertising revenues of over $11.5 billion.[15]

The leaders in online advertising gained that position precisely because of their insights into user activity and access to large amounts of consumer data. The typical online American spends two hours daily on social media.[16] On average, Americans check their Facebook, Twitter, and other social media accounts 17 times per day.[17] In the course of these interactions, social media platforms, search engines, browsers, mobile apps, and other companies gain deep insights

---

[10] *See* MarketsandMarkets, "Online Advertising Market by Search Engine Marketing, Display Advertising, Classifieds, Mobile, Video, Lead Generation, Rich Media - Global Advancements, Forecasts & Analysis (2014 - 2019)," available at http://www.marketsandmarkets.com/PressReleases/online-advertising.asp.

[11] Peter Swire (Associate Director, The Institute for Information, Security & Privacy at Georgia Tech; Huang Professor of Law, Georgia Tech Scheller College of Business), *Online Privacy & ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others* (The Institute for Information, Security & Privacy at Georgia Tech) 3 (Feb. 29, 2016) ("Swire Report, *Online Privacy & ISPs*").

[12] Aleksandra Gjorgievska, Google and Facebook Lead Digital Ad Industry to Revenue Record, Bloomberg Technology (April 21, 2016, 8:04 PM CDT), available at http://www.bloomberg.com/news/articles/2016-04-22/google-and-facebook-lead-digital-ad-industry-to-revenue-record.

[13] Moffett Nathanson, *The Digital Duopoly* 3 (May 3, 2016).

[14] Swire Report, *Online Privacy & ISPs* at 43.

[15] *Id.*

[16] *Id.*

[17] *Id.*

into users' online activity and typically utilize that collected data for targeted advertising and other purposes. These companies have an advantage, because users often log into social media and other platforms across multiple devices, such as smartphones, tablets, and laptops. Hence, Facebook, Google, Apple, Microsoft, and their peers are able to engage in *cross-device* data collection – which ISPs typically cannot. Moreover, users frequently stay logged in to these websites when they exit them so that they do not have to re-enter their log-in credentials the next time they visit; services like Facebook thus are able to track users even when the users are not actively engaged on the sites. Facebook can also gain access to customer data from sites that have Facebook social plug-ins – including any website that has a Facebook "like" button or other plug-ins.

By restricting only a small segment of the marketplace from using this same information for lawful speech, the FCC's proposed rules will severely disadvantage ISPs. As noted in a recent Moody's report, "Absent an alignment of rules between the FTC and FCC regarding these privacy laws, a distinct competitive advantage will be given to online digital advertisers as more advertising dollars will continue to move in secular fashion from traditional television providers towards digital platform providers."[18] The NPRM recognizes that edge providers "are not subject to the same regulatory framework, and that this regulatory disparity could have competitive ripple effects." (NPRM ¶ 132). In constitutional terms, this represents a substantial burden on the protected expression of broadband ISPs.

2. The First *Central Hudson* Prong: Whether the FCC Has Asserted A "Substantial" Governmental Interest.

One of the enduring principles of *Central Hudson* is that "a governmental body seeking to sustain a restriction on commercial speech must demonstrate that the harms it recites are real and

[18] Emily Field, "Moody's Says FCC Internet Privacy Rules Could Hurt ISPs," *Law360* (Mar. 15, 2016, 6:00 PM EST), available at http://www.law360.com/articles/771825/moody-s-says-fcc-internet-privacy-rules-could-hurt-isps (quoting Moody's Sector Comment on the FCC's broadband privacy proposal).

that its restriction will in fact alleviate them to a material degree." *Edenfield v. Fane*, 507 U.S. 761, 770-71 (1993). That burden "is not satisfied by mere speculation and conjecture," *id*. at 770, or by "anecdotal evidence and educated guesses," *Rubin v. Coors Brewing Co*., 514 U.S. 476, 490 (1995). In *Ibanez v. Florida Department of Business and Professional Regulation*, 512 U.S. 136 (1994), for example, the Court explained that the State's "concern about the possibility of deception in hypothetical cases is not sufficient," *id.* at 145, and demanded actual evidence of the harm the State sought to address, *id.* at 145 n.10. "Given the state of this record – the failure of the Board to point to any harm that is potentially real, not purely hypothetical – we are satisfied that the Board's action is unjustified." *Id.* at 146.

The *U.S. West* decision enforced this evidentiary burden in finding that the FCC's prior CPNI rules did not comply with *Central Hudson*. The Tenth Circuit explained that merely reciting the term "privacy" did not establish a substantial governmental interest: "When faced with a constitutional challenge, the government bears the responsibility of building a record adequate to clearly articulate and justify the state interest." *U.S. West*, 182 F.3d at 1234. The court opined that the government cannot satisfy "the *Central Hudson* test by merely asserting a broad interest in privacy. It must specify the particular notion of privacy and interest served. Moreover, privacy is not an absolute good because it imposes real costs on society. Therefore, the specific privacy interest must be substantial, demonstrating that the state has considered the proper balancing of the benefits and harms of privacy. In sum, privacy may only constitute a substantial state interest if the government specifically articulates and properly justifies it." *Id*. at 1234-35.

The Tenth Circuit found that the FCC had failed to meet that burden, explaining that "[t]he government presents no evidence showing the harm to either privacy or competition is real. Instead, the government relies on speculation that harm to privacy and competition for new

services will result if carriers use CPNI." *Id*. at 1237. The court noted that the government presented concerns "in the abstract," but had failed to demonstrate how they "may occur in reality with respect to CPNI." *Id.*

The same is true here. The FCC has failed to demonstrate that its proposal for greater regulation of ISPs than all other actors is necessary to serve an important governmental interest, let alone adequately tailored to that ostensible purpose. Certainly, 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. To the contrary, the NPRM acknowledges that "many consumers *want* targeted advertising that provides very useful information in a timely (sometimes immediate) manner." (NPRM ¶12 (italics added).)

