

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

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

COMMENTS OF ITTA

James M. Smith
Peter Karanjia
DAVIS WRIGHT TREMAINE LLP
1919 Pennsylvania Avenue, NW, Suite 800
Washington, DC 20006
(202) 973-4288
jamesmsmith@dwt.com

Genevieve Morelli
President
ITTA
1101 Vermont Ave., NW, Suite 501
Washington, DC 20005
(202) 898-1519
gmorelli@itta.us

May 27, 2016

TABLE OF CONTENTS

I.	INTRODUCTION AND SUMMARY	1
II.	THE COMMISSION LACKS THE REQUISITE LEGAL AUTHORITY TO ADOPT THE PROPOSED RULES	3
A.	Plain Language and Structure of Section 222 of the Act.....	4
B.	Legislative History of Section 222(a).....	6
C.	The Commission’s Consistent Interpretation of Section 222	7
III.	THE PROPOSED RULES ARE OVERBROAD AND WOULD DISREGARD DECADES OF FTC EXPERTISE IN CONSUMER PRIVACY AND DATA PROTECTION.....	11
A.	The Commission Should Adopt Privacy Rules Modeled Upon and Consistent With the FTC’s Time-Tested and Respected Regime	13
B.	The Commission Should Not Adopt Rules That Disproportionately Disadvantage ISPs Vis-à-Vis Edge Providers	17
C.	The Proposed Rules Are Unnecessarily Burdensome and Unworkable.....	20
1.	Multiple Notifications to An Overbroad Universe of “Customers”	21
2.	Solicitations of Opt-In and Opt-Out Customer Consents	21
3.	Data Security Requirements	22
4.	Data Breach Requirements	23
IV.	THE PROPOSAL TO INVALIDATE ARBITRATION CLAUSES IS UNLAWFUL AND UNWISE.....	24
V.	CONCLUSION.....	25

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

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

COMMENTS OF ITTA

ITTA – The Voice of Mid-Size Communications Companies (“ITTA”) hereby submits its comments in response to the Commission’s *Notice of Proposed Rulemaking* in the above-captioned proceeding.¹

I. INTRODUCTION AND SUMMARY

In this NPRM, the Commission proposes to establish a comprehensive and intricate regime of rules, procedures and prohibitions to govern the collection, use and disclosure of customer information by providers of Broadband Internet Access Service (“BIAS”), as well as to police the security of such information and the provider’s obligations in the event of any breach of that security. In so doing, the NPRM would expand exponentially upon the existing “CPNI” rules that telecommunications carriers have operated under since 1998. The Commission asserts that such rules are necessary in the wake of its February 2015 *Open Internet Order*, which reclassified providers of BIAS (also referred to herein as “ISPs”) as common carriers subject to

¹ Notice of Proposed Rulemaking, WC Docket No. 16-106, FCC 16-39 (rel. Apr. 1, 2016) (“NPRM”).

Title II of the Communications Act, thereby subjecting them to the authority of the Commission and removing them from the jurisdiction of the Federal Trade Commission (“FTC”).²

The Commission’s proposals in this proceeding are well-intentioned but ill-considered: well-intentioned in that consumer choice in the use and dissemination of private information by their service providers is inarguably an important and worthy policy goal, but ill-considered in that the NPRM’s proposals exceed the Commission’s statutory authority, are overbroad, and would undermine and supersede the time-tested, balanced and demonstrably effective privacy protection regime created and enforced by the far more experienced FTC. Rather than fashioning rules that are technology-neutral and that resemble the ground rules that govern all other U.S. companies, including the FTC framework that effectively policed ISPs until last year, the NPRM ventures far afield of all existing federal or state privacy and data security regimes. In their place, the NPRM proposes entirely new and extremely complex and burdensome rules that encompass *any* bit of information that is “linked or linkable” to an individual. In doing so, these rules ignore consumer expectations, whether any harm is caused to consumers, whether the information is in any way sensitive, or even if it is truly “private.”

Moreover, while staking claim to such an all-encompassing swath of information, the NPRM does not consider its practical consequences on the providers who will have to comply, under shortened deadlines, or on consumers who will be bombarded with notifications, consent requests and “breach” notices for information that those consumers may regard as trivial and/or unintelligible. Most importantly, these proposals would not advance their stated goal of enhancing consumer choice and privacy, but rather would *limit* consumers’ choices, sow

² *Protecting and Promoting the Open Internet*, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601 (2015) (“*Open Internet Order*”),

confusion regarding the breadth of protection afforded to their private information, and ultimately increase consumers' cost of service and inhibit ISP investment and competition between ISPs and edge providers.

II. THE COMMISSION LACKS THE REQUISITE LEGAL AUTHORITY TO ADOPT THE PROPOSED RULES

The NPRM states flatly that it “relies on Section 222” of the Communications Act,³ and proclaims that it merely “propose[s] to apply the traditional privacy requirements of the Communications Act.”⁴ In the NPRM’s telling, the Commission is simply “securing what Congress has commanded”⁵ by “appl[ying] existing statutory authority” to implement the “detailed requirements that Congress requires be applied to the provision of telecommunications services.”⁶ In fact, the NPRM does the polar opposite of these things. Such authority is nowhere to be found in the Communications Act or its legislative history. This is particularly troubling given that “[a]gencies are creatures of Congress” and “an agency literally has no power to act ... unless and until Congress confers power upon it.”⁷

The NPRM concedes, as it must, that “earlier Commission decisions focused primarily on Section 222(c)’s protection of CPNI, and could be read to imply that CPNI is the only type of customer information protected,”⁸ before rationalizing that it “simply did not need to address the broader protections offered by Section 222(a)” in any of those many prior decisions.⁹ In addition

³ NPRM at ¶ 26. *See* 47 U.S.C. § 222.

⁴ *Id.* at ¶ 2.

⁵ *Id.*

⁶ *Id.* at ¶ 13.

⁷ *City of Arlington v. FCC*, 133 S. Ct. 1863, 1880 (2013) (quoting *Louisiana Pub. Serv. Comm'n v. FCC*, 476 U.S. 355, 374 (1986)).

