Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

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

JOINT PETITION FOR STAY

Ross J. Lieberman
Senior Vice President, Government Affairs
American Cable Association
2415 39th Place, N.W.
Washington, D.C. 20007

Rick Chessen
Senior Vice President, Law & Regulatory Policy
NCTA - The Internet & Television Association
25 Massachusetts Avenue, NW, Suite 100
Washington, DC 20001

Rebecca Murphy Thompson
EVP & General Counsel
Competitive Carriers Association
805 15th Street NW, Suite 401
Washington, DC 20005

Joshua Seidemann
Vice President, Policy
NTCA – The Rural Broadband Association
4121 Wilson Boulevard, Suite 100
Arlington, VA 22203

Tom Power
Senior Vice President & General Counsel
CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036

Jonathan Banks
Senior President – Law & Policy
United States Telecom Association
14th Street, NW, Suite 400
Washington, DC 20005

Michael J. Jacobs
Vice President, Regulatory Affairs
ITTA – The Voice of Mid-Sized Communications Companies
1101 Vermont Avenue, NW, Suite 501
Washington, DC 20005

Stephen E. Coran
Wireless Internet Service Providers Association
4417 13th Street, #317
St. Cloud, FL 34769

Derrick Owens
Vice President of Government Affairs
WTA – Advocates for Rural Broadband
400 7th Street, NW, Suite 406
Washington, DC 20004

January 27, 2017

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

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

To: The Commission

JOINT PETITION FOR STAY

The American Cable Association (ACA), the Competitive Carriers Association (CCA), CTIA, ITTA – The Voice of Mid-Sized Communications Companies (ITTA), NCTA – The Internet & Television Association (NCTA), NTCA – The Rural Broadband Association, the United States Telecom Association (USTelecom), the Wireless Internet Service Providers Association (WISPA), and WTA – Advocates for Rural Broadband (together "Petitioners"), pursuant to Sections 1.41, 1.43, and 1.44(e) of the Commission's rules, respectfully request that the Commission stay the rules adopted on October 27, 2016 in the above-captioned proceeding,[1/]

[1/] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Report and Order, FCC 16-148 (rel. Nov. 2, 2016) ("*Order*"). A summary of the *Order* and rules adopted therein was published in the Federal Register on December 2, 2016. *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, 81 Fed. Reg. 87,274 (Dec. 2, 2016) (amending 47 C.F.R. § 64.2001 et seq.).

pending resolution of their respective Petitions for Reconsideration of the *Order*,[2/] as well as the Petitions for Reconsideration filed by several other parties.[3/]

INTRODUCTION AND SUMMARY

Eleven parties filed petitions for reconsideration of the Commission's privacy, data breach, and data security rules for broadband Internet access service (BIAS) providers. These petitions raise significant questions about the legal basis for the rules and their potentially deleterious impact on consumers, competition, and innovation. Notably, several petitions were filed on behalf of companies not even directly subject to the rules but that are nonetheless impacted by them due to the adverse effects of the rules on the digital economy,[4/] thereby highlighting the potential for tangible harm to the public from moving forward with the rules. Other petitions were filed by associations representing small broadband providers that face disproportionate burdens arising from the rules adopted in the *Order*.

Broadband consumers should receive consistent and uniform protection of the privacy of their personal information from all entities in the online ecosystem that come into contact with such data as it transits the Internet. As the Commission itself has recognized, the "importance of privacy protection is certainly not new to the nation's largest broadband providers, all of which have publicly available privacy policies, describing their use and sharing of confidential

---

2/ The following Petitioners submitted Petitions for Reconsideration in WC Docket No. 16-106 on January 3, 2017: NCTA ("NCTA Petition"); CTIA ("CTIA Petition"); United States Telecommunications Association ("USTelecom Petition"); WISPA ("WISPA Petition"); Competitive Carriers Association ("CCA Petition"); ITTA ("ITTA Petition"); American Cable Association ("ACA Petition"). Consistent with the positions set forth in NCTA and CTIA's Petitions for Reconsideration, while Petitioners seek a stay of the rules as they apply to BIAS customer data, they do not object to the rules to the extent they replace and update the existing CPNI rules applicable to voice telephony service. *See* NCTA Petition at n.5; CTIA Petition at 2.