Further, customer online activity today is decreasingly visible to ISPs – and certainly less visible than when the FTC concluded (in 2012) that ISPs should be treated the same as other large platform providers. Internet users are increasingly moving from single stationary devices (a single home desktop connected to the Internet by a single ISP) to multiple mobile devices and connections. By 2014, 46% of mobile data traffic was transmitted over WiFi networks (which are not visible to the user's ISP), and that figure is expected to grow to 60% by 2020.[19] In 2016, the average Internet user has 6.1 connected devices, many of which are mobile and which connect to the Internet from diverse and changing locations (from cell service to Starbucks) served by multiple ISPs.[20] 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.[21]

[19] Swire Report, *Online Privacy & ISPs* at 43.

[20] *Id.* at 3.

[21] *Id.*

In addition, online traffic is rapidly shifting to encryption (such as HTTPS), which eliminates the ability of ISPs to see users' content and the detailed URLs of the sites they visit. Today, all of the top 10 websites either encrypt by default or upon user log-in, as do 42 of the top 50 sites.[22] The HTTPS portion of total Internet traffic has risen from 13% to 49% just since April 2014, and an estimated 70% of traffic will be encrypted by the end of 2016.[23] Encryption further blocks ISPs' visibility to a growing majority of user activity.

Moreover, Internet users increasingly rely on proxy services and Virtual Private Networks ("VPNs") to provide gateway access to the Internet.[24] When this occurs, the user relies on a proxy service or VPN (rather than an ISP) to match the user's web address request to the correct domain and specific Internet Protocol ("IP") address.[25] Thus, the ISP cannot even see the domain name that a user is visiting, much less the content of the packets the user is sending and receiving.[26]

These technological and market changes make it even more implausible that the FCC could establish a substantial interest in going further than the FTC's regulatory regime or to show that the FCC's proposed restriction on speech serves a substantial governmental interest. This alone is fatal to the FCC's proposal.

[22] Swire Report, *Online Privacy & ISPs* at 3.

[23] *Id.*

[24] *Id.*

[25] *Id.*

[26] *Id.*

3. The Second *Central Hudson* Prong: Whether the Regulation is Tailored To and "Directly Advances" the Asserted Interest.

(a) The Under-Inclusiveness Of The Proposed Rules Shows That They Fail The Second Prong.

The FCC's proposal does not cover other Internet companies – including the "large platform providers" – that have access to as much or more customer data than ISPs and have an outsized presence in the online advertising market. This under-inclusiveness is also fatal to the proposed rules. The point is not that the FCC can or should regulate edge providers or that heightened privacy standards are needed for those providers. Rather, the point is that the FCC's proposed rules for broadband ISPs do not directly advance, and are not tailored to, any important governmental interest.

Under intermediate scrutiny, a restriction on speech is invalid unless it "directly advance[s] the state interest involved; the regulation may not be sustained if it provides only ineffective or remote support for the government's purpose." *Central Hudson*, 447 U.S. at 564. Thus, "the Court has declined to uphold regulations that only indirectly advance the state interest involved," such as in *Bates v. State Bar of Arizona*, 433 U.S. 350 (1977), which struck down an advertising restraint that was "an ineffective way" of achieving the asserted interest. *Id.* at 378.

The failure to regulate similar (and more obvious) harms can doom a restriction on speech under the second *Central Hudson* prong. In *Rubin v. Coors Brewing*, 514 U.S. 476 (1995), for example, the Court relied on an under-inclusive patchwork of federal laws to conclude that the challenged restriction on speech failed intermediate scrutiny. In *Rubin*, the government asserted an interest in preventing alcohol "strength wars," but the Court explained that "[t]he failure to prohibit the disclosure of alcohol content in advertising, which would seem to constitute a more influential weapon in any strength war than labels, makes no rational sense if the Government's true aim is to suppress strength wars." 514 U.S. at 488. The Court added that, "[i]f combating

strength wars were the goal, we would assume that Congress would regulate disclosure of alcohol content for the strongest beverages as well as for the weakest ones." *Id.* "One would think that if the Government sought to suppress strength wars by prohibiting numerical disclosures of alcohol content, it also would preclude brewers from indicating higher alcohol beverages by using descriptive terms." *Id.* at 489.

By the same token, in *Greater New Orleans Broadcasting Association, Inc. v. United States*, 527 U.S. 173 (1999), the Court held that the FCC could not justify (under intermediate scrutiny) a statutory restriction on advertising by private casinos, when the law allowed the same advertising by tribal casinos: "The operation of [the statute] and its attendant regulatory regime is so pierced by exemptions and inconsistencies that the Government cannot hope to exonerate it." *Id.* at 190. "[T]he Government presents no convincing reason for pegging its speech ban to the identity of the owners or operators of the advertised casinos." *Id*. at 191.

The same reasoning is applicable here. The FCC's proposal provides only ineffective and remote support for any asserted interest in protecting "privacy" and is not drawn directly to advance such an interest.