⁸ NPRM at ¶ 298. *See also id.* at ¶ 56.

⁹ *Id.* at ¶ 298.

to this rationalization being false—the Commission *did* address that question and affirmatively decided that subsection 222(a) afforded no such “broader” protections¹⁰—the clear, unbroken line of agency precedent shows that the Commission disclaimed any such protections and instead consistently and repeatedly equated subsection 222(a)’s introductory reference to “proprietary information of . . . customers” with subsection 222(c)’s detailed elaboration of that term as CPNI. At least that was the case until a bare majority of Commissioners asserted in a non-final order (a Notice of Apparent Liability in an enforcement action) a newfound authority to regulate consumer privacy to a far greater degree than the Commission or its sister agency, the FTC, has ever found appropriate. The Commission’s invention of an entirely new and muscular legal obligation under subsection 222(a) of the Act simply cannot be squared with the plain language of that statutory provision, its history, and the Commission’s own consistent holdings.

A. Plain Language and Structure of Section 222 of the Act

The text of Section 222 is ordered in a logical and straightforward fashion. First, subsection 222(a) states: “IN GENERAL— Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunications carriers, equipment manufacturers, and customers, including telecommunications carriers reselling telecommunications services provided by a telecommunications carrier.”¹¹ Subsection 222(b) then elaborates on that duty by imposing specific restrictions on a carrier’s use of “proprietary information” obtained from another

¹⁰ See, e.g., *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14409, 14488 ¶ 147 (“1999 CPNI Reconsideration Order”) (“We are not persuaded that any portion of section 222 indicates that Congress intended such a result”). See *infra* notes 28-29 and accompanying text.

¹¹ 47 U.S.C. § 222(a) (emphasis in original).

carrier.¹² Subsection 222(c) proceeds in turn to describe in minute detail a carrier’s duties with respect to *Customer Proprietary Network Information* (“CPNI”) which, to eliminate doubt, it also terms “Privacy Requirements for Telecommunications Carriers,” imposing very specific restrictions and exceptions on a carrier’s use, disclosure or sharing of CPNI.¹³ Indeed, subsection 222(c) specifies in detail the limits on carriers’ handling of CPNI: among other things, it directs that upon a customer’s “affirmative written request,” a telecommunications carrier must disclose the customer’s CPNI to anyone designated by the customer,¹⁴ and that a carrier that receives CPNI in the course of providing telecommunications service may use, disclose or permit access to “aggregate customer information” (*i.e.*, information that does not disclose individual customers’ identities).¹⁵

Finally, subsections 222(d) through (h) delineate definitions, exceptions and clarifications regarding these provisions. Subsection 222(d) enumerates specific exceptions that allow certain uses of CPNI: “Nothing in this section prohibits a telecommunications carrier from using, disclosing, or permitting access to customer proprietary network information” for certain purposes, such as billing and collection, protecting the carrier’s property, or protecting users and other carriers against fraud or unlawful use.¹⁶ Most relevant here, in subsection 222(h), Congress specifically defined this *customer* proprietary network information over which it intended to convey authority to the Commission:

The term “customer proprietary network information” means—

¹² 47 U.S.C. § 222(b) (“A telecommunications carrier that receives or obtains proprietary information from another carrier for purposes of providing any telecommunications service shall use such information only for such purpose, and shall not use such information for its own marketing efforts.”).

¹³ *Id.* § 222(c)-(h).

¹⁴ *Id.* § 222(c)(2).

¹⁵ *Id.* § 222(c)(3).

¹⁶ 47 U.S.C. § 222(d).

(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and

(B) information contained in the bills pertaining to telephone exchange or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information.¹⁷

B. Legislative History of Section 222(a)

The NPRM asserts that “Section 222(a) should be understood to mean what it says.”¹⁸

ITTA agrees. The legislative history of Section 222 explicitly confirms that, insofar as subsection 222(a) addresses carriers’ duty to protect customer information, it means CPNI and only CPNI, not some additional or different category of information.

In fact, there was no subsection (a) setting forth a “general” obligation in either the House or the Senate version of the legislation that became the Telecommunications Act of 1996; both bills contained provisions addressing only CPNI and carrier-proprietary information. The Senate bill contained only a CPNI obligation that in fact was limited in its application to the Bell Operating Companies;¹⁹ the House bill similarly contained only a CPNI obligation.²⁰ Tellingly, while a “House amendment” *would* have empowered the FCC to create additional privacy rules, the House-Senate Conference *rejected* that provision. Instead, “[t]he conference agreement adopt[ed] the Senate provisions with modifications.”²¹

What then is the legislative pedigree of subsection 222(a), upon which the NPRM so strongly relies in propounding privacy obligations far more all-encompassing than CPNI? Simply this: it appears for the first time in the House-Senate Conference version of the bill, and

¹⁷ 47 U.S.C. § 222(h)(1).

¹⁸ NPRM at ¶ 299.

¹⁹ S. Rep. No. 104-23, 104th Cong., 1st Sess. (1995) at 23-24.

²⁰ H.R. Rep. No. 104-204, 104th Cong., 1st Sess. (1995) at 89-91 (1995).

²¹ H.R. Rep. No. 104-458, 104th Cong., 2d Sess. (1996) (Conference Report) at 203-205.

the solitary paragraph describing it states: “In general, the new section 222 strives to balance both competitive and consumer privacy interests with respect to CPNI.” and then simply recites the subsection.²²

Thus, the legislative history of Section 222 is unmistakably clear that the House-Senate Conference that forged the final legislation defined customer-proprietary information exclusively as CPNI, and the explicitly-labeled “general” subsection (a) merely introduces that obligation and the additional duties of carriers with respect to proprietary information of other carriers.

C. The Commission’s Consistent Interpretation of Section 222

Nearly twenty years of Commission precedent confirms that the customer information covered by Section 222(a) is limited to CPNI—at least until a bare majority of Commissioners approved an NAL in an enforcement proceeding that subsequently settled without leaving any precedential decision.