3/ *See* Petitions for Reconsideration filed in WC Docket No. 16-106 by Association of National Advertisers, et al. ("ANA Petition"); Consumer Technology Association ("CTA Petition"); Level 3 Communications, LLC ("Level 3 Petition"); and Oracle Corporation ("Oracle Petition").

4/ *See, e.g.*, ANA Petition; Oracle Petition; CTA Petition.

customer information."[5/] Petitioners' member companies have considerable experience in safeguarding broadband service information and strong business incentives to secure and strengthen the trust of the customers with whom they share an ongoing business relationship by serving as responsible stewards of their personal information. Indeed, Internet Service Providers (ISPs) have released a voluntary set of privacy and data security principles that are predicated upon the core tenets of transparency, consumer choice, and security that undergird the Federal Trade Commission's (FTC) well-known and highly successful privacy framework.[6/]

As set forth more fully in the Petitions for Reconsideration filed by Petitioners, which are incorporated by reference herein, the rules imposed in the *Order* governing ISP use and sharing of BIAS customer data are unsound as a matter of both law and policy. Petitioners seek a stay in order to undo the *Order's* dramatic departures from the FTC's privacy framework, which effectively balances the twin objectives of providing consumers control over their personal information while preserving opportunities for beneficial uses of data that lead to innovation, new products and capabilities, customized services, and growth in the digital economy. Staying the *Order* would allow the Commission to consider the Petitions for Reconsideration without causing significant disruption to businesses and creating confusion for consumers. The Petitions aim to restore the proven and effective approach of protecting consumers' privacy rights through the consistent and uniform application of a single set of privacy obligations applicable across the Internet to all companies that come into contact with broadband consumer data.

As detailed below, Petitioners satisfy the applicable standard for grant of a stay.

5/ *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services,* Notice of Proposed Rulemaking, WC Docket No. 16-106, FCC 16-39, ¶ 10 (rel. April 1, 2016).

6/ *See* "ISP Privacy Commitments" (attached as Appendix A).

Petitioners Are Likely to Succeed on the Merits. The *Order* contravenes Section 222 of the Communications Act and violates the First Amendment. Congress did not empower the Commission to adopt the rules in question. To the contrary, Section 222 addresses only access to, and use and disclosure of, certain information pertaining to the provision of voice telephony service. Further, Congress did not authorize regulation of information that does not fall within the definition of customer proprietary network information (CPNI), such as broadband customer personally identifiable information (PII). The tortured constructions of Section 222(a) employed to reach a contrary result underscores the rupture between the *Order* and the language and structure of the statute. The constraints on ISP use and sharing of IP addresses, MAC IDs, and other device identifiers established in the *Order*, as well as the regulation of broadband customer content information, are likewise beyond the scope of the Commission's authority under Section 222. The rules also infringe on the protected speech of ISPs in a manner that cannot pass muster under the First Amendment.

Apart from its statutory and constitutional defects, the *Order* is also arbitrary and capricious in several key respects. First, disregarding voluminous evidence in the proceeding, the *Order* erroneously and irrationally concludes that ISPs have unique and pervasive visibility into broadband customer information relative to other Internet entities that come into contact with the same data, and wield undue leverage over such information by occupying a putative gatekeeper role.[7/] Both of these conclusions are contrary to the record and undergird the *Order's* core policy infirmity: the imposition of significantly more costly and onerous restrictions on ISP use of online consumer data than all other online entities.

[7/] Further, these erroneous conclusions cannot be reconciled with the Commission's statement elsewhere in the *Order* that smaller ISPs collect and use far less customer data. *See Order*, ¶ 268.

Second, the *Order* unjustifiably departs from key elements of the long-standing and effective privacy framework developed by the FTC. It imposes an opt-in consent obligation solely upon ISP use of Web browsing and app usage data, under the faulty assumption that such data is uniformly "sensitive" when accessed by ISPs. The *Order* also overrides consumer expectations and common industry practice – as well as established findings and conclusions of the FTC and the previous Administration – by subjecting most ISP first-party marketing to either opt-out or opt-in consent, instead of implied consent. The *Order* thus establishes inconsistent privacy standards that will confuse consumers and violate key principles of fair competition. The rules enshrine this asymmetric treatment into law without any showing that consumers would be harmed by the uniform application of the FTC's privacy framework to ISPs and non-ISPs alike with respect to the use of Web browsing/app usage data and first-party marketing.