Further, the speaker-specific nature of the FCC's proposal – the singling out of ISPs – raises separate concerns under First Amendment equal protection principles. The Supreme Court "ha[s] frequently condemned such discrimination among different users of the same medium for expression." *Police Department of City of Chicago v. Mosley*, 408 U.S. 92, 96 (1972); *see Rosenberger v. Rector & Visitors of University of Virginia*, 515 U.S. 819, 828 (2000) ("government regulation may not favor one speaker over another"); *Arkansas Writers' Project, Inc. v. Ragland*, 481 U.S. 221, 229 (1987) (a tax that applies to some magazines but not to others "is particularly repugnant to First Amendment principles"). The proposed rules would both

distinguish among different speakers in the same medium (such as online advertising) and distinguish among technologies and thus among media.

Speaker-specific restrictions are problematic even under intermediate scrutiny. The *Greater New Orleans* Court explained that, "[e]ven under the degree of scrutiny that we have applied in commercial speech cases, decisions that select among speakers conveying virtually identical messages are in serious tension with the principles undergirding the First Amendment." 527 U.S. at 193-94. And *Sorrell* treated the speaker-based nature of the restriction both as a reason that "heightened scrutiny" might apply under the First Amendment[27] *and* as a reason that the Vermont law failed intermediate scrutiny. *See* 564 U.S. at 573 ("The explicit structure of the statute allows the information to be studied and used by all but a narrow class of disfavored speakers. Given the information's widespread availability and many permissible uses, the State's asserted interest in physician confidentiality does not justify the burden that [Vermont law] places on protected expression.").

(b) The Commission's Reasons For The Limited Scope Of Its Proposal Do Not Justify the Restrictions On Speech.

The FCC's proposal asserts that "a consumer, once signed up for a broadband service, simply cannot avoid that network in the same manner as a consumer can instantaneously (and without penalty) switch search engines (including to ones that provide extra privacy protections), surf among competing websites, and select among diverse applications." (NPRM ¶4.) But this assertion is cannot be squared with the factual record, which shows that the average Internet user

[27] *Sorrell*, 564 U.S. at 563-64 ("Vermont's law enacts content-and speaker-based restrictions on the sale, disclosure, and use of prescriber-identifying information."); *id.* at 564 (noting that Vermont's restrictions were "speaker-based rules"); *id.* at 567 ("Vermont's law does not simply have an effect on speech, but is directed at certain content and is aimed at particular speakers"); *id.* at 571 (Vermont "imposes a speaker- and content-based burden on protected expression, and *that circumstance is sufficient to justify application of heightened scrutiny*.") (emphasis added).

moves among six different devices (many of which are mobile and which connect to the Internet from diverse and changing locations served by multiple ISPs) and that as much as 70% of Internet traffic will be encrypted by the end of 2016. The average user can readily switch her mobile broadband provider during a coffee break, but switching an e-mail address, social network, or operating system platform can be truly disruptive.

The NPRM further states that the under-inclusiveness of the proposed rules is "mitigated" by the fact that the "the FTC actively enforces the prohibitions in its organic statute against unfair and deceptive practices against companies in the broadband ecosystem" and that "large edge providers are increasingly adopting opt-in regimes for sharing of some types of sensitive information," such as geo-location information. (NPRM ¶ 132). These justifications do not withstand scrutiny. The FTC applies a *different set of rules* to non-ISPs, which is the key problem, so it matters not (for purposes of this constitutional analysis) whether the FTC will vigorously enforce them. Indeed, the availability of the FTC's regulatory scheme as an obvious alternative that is less speech-suppressing dooms the FCC's proposed rules under the third prong of the *Central Hudson* test. In addition, the fact that certain members of the industry have implemented an opt-in system for sharing certain sensitive data with third parties does not help the FCC's proposal, which (i) makes no distinction between sensitive and non-sensitive data but rather treats all data equally harshly, (ii) restricts both use and third-party sharing of customer data, and (iii) is mandatory, not a form of voluntary self-regulation.

The FCC also defends the under-inclusiveness of its proposal by contending that it lacks authority to impose its new privacy rules on edge providers because they are not "telecommunications carriers" and thus are beyond the scope of Section 222. But that misses the point: the question is not why the FCC is refraining from regulating edge providers, but why it is

imposing especially burdensome rules on broadband ISPs when (i) ISPs have been under the FTC rules for many years without a problem (as FTC Chairwoman Ramirez and FTC Commissioner Ohlhausen recently told a Senate Judiciary hearing on the FCC's privacy NPRM),[28] (ii) large Internet companies remain subject to the FTC regime, and (iii) nothing has changed in the marketplace or otherwise that would justify this radical departure. The FCC has no valid answer to these points.

The Supreme Court has not endorsed statutory limits on regulatory authority or jurisdiction as a justification for discriminatory speech rules. The First Amendment is, after all, a prohibition *directed to Congress* and thus applicable to the legislative schemes Congress enacts without regard to how the national legislature chooses to allocate and subdivide administrative authority and regulatory jurisdiction among distinct federal agencies. Accordingly, the Court has analyzed regulatory schemes *as a whole*, rather than permitting the government to divide and conquer by confining its tailoring defense to individual statutory provisions viewed in isolation. In *Greater New Orleans*, for example, the Court summarized its decision in *Rubin* as "conclud[ing] that the effect of the challenged restriction on commercial speech had to be evaluated *in the context of the entire regulatory scheme*, *rather than in isolation*, and we invalidated the restriction based on the '*overall irrationality* of the Government's regulatory scheme.'" 527 U.S. at 192-93 (quoting 514 U.S. at 488) (emphasis added).