In its initial order implementing Section 222, the Commission—in fidelity to the explicit legislative history just quoted—referenced “the duty in section 222(a) upon all telecommunications carriers to protect the confidentiality of *customers’ CPNI.*”²³ The Commission comprehensively itemized the types of information Section 222 addresses—none of which included “customer proprietary information” that does not qualify as CPNI. Specifically, the Commission explained that “Sections 222(a) and (b) . . . establish obligations and restrictions in connection with carrier proprietary information” and that “Section 222 sets forth three categories of customer information to which different privacy protections and carrier obligations apply – individually identifiable CPNI, aggregate customer information, and subscriber list

²² *Id.* at 205 (emphasis added).

²³ See *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, Second Report & Order & Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061, 8203 ¶ 208 (emphasis added) (“1998 CPNI Order & FNPRM”).

information.”²⁴ The Commission did not find that Section 222 addresses any type of information other than those enumerated categories: carrier proprietary information, CPNI, aggregate information, and subscriber list information.

In the same Order, the Commission opened a Further Notice of Proposed Rulemaking (“FNPRM”) in which it sought comment on, among other things, “what, if any, further enforcement mechanisms . . . may be necessary to encourage appropriate carrier discharge of their duty under section 222(a) to protect the confidentiality of customer information.”²⁵ But in subsequent orders, the Commission repeatedly and expressly declined to either address this question or to adopt any rules whatsoever relating to Section 222(a).²⁶ It finally dropped the issue entirely in adopting a later FNPRM that focused only on carrier-proprietary information.²⁷ Throughout the ensuing decades, it continued to make clear Section 222(a)’s reference to “customers” meant CPNI. On reconsideration of the *1998 CPNI Order & FNPRM*, for example, the agency expressly denied a request that it “hold that section 222 controls all issues involving customer information, rather than *issues pertaining to CPNI*.”²⁸ In doing so, the Commission stated: “We are not persuaded that any portion of section 222 indicates that Congress intended such a result.”²⁹ And the Commission continued to reiterate its description of the categories of

²⁴ *Id.* at 8064 ¶ 2 & n.4.

²⁵ *Id.* at 8202 ¶ 207.

²⁶ *1999 CPNI Reconsideration Order*, 14 FCC Rcd 14409, 14412 n.1 (1999); *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, Clarification Order and Second Further Notice of Proposed Rulemaking, 16 FCC Rcd 16506 n.2 (2001).

²⁷ *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, Third Report & Order & Third Further Notice of Proposed Rulemaking, 17 FCC Rcd 14860, 14867 ¶¶ 14 & n. 6, 14923-24 ¶¶ 143-46 (2002) (“*2002 CPNI Order*”).

²⁸ *1999 CPNI Reconsideration Order*, 14 FCC Rcd at 14488 ¶ 147 (emphasis added).

²⁹ *Id.*

information governed by Section 222—notably excluding each time any mention of customer information that does not qualify as CPNI.³⁰

The import of these orders is unmistakable: “Every telecommunications carrier has a general duty pursuant to section 222(a) to protect the confidentiality of *CPNI*,” and “Congress accorded CPNI . . . the *greatest level of protection* under this framework.”³¹ To the extent customer information is concerned, CPNI is what Section 222(a) protects. Indeed, the Commission stated succinctly only three years ago that “if the [customer] information a carrier collects . . . does not meet the statutory definition [of CPNI], then section 222 *will not apply*.”³²

Given this mountain of plain statutory language, explicit legislative history and nearly two decades of Commission precedent, the NPRM’s novel and expansive interpretation of Section 222(a) is unsustainable. Indeed, as the NPRM admits,³³ the entirety of the Commission’s purported precedent for its new, contradictory interpretation consists of (1) an October 2014 NAL charging a wireless Lifeline service provider with liability for a data breach involving information that was not CPNI, which has no precedential effect because the case was settled;³⁴ (2) a cursory discussion in the 2015 *Open Internet Order* on which the instant NPRM

³⁰ 2002 *CPNI Order*, 17 FCC Rcd 14860, 14864 ¶ 6 (2002); *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, Report & Order & Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927, 6930 ¶ 4 n.7 (2007) (“2007 *CPNI Order*”).

³¹ 2007 *CPNI Order* at 6930-31 ¶¶ 4, 6 (emphases added). See also *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, Notice of Proposed Rulemaking, 21 FCC Rcd 1782, 1784 ¶ 4 (2006) (same); *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, Clarification Order & Second FNPRM, 16 FCC Rcd 16506, 16506-07 ¶ 1 (2001) (“Section 222 of the Communications Act . . . governs carrier use and disclosure of CPNI”).

³² *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, Declaratory Ruling, 28 FCC Rcd 9609, 9617 ¶ 24 (2013) (“2013 *Declaratory Ruling*”) (emphasis added).

³³ NPRM at ¶ 299.

³⁴ See *TerraCom, Inc. and YourTel America, Inc.*, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd

is based;³⁵ and (3) a passing reference in a June 2015 Lifeline order which has yet to be tested on appeal.³⁶ These spare revisionist statements cannot overcome the fact that Congress expressly stated, and the Commission until recently duly concurred, that “section 222 strives to balance both competitive and consumer privacy interests *with respect to CPNI*.”³⁷

In an effort to bolster its legal authority for the broad privacy rules now proposed, the NPRM adds that the Commission “believe[s] that we can also find support in other sections of the Communications Act,” including Sections 201 and 202, which prohibit telecommunications carriers from engaging in unjust, unreasonable, or unreasonably discriminatory practices; Section 706, which requires the Commission to remove barriers to infrastructure investment; and Section 705, which restricts the unauthorized publication or use of communications.³⁸ As Commissioner O’Rielly’s dissenting statement explains, however, this “shotgun approach”