Third, the *Order* fails to undertake any analysis of whether the economic and consumer welfare costs of the rules' constraints on beneficial uses of data outweigh the benefits, if any, associated with such restrictions. The disparate treatment of Web browsing/app usage data and first-party marketing will interfere with the ability of consumers to receive customized services and capabilities they enjoy and information about new products and discount offers. It also will hinder the ability of ISPs to innovate by developing and furnishing new customized offerings and to provide much-needed competition in the highly concentrated online advertising market. These costs to consumers and competition will be incurred with little, if any, corresponding benefit to consumer privacy, since the same broadband consumer data that ISPs will be constrained from using will continue to be used by all other Internet ecosystem entities subject to the FTC's more flexible regulatory approach. Further, the Commission ignored its responsibilities under the Regulatory Flexibility Act (RFA), which includes a duty to describe

and assess the significant economic impact the Commission's proposals might have on small entities. Indeed, the record reflects that small BIAS providers with limited resources, most of which do not monetize consumer data, will struggle to shoulder the costs imposed by the *Order*. Therefore, on multiple counts, the *Order* ignores the Commission's responsibility to rigorously assess whether the benefits of its rules are worth its substantial costs.

Fourth, the *Order* subjects such a broad swath of non-sensitive data to its data breach and data security requirements that the implementation of these requirements will be costly, burdensome, and unworkable due to the ready availability of such data to countless entities in the Internet ecosystem. The defects of the data breach rules are compounded by the *Order's* vague definition of harm and its decision to peg the short timetable for notifying law enforcement and the Commission to the date of breach determination – rather than the date of determination of harm – which will lead to over-notification of putative data breaches that do not actually cause consumer injury, creating customer confusion and potential unwarranted distrust of ISPs.

Absent a Stay, Petitioners Will Suffer Irreparable Harm. Petitioners' member companies will suffer immediate and irreparable harm in the absence of a stay of the broadband privacy rules. As an initial matter, the rules adopted by the Commission contravene the First Amendment rights of ISPs, and constitutional harms are sufficient on their own to meet the harm threshold for a stay. Moreover, to come into compliance with the rules by their various upcoming effective dates, ISPs must take costly and time consuming technical, operational, and administrative steps now. Those steps include making changes to hardware and software assets and configurations across their networks to account for new choice mechanisms, constraints on data use and sharing, and data breach notification and data security requirements. They also include (1) the development of new internal privacy business rules that must be reflected in

operating manuals, organized into training programs, and taught to thousands of employees and vendor personnel; and (2) the creation of new notices to consumers about those new privacy practices and the consumers' data rights under the law, and procedures for the collection and administration of new customer consents that must be in place before the rules go into effect. These administrative and compliance burdens are particularly onerous for small providers serving unserved and underserved communities that cannot readily absorb the costs and must pass them through to their customers in order to stay in business.

Requiring ISPs alone make changes to their privacy policies for data subject to the Commission's asymmetrical privacy rules is inherently confusing for customers, and will lead to a loss of goodwill, particularly since (1) many other companies using the same data will continue to be subject to the FTC's privacy framework, and (2) such company policy changes are likely to change again if the FCC modifies or eliminates the new rules on reconsideration. In short, the harms caused by subjecting ISPs to the substantial costs and burdens of operationalizing rules that are unlikely to be retained in their current form are unnecessary, counterproductive, and irreparable. Petitioners' member companies will also suffer competitive harms as they are forced to forgo potential business opportunities to their non-ISP competitors, due to the disparate restrictions on the use of the same customer data and the likelihood of notice fatigue and customer alienation engendered by the defects in the data breach rules.

A Stay Will Not Injure Other Parties and Will Further the Public Interest. Grant of a stay will not harm any other party.[8/] Instead, it will maintain a status quo that has been in place

[8/] The FCC should not reverse its decision to streamline its existing voice CPNI rules by eliminating the outdated recordkeeping and annual certification requirements. Telecommunications carriers and interconnected VoIP providers are operating in reliance on the FCC's recent Public Notice confirming that these requirements are no longer in effect. Public Notice, *Wireline Competition Bureau Announces Effective Dates of Broadband Privacy Rules*, DA 16-1387 (rel. Dec. 14, 2016) (noting that the *Order* "relieved telecommunications carriers and interconnected VoIP providers of the specific compliance recordkeeping and annual certification requirements in