Here, the overall effect of the government's regulatory regime is to subject broadband ISPs to the harshness of the FCC's proposal even though other *non-ISP* speakers collecting and using the very same online customer data for the very same purposes as ISPs will continue to be governed

[28] Examining the Proposed FCC Privacy Rules: Hearing before the Subcommittee on Privacy, Technology and the Law, Senate Committee on the Judiciary (May 11, 2016) (available at http://www.judiciary.senate.gov/meetings/examining-the-proposed-fcc-privacy-rules/).

by the FTC's far less speech-suppressing regime. The disparate treatment of ISPs does not pass muster under the second prong of *Central Hudson.*

(c) The Proposed Rules Suffer From Additional Mis-Matches Between The FCC's Asserted Interests and the Restrictions on Speech.

The proposed rules suffer from further profound mis-matches. The proposal is not keyed to the sensitivity of consumer information, unlike the FTC's existing regulatory scheme. The FCC's proposal uses the same blunderbuss approach for all types of information. Further, the FCC's asserted interests arise from the *sharing* of information between an ISP and unaffiliated third parties, but its proposal seeks to regulate how an ISP itself or its affiliates can *use* information – for example, by targeting online advertising to the consumers for whom it is most relevant. And, as noted, the proposal also raises content-based distinctions that trigger additional constitutional concerns.

(i) The Proposed Rules Are Not Tailored To Any Interest In Restricting The Sharing of Private Information With Third Parties.

The FCC does not assert an interest in preventing customers from *receiving* targeted commercial messages that are most relevant to them. As noted earlier, the Commission concedes that "many consumers want targeted advertising that provides very useful information in a timely (sometimes immediate) manner." (NPRM ¶12.)

Rather, the FCC is asserting an interest primarily in preventing the unauthorized *sharing* or *disclosure* of personal information that would violate a consumer's privacy. The purported evils cited by the NPRM all relate to situations in which *sensitive* personal information is *shared*.[29] For example:

[29] To the extent the FCC might argue that there is a substantial interest in limiting an ISP's use of information in its possession, the Commission has not even tried to make that case.

- The NPRM cites such "personal interests" as "freedom from identity theft, financial loss, or other economic harms" and "concerns that intimate, personal details could become grist for the mills of public embarrassment or harassment or the basis for opaque, but harmful judgments, including discrimination." (NPRM ¶3.)
- The NPRM discusses "very sensitive and very personal information that could threaten a person's financial security, reveal embarrassing or even harmful details of medical history, or disclose to prying eyes the intimate details of interests, physical presence, or fears." (NPRM ¶2.)
- The NPRM refers to the Facebook30 and Google31 FTC proceedings, which involved the disclosure of user information to third parties. For example, the FTC alleged that Facebook acted unfairly when, after representing to its users that it would honor their privacy preferences and not share certain personal information with third parties, it retroactively began to share precisely such information without sufficiently clear notice to its customers.32

Despite these assertions, the FCC has not shown that ISPs are in a position, much less a unique position, to disclose "very sensitive and very personal information," such as "details of medical history." In fact, the cited examples in the NPRM all involve edge providers, *not* ISPs. Nor are the proposed rules limited to the sharing of such intimate information. Rather, they govern *all* types and *all* uses of customer information. There is thus a fundamental mis-match between the proposed rules and their rationale.

Moreover, the proposed rules go far beyond situations where an ISP *sells* or *shares* information with unaffiliated *third parties* for the latter's own purposes. The rules are not tailored to any supposed interest in preventing the *disclosure* of sensitive or embarrassing personal

---

[30] *See* Facebook, Inc., Complaint, F.T.C. File No. 092-3184 (2012), available at https://www.ftc.gov/enforcement/casesproceedings/092-3184/facebook-inc; Facebook, Inc., Decision and Order, F.T.C. File No. 092-3184 (2012), available at https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc (Facebook Consent Order).

[31] Google, Inc., Complaint, F.T.C. File No. 102-3136 (2011), available at https://www.ftc.gov/enforcement/cases-proceedings/102-3136/google-inc-matter; Google, Inc., Decision and Order, F.T.C. File No. 102-3136 (2011), available at https://www.ftc.gov/enforcement/cases-proceedings/102-3136/google-inc-matter.

[32] *See* Facebook, Inc., Complaint, F.T.C. File No. 092-3184 (2012), available at https://www.ftc.gov/enforcement/casesproceedings/092-3184/facebook-inc.

information. Rather, the rules also cover *wholly internal use* of information within an ISP. For example, the proposal would require an affirmative opt-in procedure (which would discourage or suppress speech) where ISPs seek to *use* customer information *within the ISP itself* to develop and communicate online ads on social media, *even where the ISPs do not disclose any customer information to a third party*. In addition, opt-in would be required before a broadband ISP could disclose information to an affiliate for non-communications-related services *even if the affiliate does not actually use the data*. This imposes a significant burden on broadband ISPs providers to maintain separate databases and extensively track the information that can be shared with specific affiliates.[33]

Similarly, the proposal would require an opt-in procedure where ISPs seek to use customer information to market non-communications-related services such as home security, energy management, or music services to the ISPs' *existing customers* – again, *even where the ISPs do not disclose customer information to a third party.* To illustrate, the proposal would prohibit an ISP *from using information about its customers to offer a discounted bundle of its own services to its own customers without their opt-in consent or to offer an accessory that is compatible with the customer's device*.

Because the proposal regulates the *internal use* of customer information in these extreme ways, it fails to meet the requirement of *Central Hudson* that the restriction on speech be tailored to the asserted governmental interest.