13325 (2014) (*TerraCom NAL*); *Terracom, Inc., & Yourtel America, Inc.*, Order and Consent Decree, 30 FCC Rcd. 7075 (Enf. Bur. 2015) (specifying that the decree “shall not be used as evidence or precedent in any action . . . except an action to enforce this [decree],” 30 FCC Rcd at ¶ 20). In the *TerraCom NAL*, the only support for the Commission’s new interpretation of its authority under Section 222 was a single sentence in the *2007 CPNI Order* stating that “[w]e fully expect carriers to take every reasonable precaution to protect the confidentiality of proprietary or personal customer information.” *TerraCom NAL* ¶ 14 & nn.30, 33, quoting *2007 CPNI Order*, 22 FCC Rcd at 6959 ¶ 64). But the next two sentences of the *2007 CPNI Order* make clear the Commission was referring to CPNI, not some broader category of customer information: “Of course, we require carriers to implement the specific minimum requirements set forth in the Commission’s rules. We further expect carriers to take additional steps to protect the privacy of CPNI to the extent such additional measures are feasible for a particular carrier”) (emphasis added). *2007 CPNI Order* at ¶ 64. Further, the immediately preceding and following paragraphs likewise contain no fewer than seven explicit references to CPNI. See *id.* at 6959-60 ¶¶ 63, 65. In a footnote, the *NAL* also cited a sentence from the *2013 Declaratory Ruling* stating “subsection (a)’s obligation to protect customer information is not limited to CPNI that the carrier has obtained or received.” *NAL* at n.37, quoting *2013 Declaratory Ruling*, *supra* note 32, 28 FCC Rcd at 9618 ¶ 27. Again, as the context makes clear, the Commission was emphasizing that receipt of information that otherwise would be CPNI is not a prerequisite to protection under Section 222(a): “The fact that CPNI is on a device and has not yet been transmitted to the carrier’s own servers . . . does not remove the data from the definition of CPNI.” *Id.* That Commission statement thus confirms that Section 222(a) applies to CPNI only and not to customer information more broadly.

³⁵ *Open Internet Order*, 30 FCC Rcd 5601, ¶¶ 53, 462-67 & nn. 47-48, 1381, 1388, 1394, 1396 (2015), citing the *TerraCom NAL* and the aforementioned statements in the *2007 CPNI Order* and *2013 CPNI Declaratory Ruling*. See note 34 *supra*.

³⁶ *Lifeline and Link Up Reform and Modernization et al.*, Second Further Notice of Proposed Rulemaking, Order on Reconsideration, Second Report and Order, and Memorandum Opinion and Order, 30 FCC Rcd 7818, 7895-96 ¶ 234 (“2015 Lifeline Reform Order”).

³⁷ H.R. Rep. No. 104-458 at 205 (emphasis added). See *supra* notes 21-22 and accompanying text.

³⁸ NPRM at ¶ 294 (citations omitted).

cannot salvage the lack of authority for the Commission’s proposed action.³⁹ In any event, the NPRM states categorically that it “relies on section 222,”⁴⁰ and, with specific reference to the NPRM’s principal alternative sources of authority, the Commission has expressly “conclude[d] that the specific consumer privacy and consumer choice protections established in Section 222 supersede the general protections identified in sections 201(b) and 202(a).”⁴¹

The NPRM takes a revisionist, result-driven approach that runs afoul of cardinal rules of statutory interpretation and the Commission’s own long-held adherence to its governing law.⁴² Rather than attempting to rewrite the Communications Act, the Commission should remain faithful to the statute and Congress’ stated intent in crafting it, and recognize that its proposed interpretation is untenable.

III. THE PROPOSED RULES ARE OVERBROAD AND WOULD DISREGARD DECADES OF FTC EXPERTISE IN CONSUMER PRIVACY AND DATA PROTECTION

Aside from the demonstrated lack of legal authority for the rules proposed in the NPRM, the proposals are striking for their abrupt departure from virtually all consumer privacy-related rules and regimes that have governed the Internet ecosystem to date. The NPRM would subject ISPs who have been reclassified as Title II telecommunications carriers by the *Open Internet Order* to an enormously different privacy regime than the one that has been applied to them for many years by the FTC.

³⁹ *Id.*, Dissenting Statement of Commissioner O’Rielly at 2.

⁴⁰ *Id.* at ¶ 26.

⁴¹ *1999 CPNI Reconsideration Order*, *supra* note 10, 14 FCC Rcd 14409, 14491 ¶ 153 (1999).

⁴² *See Util. Air Regulatory Grp v. EPA*, 134 S. Ct. 2427, 2446 (2014).

Moreover, the BIAS – and possibly the other services under the rubric of “harmonization” that pervades the NPRM⁴³ – provided by traditional telecommunications, cable and satellite service providers, including ITTA members, would be subject to significantly expanded regulation by dint of the proposed melding of CPNI and “personally identifiable information” (“PII”) into a new category of “customer proprietary information” that sweeps in any information that is either “linked or linkable” to an individual.⁴⁴ That new definition would encompass massive swaths of customer (even past and prospective customer)⁴⁵ information, including information that is arguably not even “private,” much less “sensitive,” and would tremendously increase burdens on all providers and their customers.⁴⁶

Put simply, the NPRM does not answer the basic and logical question of why, given this Commission-imposed convergence, a privacy and data security regime modeled on the successful and universally respected FTC model applicable to all other participants in the Internet ecosystem is inadequate, and why telecommunications carriers must be subjected to such a different, more restrictive, difficult and costly privacy and security regime than their fellow stakeholders and competitors across that ecosystem.

⁴³ See NPRM at ¶¶ 24, 27, 54, 57, 59, 80, 103-05, 108, 113, 152-53, 166, 235, 254.

⁴⁴ *Id.* at ¶¶ 57, 61-66, App. A, proposed new 47 C.F.R §64.2003(o).

⁴⁵ *Id.* at ¶ 31.

⁴⁶ The NPRM lists as “illustrative, non-exhaustive” examples of covered information, in addition to all existing categories of CPNI: service plan information, including type of service (e.g., cable, fiber, or mobile), service tier (e.g., speed), pricing, and capacity (e.g., information pertaining to data caps); current or historical geo-location; media access control (“MAC”) addresses and other device identifiers; source and destination Internet Protocol (“IP”) addresses and domain name information; traffic statistics; name; Social Security number; date and place of birth; mother’s maiden name; unique government identification numbers (e.g., driver’s license, passport, taxpayer identification); physical address; email address or other online contact information; phone numbers; persistent online identifiers (e.g., unique cookies); eponymous and non-eponymous online identities; account numbers and other account information, including account login information; Internet browsing history; traffic statistics; application usage data; financial information (e.g., account numbers, credit or debit card numbers, credit history); shopping records; medical and health information; the fact of a disability and any additional information about a customer’s disability; biometric information; education information; employment information; information relating to family members; race; religion; sexual identity or orientation; other demographic information; and information identifying personally owned property (e.g., license plates, device serial numbers). See NPRM at ¶¶ 41, 62.

A. The Commission Should Adopt Privacy Rules Modeled Upon and Consistent With the FTC’s Time-Tested and Respected Regime

Early in the NPRM, the Commission notes that “as consumer use of the Internet exploded, the FTC, using its authority to prohibit ‘unfair or deceptive acts or practices in or affecting commerce,’ entered into a series of precedent-setting consent orders addressing privacy practices on the Internet.”⁴⁷ It observes with approval that “the FTC’s online privacy cases focus on the importance of transparency; honoring consumers’ expectations about the use of their personal information and the choices they have made about sharing that information; and the obligation of companies that collect personal information to adopt reasonable data security practices,” and goes on to hail that agency’s 2011 actions against Facebook and Google as prime examples of its activism in holding Internet companies accountable for their decisions to “collect personal information or to share personal information with advertisers or the public in violation of [their] publicly stated privacy policies [as] a deceptive act or practice. . . .”⁴⁸

This accurate depiction of the FTC’s consumer privacy policies, guidelines and enforcement regime under Section 5 of the FTC Act⁴⁹ closely matches the NPRM’s lodestars of “transparency, choice and security.”⁵⁰ Yet, although the NPRM repeatedly praises “the important leadership of the Federal Trade Commission” as being “critically important in this sphere,” and claims that it “looks to learnings from the FTC,”⁵¹ it proceeds to reject the FTC’s well-honed consumer privacy regime and the “learnings” of that agency’s more than 500

⁴⁷ NPRM at ¶ 8, *quoting* 15 U.S.C. § 45(a)(1).

⁴⁸ *Id.* (citations omitted).

⁴⁹ 15 U.S.C. § 45(a).

⁵⁰ *See, e.g.*, NPRM at ¶¶ 5, 9, 16-18.

⁵¹ *Id.* at ¶¶ 2, 4, 8, 9.

privacy-related enforcement actions⁵² in favor of its own, sector-specific, wholly asymmetric and vastly more complex and burdensome customer privacy rules. The NPRM merely asserts summarily that “the federal privacy regime” practiced by the FTC and other federal departments and agencies “does not now comprehensively apply the traditional principles of privacy protection to these 21st Century telecommunications services provided by broadband networks”⁵³ without ever saying *why* that is the case. In fact, most of the FTC’s prolific work product in this area has occurred in the past ten years of the new century. Unless there is a very good reason to depart so completely from the privacy framework that guides and is applied to virtually all other businesses in the nation, it stands to reason that this Commission should defer to the FTC’s experience and expertise in this area—or, at a minimum, adopt a similar, consistent approach. Among other important virtues, FCC rules for BIAS that are consistent with the FTC’s privacy framework would ensure that privacy enforcement is fair, technology-neutral and based on the type of data being collected and how it is used, rather than on the regulatory classification of the entity collecting the data.

The FTC has an unparalleled, 40-year history of consumer privacy enforcement, based on its authority under Section 5 of the FTC Act, to act against companies engaged in “unfair or deceptive practices” involving the privacy and security of consumers’ information.⁵⁴ It has brought over 500 enforcement actions protecting the privacy of consumer information, covering

⁵² See Prepared Statement of Federal Trade Commission on “Examining the Proposed FCC Privacy Rules” before the U.S. Senate Committee on the Judiciary, Subcommittee on Privacy, Technology & the Law (May 11, 2016) (“FTC 2016 Testimony”) at 3.

⁵³ NPRM at ¶ 2.

⁵⁴ See FTC 2014 Privacy and Data Security Update at 2, available at https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf (describing the FTC’s “unparalleled experience in consumer privacy enforcement”); see also FTC 2016 Testimony at 3-4.

both offline and online information, against providers and businesses large and small.⁵⁵ It has policed privacy practices in every corner of the Internet ecosystem, including social networks, search engines, ad networks, online retailers, mobile apps, mobile handsets, and—until the *Open Internet Order* ousted the FTC from its privacy enforcement role—ISPs. In these cases, the FTC has charged companies with making deceptive claims about how they collect, use, and share consumer data; failing to provide reasonable security for consumers’ personal information; deceptively tracking consumers online; and myriad other privacy and data-security-related violations.⁵⁶ Moreover, the FTC has amassed expertise in and protected Internet privacy for twenty years, holding its first workshop on the subject in June 1996.⁵⁷ These workshops have continued ever since, including a November 2015 workshop on “cross-device tracking.”⁵⁸

The FTC’s policies and enforcement actions have always been technology-neutral, with a focus on whether a company’s privacy or data security practices cause or are likely to cause substantial harm to consumers that is neither reasonably avoidable by consumers nor outweighed by countervailing benefits to consumers or to competition.⁵⁹ If those practices do not meet the standard, they can be found to be in violation of Section 5. Similarly, if a business makes misleading statements or omissions about its privacy or data security features, and such statements or omissions are likely to mislead reasonable consumers, such statements or

⁵⁵ FTC 2016 Testimony at 3.

⁵⁶ See FTC 2014 Privacy and Data Security Update at 2 (“The FTC has brought enforcement actions addressing a wide range of privacy issues, including spam, social networking, behavioral advertising, pretexting, spyware, peer-to-peer file sharing, and mobile.”); FTC 2016 Testimony at 3.