[33] In *FEC v. Massachusetts Citizens for Life*, 479 U.S. 238 (1986), a plurality treated the burden of keeping track of a separate segregated fund for making expenditures in connection with federal elections as too heavy to meet First Amendment standards, citing "[d]etailed recordkeeping" obligations, "administrative costs," and "the statute's practical effect" of "discourag[ing] protected speech." *Id.* at 254-55. Writing separately, Justice O'Connor agreed that the "additional organizational restraints" violated the First Amendment. *Id.* at 266 (opinion concurring in part and concurring in the judgment).

(ii) The Proposal Draws Impermissible Content-Based Distinctions Based On What a Marketer Says.

Besides failing *Central Hudson's* tailoring requirement, the proposal draws content-based distinctions that trigger additional constitutional concerns.

The proposal would impose an *opt-out* requirement for ISPs to use customer data (and to share it with their affiliates) to market *communications-related* services. But the proposal would impose an *opt-in* requirement (again, a significant suppression of speech) if an ISP sought to use or share customer information to market *non-communications-related* services. Thus, the degree of the burden on speech turns on *what the speaker says* and the *content of the speaker's message* – whether the marketing relates to a "communications-related service" (such as voice) or a "non-communications-related service" (such as home security, energy management, or music services).

The burden on speech is thus unquestionably "content-based." Highly instructive here is *Sorrell*, where the Court opined that restrictions on the availability and use of prescriber-identifying information were "content-based" because they applied only to marketing speech. *See* 564 U.S. at 571 ("So long as they do not engage in marketing, many speakers can obtain and use the information."). Similarly, in *City of Cincinnati v. Discovery Network, Inc.*, 507 U.S. 410 (1993), the Court explained that a municipal ban on newsracks for "commercial handbills" but not "newspapers" was "content-based": "Under the city's newsrack policy, whether any particular newsrack falls within the ban is determined by the content of the publication resting inside that newsrack. Thus, by any commonsense understanding of the term, the ban in this case is 'content based.'" *Id.* at 429. The Court added that "the very basis for the regulation is the difference in content between ordinary newspapers and commercial speech." *Id.*; *see also Reed v. Town of Gilbert*, 135 S. Ct. 2218, 2227 (2015) ("The Town's Sign Code is content based on its face. It

defines 'Temporary Directional Signs' on the basis of whether a sign conveys the message of directing the public to church or some other 'qualifying event.'").

Precisely the same reasoning applies here, because the very basis for the FCC's proposal is the difference in content between communications-related marketing and non-communications-related marketing. Content-based burdens, of course, "are presumptively invalid." *R.A.V. v. St. Paul*, 505 U.S. 377, 382 (1992).

The content-based nature of the FCC's proposal provides an additional ground for concluding that it fails the *Central Hudson* tailoring requirement. As the *Discovery Network* Court held in striking down the newsrack prohibition: "Because the distinction Cincinnati has drawn [between 'newspapers' and 'commercial handbills'] has absolutely no bearing on the interests it has asserted, we have no difficulty concluding, as did the two courts below, that the city has not established the 'fit' between its goals and its chosen means that is required by" intermediate scrutiny. 507 U.S. at 428.

Here, too, the FCC's proposal draws impermissible content-based distinctions based on what a marketer says – distinctions that are not related to the asserted governmental interest. The Commission appears to suggest that these distinctions track customer expectations (*see* NPRM ¶¶123, 127), but the Commission's suggestion rests on supposition rather than evidence. Indeed, the NPRM all but confesses the lack of evidence on the point, because it "invite[s] comment" "specifically on customers' expectations and preferences." (NPRM ¶123.) In all events, "customer expectations" do not provide an adequate basis for content-based restrictions on speech. Indeed, a primary purpose of the First Amendment is to safeguard speech that *defies* the expectations of its audience. *E.g.*, *Snyder v. Phelps*, 562 U.S. 443, 458 (2011); *Hurley v. Irish–American Gay, Lesbian and Bisexual Group of Boston, Inc.*, 515 U.S. 557, 574 (1995).

(iii) The Proposal Provides No Adequate Basis For Distinguishing Between Corporate Affiliates and Third-Party Agents/Vendors.

The FCC's proposal suffers from yet another tailoring flaw: it distinguishes between all third parties and corporate affiliates, without providing a sufficient basis for that distinction. The proposal would impose an *opt-out* consent requirement for a broadband ISP's sharing of customer data with its *corporate affiliates* for marketing communications-related services, but an *opt-in* requirement if broadband ISPs instead seek to use third parties as agents/vendors to do exactly the same thing. ISPs face an opt-in rule even if they bind these agents/vendors to strict confidentiality duties and even if the ISPs take every other conceivable step to ensure that contractors treat the customer information as carefully as do corporate affiliates. Moreover, under the Communications Act, the act, omission, or failure of these agents are "deemed to be the act, omission, or failure of [the employing] carrier . . . as well as the person."[34] By operation of law, therefore, these agents/vendors are treated no differently from direct employees of the ISP itself for purposes of § 222 and related FCC privacy rules when they use customer information on behalf of, and under the direction of, an ISP. The FCC's legacy CPNI rules likewise draw no distinction between carriers and their affiliates and agents.[35]

The proposal offers little evidentiary justification for departing from past precedents and drawing such distinctions between corporate affiliates and third-party agents/vendors when they use customer information solely on behalf of, and at the direction of, an ISP. The proposal's

[34] 47 U.S.C. § 217. The Commission did not forbear from this enforcement provision in its Open Internet Order. *See Protecting and Promoting the Open Internet*, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd. 5601, ¶453 (2015).

[35] 47 C.F.R. § 64.2007(3)(b) ("A telecommunications carrier may, subject to opt-out approval or opt-in approval, disclose its customer's individually identifiable CPNI, for the purpose of marketing communications-related services to that customer, *to its agents and its affiliates* that provide communications-related services.") (emphasis added).

discussion of the privacy risks posed by third parties rests on sheer speculation. (NPRM ¶¶129-31.) Arbitrary lines on an organization chart do not provide the kind of rigorous basis for a restriction on speech that the First Amendment demands. Indeed, the FCC would likely hold an ISP accountable under Section 217 of the Act for violations of FCC rules by an agent – yet it seeks to severely restrict and effectively deny an ISP the ability to use third parties as agents for customer marketing efforts. The FCC should not be permitted to have it both ways.

4. The Third *Central Hudson* Prong: A Notice-and-Choice Regulatory Regime Consistent with the FTC's Approach Provides An Obvious Alternative That Is Less Speech-Suppressing.

In 1999, when *U.S. West* was decided, there was no alternate regulatory scheme that could address the FCC's privacy concerns in the voice CPNI context. Today, the industry has had years of experience with the more tailored privacy protections of the FTC, which is the nation's chief privacy policy and enforcement agency. The NPRM recognizes the importance of the FTC's "leadership" and "expertise," as well as the series of "precedent-setting consent orders addressing privacy practices on the Internet" secured by the FTC. (NPRM ¶ 8.)

The FTC's approach to privacy protection focuses on punishing deceptive or unfair practices rather than creating a highly burdensome opt-in requirement. The FTC has adopted best practice guidance for ISPs and edge providers alike regarding notice and consumer choice. Of particular relevance for our purposes, the FTC's privacy framework:[36]

- Allows parties to engage in first-party marketing for *all* of their services to their customers (i.e., no limits on "communications-related services" or otherwise) based on *implied consent*, because, as the FTC correctly explained such marketing is within the context of the relationship between the company and customer and within the expectation of the customer.
- Only requires *opt-in consent* with respect to the collection and use of a very narrow category of "sensitive data" defined to include data about children,

[36] *See* FTC, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers" (Mar. 2012).

financial and health information, Social Security numbers, and certain geolocation data.

- Allows all other uses and disclosures by companies to occur under an *opt-out* consent mechanism that begins with a baseline of speech rather than a baseline of no speech.

In short, whereas the FTC's privacy framework is based primarily on an *opt-out* regime, the FCC's proposal flips this on its head, proposing an unprecedented and far-reaching *opt-in* regime targeted solely at ISPs and covering *all* data, not just sensitive data.

Moreover, the FTC experience demonstrates that there is nothing unique about ISPs' data collection, use, or sharing practices that would justify the FCC's proposed Draconian privacy rules. The FTC's 2012 Privacy Report specifically included ISPs in a group of "large platform providers," along with browsers, operating systems, and social media platforms.[37] The FTC's 2012 Privacy Report concluded, "[T]he Commission agrees that any privacy framework should be technology neutral. ISPs are just one type of large platform provider that may have access to all or nearly all of a consumer's online activity."[38] Tellingly, the FTC grouped ISPs with the other "large platform providers" in 2012 – prior to the recent rise of encryption and the explosion in WiFi access, which have blocked ISPs from a comprehensive view of any given consumer's behavior. The FTC's approach (of grouping ISPs with other platform providers) has even greater force in the current technological environment.

An FTC public workshop in December 2012 resulted in no new findings that ISP privacy practices were somehow especially problematic. Indeed, the summary of the consensus findings by the Associate Director of the Privacy Division at the FTC underscored that there is nothing unique about ISPs. The workshop found:

[37] *Id.* at ix.

[38] *Id.* at 56.

- Many Internet company platforms afford a fairly comprehensive window into consumers' browsing behavior.[39]
- There are numerous benefits of tracking: Google was able to anticipate flu trends, cities use traffic flow data to install traffic lights, and advertising pays for free content.[40]
- There is a need for regulatory neutrality across providers and technology. In the words of the Associate Director, "[w]e can't be picking winners and losers in this space."[41]

The FTC never adopted special rules for ISPs or other large platform providers. In fact, the FTC has consistently adhered to a technology-neutral and speaker-neutral approach to privacy regulation. Nor did the FTC make any distinction with respect to ISPs in the numerous privacy-related studies, round tables, analyses, and reports that the FTC has conducted and produced in this period, including on the Internet of Things, Data Brokers, and Cross-Device Tracking[42] – yet the Internet continued to boom with relatively few consumer privacy issues.

---

[39] Transcript of Federal Trade Commission Workshop, *The Big Picture: Comprehensive Online Data Collection* 272 (Dec. 6, 2012), available at https://www.ftc.gov/sites/default/files/documents/public_events/The%20Big%20Picture%3A%20Comprehensive%20Online%20Data%20Collection/bigpicture_transcript_21206ftc.pdf.

[40] *Id.*

[41] *Id.*

[42] For example, in the FTC's report on the Internet of Things adopted just last year, the FTC maintained its technology-neutral approach and reiterated the notice and choice principles that it had adopted in its 2012 Privacy Report. *See* FTC Staff Report, Internet of Things v (Jan. 2105), available at https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf ("[T]here is no one-size-fits-all approach. . . . This does not mean that every data collection requires choice. The Commission has recognized that providing choices for every instance of data collection is not necessary to protect privacy. In its 2012 Privacy Report, which set forth recommended best practices, the Commission stated that companies should not be compelled to provide choice before collecting and using consumer data for practices that are consistent with the context of a transaction or the company's relationship with the consumer. Indeed, because these data uses are generally consistent with consumers' reasonable expectations, the cost to consumers and businesses of providing notice and choice likely outweighs the benefits. This principle applies equally to the Internet of Things."); *id.* at vi ("Recognizing concerns that a notice and choice approach could restrict beneficial new uses of data, staff has incorporated certain elements of the use-based model into its approach. For instance, the idea of choices being keyed to context takes into account how the data will be used: if a use is consistent with the context of the interaction – in other words, it is an expected use – then a company need not offer a choice to the consumer."); *id.* at viii (any legislation should be "flexible" and "technology-neutral").