⁵⁷ FTC 2016 Testimony at 5.

⁵⁸ *Id.* at 7 & n.20.

⁵⁹ See 15 U.S.C. § 45(n) (2011) (codifying the FTC Act Amendments of 1994, Pub. L. No. 103-312, § 9, 108 Stat. 1691, 1695 (1994)); FTC Policy Statement on Unfairness (Dec. 17, 1980).

omissions can be found to be deceptive in violation of the Act. The FTC framework also focuses on the sensitivity of the type of data collected and how the data is used.⁶⁰

In stark contrast to the FTC’s experience and expertise in this area, the Commission and its Enforcement Bureau never exercised authority or brought a single action regarding customer privacy or data security that did not involve CPNI until twenty months ago.⁶¹ Yet the NPRM inexplicably seeks to ignore the FTC’s real-world experience and implement a novel, sector-specific, and extremely far-reaching privacy and data security regime—extending to every imaginable bit of customer information that is arguably “linked or linkable” to an individual. The NPRM proposes untried but intricate and onerous requirements for privacy notifications and disclosures, opt-in and opt-out customer consents, customer authentication, risk assessments, training, record retention, contract provisions, de-identification of aggregated information, and myriad other matters. And the Commission would impose all of these rules and restrictions only on ISPs (including traditional telecom and cable providers who offer BIAS), while leaving all edge providers and others who collect, use and monetize infinitely more customer information in the Internet ecosystem untouched.⁶²

In the interest of fostering an effective, technology and competitor-neutral broadband privacy framework, on March 1, 2016 five associations of wireline and mobile carriers and ISPs submitted for the Commission’s consideration a joint proposal setting forth detailed guidelines and principles for a privacy framework based on the FTC model and incorporating the

⁶⁰ *Id.*

⁶¹ See discussion at pp. 9-10 *supra*.

⁶² See NPRM at ¶ 4; Statement of Chairman Wheeler at 2 (“To be clear, this is not regulating what we often refer to as the edge – meaning the online applications and services that you access over the Internet, like Twitter and Uber. It is narrowly focused on the personal information collected by broadband providers as a function of providing you with broadband connectivity, not the privacy practices of the websites and other online services that you choose to visit.”) See also discussion *infra* at pp. 17-20.

Commission’s stated principles of transparency, choice and security.⁶³ In just three paragraphs—and without comment—the NPRM briefly summarized this “Industry Framework,” but otherwise disregarded it.⁶⁴ ITTA submits that the Commission should carefully consider the Industry Framework, and in any event adopt rules, policies and enforcement practices for BIAS that are technology and competitor-neutral and modeled after the FTC’s well-tested and successful privacy and data security regime.

B. The Commission Should Not Adopt Rules That Disproportionately Disadvantage ISPs Vis-à-Vis Edge Providers

As in other pending proceedings,⁶⁵ the Commission in this NPRM proposes sector-specific regulation of ISPs and other telecommunications carriers but eschews any equivalent scrutiny of edge providers, which have far greater access to exponentially greater quantities and varieties of consumer information than ISPs. In so doing, the NPRM simply asserts without support that “ISPs are the most important and extensive conduits of consumer information,”⁶⁶ and states dismissively: “To those who say that broadband providers and edge providers must be treated the same, this NPRM proposes rules that recognize that broadband networks are not, in fact, the same as edge providers in all relevant respects.” It then adds: “But this NPRM looks to learnings from the FTC and other privacy regimes to provide complementary guidance.”⁶⁷

In fact, the FTC has issued guidance on the subject of the virtual equivalence of ISPs and edge providers with regard to access to private customer information. In its landmark 2012

⁶³ Letter from American Cable Ass’n, Competitive Carriers Ass’n, CTIA, NCTA and USTelecom to Chairman Wheeler (Mar. 1, 2016).

⁶⁴ NPRM at ¶¶ 280-282.

⁶⁵ See, e.g., *Expanding Consumers’ Video Navigation Choices; Commercial Availability of Navigation Devices*, Notice of Proposed Rulemaking and Memorandum Opinion and Order, MB Docket No. 16-42, CS Docket No. 97-80, 31 FCC Rcd 1544 (2016).

⁶⁶ NPRM at ¶ 2.

⁶⁷ *Id.* at ¶ 4.

Privacy Report, “Protecting Consumer Privacy in an Era of Rapid Change,” a product of six years of workshops and hearings and over 450 comments from consumer and industry interests, technology and policy experts and the public, the FTC concluded: “Any privacy framework should be technologically 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. Like ISPs, operating systems and browsers may be in a position to track all, or virtually all, of a consumer’s online activity to create highly detailed profiles.*”⁶⁸

As the Commission is aware, the major change that has occurred since 2012 is the precipitous increase in encryption, which has significantly decreased the online customer information that is viewable by ISPs, while leaving edge providers in full command of the panoply of this information. As President Clinton’s Chief Counselor for Privacy and President Obama’s special assistant for economic policy, Professor Peter Swire, found in an exhaustive recent study, more than 50% of Internet traffic is now encrypted, and it is estimated that 70% of such traffic will be encrypted by the end of this year.⁶⁹ Because ISPs cannot “read” encrypted communications, they have no access to that information, while the edge providers and websites that consumers visit do have such access. Moreover, an ISP is hardly the “bottleneck” conduit provider to customers that the NPRM imagines. Today, “the average Internet user has 6.1 connected devices, many of which are mobile and connect from diverse and changing locations

⁶⁸ FTC Report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers* (Mar. 2012) (emphasis added), available at <https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers>.

⁶⁹ Peter Swire, *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others* at 3 (Feb. 29, 2016), available at <http://b.gatech.edu/1RIWXUa>

that are served by multiple ISPs. . . . Any one ISP today is therefore the conduit for only a fraction of a typical user’s online activity.”⁷⁰

At the same time, edge providers have much broader access to more and more diverse consumer data across multiple platforms, including social networks, search engines, webmail and messaging, operating systems, mobile apps, interest-based advertising, browsers, Internet video, and e-commerce. Non-ISPs similarly dominate in cross-context and cross-device tracking. As Professor Swire concludes:

Based on a factual analysis of today’s Internet ecosystem in the United States, ISPs have neither comprehensive nor unique access to information about users’ online activity. Rather, the most commercially valuable information about online users, which can be used for targeted advertising and other purposes, is coming from other contexts. Market leaders are combining these contexts for insight into a wide range of activity on each device and across devices.⁷¹

The competitive harm that the NPRM’s proposals could wreak on ISPs vis-à-vis edge providers is starkly set forth in a recent Moody’s Investors Service warning, which predicted that adoption of the regime proposed in the NPRM could significantly harm ISPs’ debt ratings, affecting more than half a trillion dollars of rated debt. Moody’s analysis showed that, under the proposed rules, ISPs “would be severely handicapped in competing with digital advertisers like Facebook and Google, who are able to collect the same type of information from consumers who use their websites . . . 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

⁷⁰ *Id.* at 7.

⁷¹ *Id.* at 8.

advertising dollars will continue to move in secular fashion from traditional television providers towards digital platform providers.”⁷²

Among many other disadvantages, the Commission’s proposal would make difficult-to-obtain affirmative “opt-in” consent the *de facto* “default” requirement for many uses of customer information, including for the marketing of an ISP’s own products and services. Under the NPRM, a broadband provider would not be able to market its own non-communication-related products, including such common offerings as home security systems, to its customers without prior opt-in consent, regardless of the marketing channel used. It would also require opt-in consent prior to sharing information with the ISP’s affiliates; and it would require opt-in consent for all forms of online tracking, without regard to the sensitivity of the data used in tailoring online advertising, in contrast to the FTC’s framework, which calls only for opt-out consent in almost all cases. In sum, the NPRM’s overbroad opt-in approach would certainly stifle competition in the online advertising marketplace, to the needless detriment of all BIAS providers.

C. The Proposed Rules Are Unnecessarily Burdensome and Unworkable

As Commissioner Rosenworcel observed in her separate statement, the NPRM poses over 500 questions.⁷³ This is unsurprising in a set of proposals that would impose a massive array of new requirements on BIAS providers, but no other American companies. The following sections

⁷² Moody’s Investor Service, Sector Comment: “FCC’s broadband privacy proposal credit negative for linear TV and wireless providers”, March 14, 2016, *available at* https://www.moody.com/MdcAccessDeniedCh.aspx?lang=en&cy=global&Source=https%3a%2f%2fwww.moody.com%2fviewresearchdoc.aspx%3fdocid%3dPBC_1019671%26lang%3den%26cy%3dglobal; “Proposed Privacy Rules Threat to ISP Debt Ratings, Moody’s Warns,” Communications Daily, Mar. 16, 2015, p.1.

⁷³ NPRM, Statement of Commissioner Rosenworcel at 1.

describe just a few examples of the overbroad and burdensome new requirements that this NPRM would impose.

1. Multiple Notifications to An Overbroad Universe of “Customers”

The NPRM would impose a new requirement⁷⁴ that very detailed⁷⁵ privacy notices be provided to all “prospective customers at the point of sale, prior to the purchase of BIAS, whether such purchase is being made in person, online, over the telephone, or via some other means,”⁷⁶ then be made “persistently available” online and by other means,⁷⁷ and that equally detailed notices of any material changes to privacy policies be communicated by email to all customers, on customer bills, and online.⁷⁸ In addition to the difficulty of determining in real time who is a “prospective” customer for purposes of this rule, the requirement to provide a privacy policy at the “point of sale” to each such prospect, including during telephone marketing, would make the marketing and sign-up process significantly more difficult, and require new employee training. The requirement becomes even more problematic when this proposed rule is read in concert with the NPRM’s definition of “customer,” which includes “a current or former, paying or non-paying, subscriber” as well as any “applicant.”⁷⁹

2. Solicitations of Opt-In and Opt-Out Customer Consents

While the NPRM says that it is “cognizant of the risk of information-overload if consumers are given more information than they need to make an informed decision,”⁸⁰ the

⁷⁴ The NPRM acknowledges that “current Section 222 rules do not require voice providers to have privacy notices.” *Id.* at ¶ 86.

⁷⁵ *Id.* at ¶ 83.

⁷⁶ *Id.*

⁷⁷ *Id.*

⁷⁸ *Id.* at ¶ 96.

⁷⁹ *Id.* at ¶ 31.

⁸⁰ *Id.*

Commission proposes to require BIAS providers to solicit post-sale customer approval when the provider first intends to use, disclose or permit access to customer information. The BIAS provider must notify its customers of the type of information it is seeking approval to use, disclose or permit access to, the purposes for which the information will be used, and the entity or types of entities with which the information will be shared.⁸¹ This proposed requirement makes it inevitable that such overload will occur regularly. Yet more troublesome is that such consent must be solicited before any use of “linked or linkable” customer information⁸²—an astonishingly broad category that makes no distinction among non-sensitive, less sensitive and more sensitive information, or even between information that is truly “private” versus information that is not. Even the NPRM’s exhaustive list of examples is non-inclusive,⁸³ so the predictable result is that, out of caution, BIAS providers will feel compelled to solicit consent prior to any use of almost every kind of customer information. This extremely burdensome and repetitive requirement would create absurd results that would not occur if the Commission instead adopted rules modeled on the FTC framework, which does consider all of these distinctions.⁸⁴

3. Data Security Requirements

Next, the NPRM proposes “robust and flexible data security requirements for BIAS providers,” including “specific types of practices they must engage in to comply with the overarching requirement.” There follow 65 paragraphs of rule proposals and questions. Among many other concerns, the NPRM’s discussion does not consider a business customer exception to

⁸¹ *Id.* at ¶ 140.

⁸² *Id.* at ¶ 57. *See* discussion *supra* at p. 12.