And, to the extent issues arose, the FTC brought far more privacy enforcement actions against social media companies and other edge providers (such as Google, Facebook, and Amazon) than against ISPs.[43]

Despite this substantial record evidence, the FCC proposes to depart from the FTC's approach in significant and burdensome ways:

- As shown, the FCC proposal requires customer opt-in for "*all . . . uses and sharing of customer data*" except "for the purposes of marketing other communication-related services" and "marketing the type of broadband service purchased by the consumer." In contrast, the FTC Privacy Report recommends requiring an opt-in consent only for the use of sensitive information, for example, about children, and financial and health-related data (as well as for the use of so-called deep packet inspection ("DPI") for marketing purposes, which the FTC suggested should require affirmative express consent).
- In addition to proposing customer opt-in as the default standard, the FCC proposal further requires ISPs to allow customers to opt out of the use of customer data for marketing "other communications-related services" offered by the ISP or its affiliates. In contrast, the FTC Report does not identify any need for companies to provide a mechanism that allows customers to opt out from first-party marketing, because, as noted, the FTC found that such first-party marketing (including when it comes from commonly branded affiliates) is within the expectations of the customer, in which case the customer's consent can reasonably be deemed to be implied. Indeed, the Obama Administration's "Consumer Privacy Bill of Rights," adopted in 2012, also agreed that first-party marketing is within the expectations of customers and thus consent may be implied.[44]

---

[43] *See* Snapchat, Inc., Administrative Action (132 3078) and Consent Order (December 31, 2014); Path, Inc., Federal Action (122 3158), Consent Decree, Order for Civil Penalties, Permanent Injunction (February 1, 2013); Myspace LLC, Administrative Action (102 3058); Consent Order (September 11, 2012); Facebook, Inc., Administrative Action (092 3184), Consent Order (August 10, 2012); Google, Inc. (Buzz), Administrative Action (102 3136), Consent Order (October 24, 2011); Twitter, Inc., Administrative Action (092 3093), Consent Order (March 11, 2001); Yelp Inc., Federal Action (132 3066), Permanent Injunction and Civil Penalty (September 17, 2014); Fandango, LLC, Administrative Action (132 3089), Consent Order (August 19, 2014); Google, Inc. (Safari), Federal Action (C-4336), Permanent Injunction and Civil Penalty (November 20, 2012); Upromise, Inc., Administrative Action (102 3136), Consent Order (April 3, 2012); Amazon.com, Investigation (May 24, 2001).

[44] White House Report, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* 36 (Feb. 2012), available at www.whitehouse.gov/sites/default/files/privacy-final.pdf; *id.* at 17 ("Similarly, companies may infer consent to use personal data to conduct marketing in the context of most first-party relationships, given the familiarity of this activity in digital and in-person commerce, the visibility of this kind of marketing, the presence of an easily identifiable party to contact to provide feedback, and consumers' opportunity to end their relationship with a company if they are dissatisfied with it.").

- The customer opt-in standard proposed by FCC is far more restrictive than the FTC's approach to consent, which provides companies with flexibility in how they seek consent from consumers.
- Unlike the FTC Privacy Report, the "large platform provider" workshop in 2012, and every FTC report since then, which all have consistently recognized that other large platform providers like Facebook and Google may have similar or greater access to consumer data, the FCC proposal does not acknowledge that other entities in the Internet ecosystem collect as much or more data than broadband providers. Rather, while the FCC cites to the FTC's 2012 Privacy Report regarding ISPs' data collection practices (NPRM ¶ 4), it omits any reference to statements in that report regarding other large platform providers that, as noted, the FTC also found collect substantial customer data and should be treated the same as ISPs. The FCC proposal would thus depart from a "technology-neutral" privacy framework and create inconsistent privacy standards with no attempted justification for this radical departure or its anti-competitive, anti-consumer results.

The successful history of the FTC's privacy protections refutes the FCC's assertion that its new rules impose no more restrictions on speech than necessary. Indeed, even prior to the FTC's policy, the *U.S. West* court pointed to "the FCC's failure to adequately consider an obvious and substantially less restrictive alternative" as an indication "that it did not narrowly tailor the CPNI regulations regarding customer approval." 182 F.3d at 1238-39. The Tenth Circuit held that the FCC could not "rely upon its common sense judgment based on experience." *Id*. at 1239. "Such speculation hardly reflects the careful calculation of costs and benefits that our commercial speech jurisprudence requires." *Id.* Now, with a well-established record of experience under the many years of the successful FTC privacy regime, the constitutional case against the FCC's proposal is even stronger. *See also Thompson v. W. States Med. Ctr.*, 535 U.S. 357, 371 (2002) ("if the Government could achieve its interests in a manner that does not restrict speech, or that restricts less speech, the Government must do so"); *Rubin*, 514 U.S. at 491 (the fact that "all of [these alternatives] could advance the Government's asserted interest in a manner less intrusive to . . . First Amendment rights" indicated that the law was "more extensive than necessary"); *44 Liquormart*, 517 U.S. at 507 (plurality opinion) (striking down a prohibition on advertising the

price of alcoholic beverages in part because "alternative forms of regulation that would not involve any restriction on speech would be more likely to achieve the State's goal of promoting temperance").