⁸³ *See* note 46 *supra* and accompanying text.

⁸⁴ *See* 2012 FTC Privacy Report, *supra* note 68.

the proposed customer authentication requirements, as the current CPNI rules provide,⁸⁵ and it makes clear that providers will be held accountable for privacy violations of third parties, implying a strict liability standard.⁸⁶ Again, the NPRM’s proposals suffer from overbreadth and a one-size-fits-all approach that is totally at odds with the policies and distinctions that are applied to all non-telecommunications entities under the FTC’s privacy framework.

4. Data Breach Requirements

The NPRM’s data breach rules and notification requirements⁸⁷ suffer from multiple flaws. Among others, the proposed definition of PII as any information that is “linked or linkable” to an individual is likely to create a huge increase in the number of possible “breaches” that will create obligations for reporting to law enforcement and customer notifications, whether or not the information is sensitive or whether the “breach” causes any harm to customers or even leaves the confines of the company. Further, the proposed definition of “data breach” itself (“any instance in which a person, without authorization or exceeding authorization, has gained access to, used, or disclosed customer proprietary information”)⁸⁸ expands tremendously the definition currently used in the CPNI rules, by simply omitting one word used in the CPNI rule definition: “intentionally.”⁸⁹ Removing the concept of intent is totally unjustified, and will greatly expand the number of scenarios in which such a “breach” occurs and requires disclosure and customer notification. Moreover, in another example of overbreadth and overregulation, the NPRM inexplicably decreases the time frame for customer notifications—which must be

⁸⁵ 47 C.F.R § 64.2010(g).

⁸⁶ See NPRM at ¶ 211.

⁸⁷ *Id.* at ¶¶ 233-255.

⁸⁸ See *id.* at ¶ 75; App. A, proposed 47 C.F.R § 64.2003(d).

⁸⁹ See 47 C.F.R § 64.2011(e).

preceded by discovery, investigation and disclosure to law enforcement and states—from the 14 or more days after the event provided in the current CPNI rules to ten days, again without justification.⁹⁰ Accordingly, the proposed rules will expand exponentially the number of events that will qualify as breaches while simultaneously according providers much less time to notify customers about them.

IV. THE PROPOSAL TO INVALIDATE ARBITRATION CLAUSES IS UNLAWFUL AND UNWISE

Straying even further into uncharted territory, the NPRM proposes to invalidate certain arbitration clauses in subscription agreements between broadband providers and their customers.⁹¹ If adopted, this proposal would exceed the FCC’s authority, undermine the policies of the Federal Arbitration Act, and arbitrarily preclude a cost-effective and efficient means of dispute resolution without any basis in the record for such restrictive measures.

The NPRM is ambiguous as to the potential scope of the contemplated preclusion of arbitration agreements. The NPRM “seek[s] comment on whether to prohibit BIAS providers from compelling arbitration in their contracts,”⁹² but it is unclear whether by this the FCC intends to include standard-form arbitration clauses to which broadband subscribers have agreed. Nor is it clear whether the contemplated prohibition would extend to the preclusion of arbitration as to claims that do not arise under the Communications Act (e.g., claims alleging violations of state consumer protection laws). To the extent that the FCC is contemplating this broader preclusion, it has not articulated—nor could it articulate—any jurisdictional basis for precluding the arbitration of claims that do not arise under the Communications Act itself.

⁹⁰ NPRM at ¶¶ 236-240.

⁹¹ *Id.* at ¶ 274.

⁹² *See id.*

In any event, prohibiting arbitration clauses runs counter to the strong federal policy in favor of arbitration agreements under the Federal Arbitration Act. As the Supreme Court has explained, that statute “‘embod[ies] [a] national policy favoring arbitration,’”⁹³ and “‘arbitration is a matter of contract.’”⁹⁴ The FCC has neither the authority to undermine that federal policy nor the expertise to substitute its judgment for that of Congress.

The FCC’s proposal to further insert itself into uncharted territory by precluding certain agreed-upon arbitration clauses is particularly unwise because there is no record that the costs of arbitration clauses outweigh the benefits, such that any prohibition of arbitration clauses on this record would be arbitrary and capricious. If anything, a large body of evidence shows the considerable benefits of arbitration, which is generally more cost effective and efficient than dispute resolution in other forums, including courts.⁹⁵

V. CONCLUSION

In light of the serious issues regarding the Commission’s lack of legal authority to adopt the proposed rules, the starkly un-level playing field that these rules would create, and the real prospect for harm to innovation, investment and competition in the information ecosystem, the Commission should not adopt the proposed rules, but instead craft fair, focused and technology-neutral rules and policies that are consistent with the longstanding FTC privacy policies and

⁹³ *AT&T Mobility LLC v. Concepcion*, 563 U.S. 333, 346 (2011) (citation omitted).

⁹⁴ *Am. Exp. Co. v. Italian Colors Rest.*, 133 S. Ct. 2304, 2309 (2013).

⁹⁵ *See, e.g.*, Comments of the American Bankers Association, the Consumer Bankers Association, and the Financial Services Roundtable on Request for Information Regarding Scope, Methods and Data Sources for Conducting Study of Pre-Dispute Arbitration Agreements (Docket No. FCPB-2012-0017) (filed June 22, 2012) at 6-11; Comments of Consumer Credit Industry Association on Request for Information Regarding Scope, Methods and Data Sources for Conducting Study of Pre-Dispute Arbitration Agreements (Docket No. FCPB-2012-0017) (filed June 22, 2012) at 2-4 (citing various studies).

framework that have been successfully applied to all other American businesses.

Respectfully submitted,

James M. Smith
Peter Karanjia
DAVIS WRIGHT TREMAINE LLP
1919 Pennsylvania Avenue, NW, Suite 800
Washington, DC 20006
(202) 973-4288
jamesmsmith@dwt.com
Its Attorneys

/s/ Genevieve Morelli

President
ITTA
1101 Vermont Ave., NW, Suite 501
Washington, DC 20005
(202) 898-1519
gmorelli@itta.us

May 27, 2016