C. The Canon Of Constitutional Avoidance Requires That the FCC Narrowly Construe Its Authority.

As shown above, the FCC's proposal raises serious constitutional questions under the First Amendment. Given these concerns, the deference ordinarily afforded under *Chevron* is inapplicable. Instead, the Communications Act should be construed as not authorizing the proposed rules. *See United States v. X-Citement Video, Inc*., 513 U.S. 64, 78 (1995); *Edward J. DeBartolo Corp. v. Fla. Gulf Coast Trades Council*, 485 U.S. 568, 575 (1988); *Ashwander v. Tenn. Valley Auth.*, 297 U.S. 288, 347 (1936) (Brandeis, J., concurring).

The rule of constitutional avoidance is particularly salient because the NPRM rests on very thin statutory ice. The FCC is relying on Section 222 of the Communications Act, which governs telecommunications carriers rather than broadband Internet access service providers. Even if the FCC's authority to reclassify broadband services is upheld, there is *no clear congressional statement* purporting to authorize the FCC to go to – much less *beyond* – the limits of its authority under the First Amendment to impose a blanket opt-in consent requirement and other speech restrictions on ISPs with respect to an extremely broad definition of "customer data" with no distinctions based on the data's degree of sensitivity but with distinctions based on the identity of the speaker and the content of the speaker's message.

Section 222 certainly does not *require* the FCC to adopt an opt-in consent requirement – either by its terms or by clear implication. Section 222(f) requires opt-in consent only for location information and only in two specific situations (certain call location information and automatic crash notifications) – confirming that the Commission undoubtedly has discretion to adopt opt-out

consent in other circumstances. Section 222(c)(1) at most *authorizes* a carrier to use CPNI upon "the approval of the customer" – and consent mechanisms used by the FTC and other regulators around the world show that such approval obviously can be obtained via an opt-out procedure as well as via an opt-in procedure. Indeed, the FCC has previously recognized that Section 222's language is flexible enough to allow either opt-out or opt-in consent (or even implied consent in certain cases) to be used to satisfy congressional intent.[45] And the federal CAN-SPAM Act[46] allows third parties who have absolutely no relationship with a consumer to send any kind of marketing or advertising material to that U.S. consumer, subject only to the ability of the consumer/recipient to opt out of such further marketing after the fact. The FCC's proposal, with its opt-in consent requirement for any marketing for non-communications-related services, is directly contrary to the federal policy on email and online marketing (which allows opt-out consent for all companies with respect to *any* marketing).

Accordingly, the FCC should decline to adopt the proposed rules under the canon of constitutional avoidance. Because the Commission's proposals fail under all three prongs of the *Central Hudson* test, *a fortiori* they would also fail under the heightened form of First Amendment scrutiny suggested in *Sorrell.*

D. The 2009 *NCTA* Decision Does Not Support the NPRM.

Finally, the D.C. Circuit's decision in *NCTA v. FCC*, 555 F.3d 996 (D.C. Cir. 2009), provides no support for the FCC's proposal. *NCTA* involved the *sale* of customer information to

[45] *See*, *e.g.*, *In The Matter Of Implementation Of The Telecommunications Act Of 1996: Telecommunications Carriers' Use Of Customer Proprietary Network Information And Other Customer Information*, 17 FCC Rcd. 14860 (2002) (responding to *U.S. West* decision by finding that opt-out consent can also be used to satisfy Section 222, while retaining opt-in consent for certain uses by voice carriers).

[46] CAN-SPAM Act of 2003, 15 U.S.C. §§ 7701 et seq. (establishing confidentiality rules and requirements for commercial email messages, including a consumer opt-out mechanism, rather than adopting an affirmative opt-in requirement).

data brokers. In contrast, the proposed rules govern an ISP's own *use* of customer information, even to market its own products and services to its own customers. The proposed rules further suffer from tailoring flaws and content- and speaker-based distinctions explained above that were not present in *NCTA*. The record of the two proceedings is substantially different. And the Supreme Court's subsequent decision in *Sorrell* made clear that rules restricting the use of customer information trigger First Amendment scrutiny and that mis-matched tailoring (as well as under-inclusive restrictions) are fatal under such scrutiny. Thus, *NCTA*'s reliance on "common sense" to support the FCC's opt-in system (555 F.3d at 1001) does not survive *Sorrell.*

Moreover, the force of the *NCTA* decision is substantially weakened by the petitioners' concessions in that case, which the D.C. Circuit repeatedly stressed.[47] In contrast, the parties to this proceeding have made no such concessions. To the contrary, they have made clear that the proposal's opt-in consent requirement needlessly burdens speech in violation of the First Amendment. And, to the extent Section 222 could be construed as authorizing such an onerous and impermissible regulatory scheme, the statute would be unconstitutional.

Conclusion

The FCC's proposed rules would violate the First Amendment. At minimum, they raise a host of grave constitutional questions and should not be adopted.

[47] *NCTA*, 555 F.3d at 353 ("[T]his case comes to us in a different posture. By conceding the constitutionality of § 222, petitioners necessarily concede at least two factual predicates underlying both the statute and the FCC's Order . . . ."); *id.* at 354 ("[I]s there a 'substantial' governmental interest? Petitioners seem to recognize that they cannot contest the point in light of their agreement that § 222 is constitutional."); *id.* ("The next question that must be posed under *Central Hudson* is whether the FCC's 2007 Order 'directly advances' the governmental interest just identified. Here again petitioners' agreement that § 222 complies with the First Amendment all but settles the issue.").