for nearly two years since the Commission adopted the *Open Internet Order* and reclassified BIAS as a telecommunications service, thereby removing ISPs from the purview of the FTC privacy and data security framework. During that time period, ISPs continued to honor their commitments to consumers set out in their privacy policies, and to provide appropriate choices to consumers concerning the use of their information. If a stay is granted, consumers will remain subject to those protections, as ISPs will continue to adhere to privacy policies predicated upon the FTC's core principles of transparency, choice, and security. Further, the voluntary privacy and data security principles that ISPs have pledged to follow will provide consumers with additional safeguards should the Commission's broadband privacy rules be stayed.[9/] In addition, the guidance previously provided by the Commission to deter bad faith and unreasonable privacy practices can, if necessary, remain in effect pending a resolution of the merits of the reconsideration petitions.[10/] Thus, while ISPs have not been subject to specific implementing rules for nearly two years now, they have complied with the Commission's interim guidance, other applicable federal and state privacy, data security, and breach notification laws, and their own privacy policies, with scant evidence of harm to consumers.

The public interest also favors a stay. Preserving the status quo pending further examination of whether to uphold the *Order's* repudiation of key components of the FTC's successful privacy framework would benefit consumers, competition, innovation, and the digital economy – and thus furthers the public interest. There are no public benefits from compelling ISPs to incur substantial costs and burdens to implement rules tainted with the legal and policy

existing section 64.2009, specifically subsections (c) and (e)" and that after January 3, 2017 these provisions would no longer be operative).

9/ *See* Appendix A.

10/ Public Notice, *Enforcement Bureau Guidance: Broadband Providers Should Take Reasonable, Good Faith Steps To Protect Consumer Privacy*, DA 15-603 (rel. May 20, 2015).

defects identified by Petitioners in their Reconsideration Petitions. Further, the prospect of the Commission revisiting Title II reclassification also militates in favor of a stay,[11/] because the relief requested here would permit the Commission to defer the operative effect of the broadband privacy rules until the issue of the appropriate regulatory classification of broadband service is definitively resolved. As with the relief requested in the instant stay request, revisiting the decision to reclassify BIAS as a Title II service would benefit consumers by helping to restore the application of consistent and uniform privacy and data security obligations across the Internet.

STANDARD OF REVIEW

When considering stay requests, the Commission employs a four-part test established by the D.C. Circuit Court of Appeals.[12/] A stay is appropriate when a petitioner shows that: (1) it is likely to prevail on the merits; (2) it will suffer irreparable harm absent the grant of a stay; (3) grant of a stay will not injure other parties; and (4) the grant of a stay furthers the public interest.[13/] The Commission's consideration of each factor is weighed against the others, with no single factor dispositive.[14/]

In considering whether to grant a stay, "[t]he necessary 'level' or 'degree' of possibility of success will vary according to the [adjudicator's] assessment of the other factors."[15/] It is not

---

11/ Letter from Commissioners Ajit Pai and Michael O'Rielly, to Meredith Atwell Baker, et. al. (Dec. 19, 2016), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db1219/DOC-342677A1.pdf.

12/ *Washington Metropolitan Area Transit Commission v. Holiday Tours, Inc.*, 559 F.2d 841, 843, (D.C. Cir. 1977); *Virginia Petroleum Jobbers Association v. Federal Power Commission*, 259 F.2d 921, 925 (D.C. Cir. 1958). *See also City of Boston, Mass., and Sprint Nextel*, 22 FCC Rcd 2361, ¶ 8 (2007); *Comcast Cable Communications, LLC Petition for Emergency Stay*, Order, 20 FCC Rcd 8217, ¶ 2 (2005) ("*Comcast Cable*"); *Brunson Communications, Inc. v. RCN Telecom Services, lnc.*,15 FCC Rcd 12883 (2000).

13/ *Id.*

14/ *AT&T Corp. v. Ameritech Corp.*, 13 FCC Rcd 14508 ¶ 14 (1998).

15/ *Washington Metropolitan Area Transit Commission*, 559 F.2d at 843.

necessary to show a "mathematical probability" of success on the merits if "the remaining three factors strongly favor granting the motion for stay."[16/] In that case, even a substantial showing on the merits rather than a demonstration of likely success is sufficient to grant the stay.[17/] "[A]n order maintaining the status quo would be appropriate when a serious legal question is presented, if little harm will befall others if the stay is granted and denial of the stay would inflict serious harm."[18/] And if a sufficiently strong showing is made on the merits, the other three factors may be satisfied with a lesser showing.[19/] Further, the Commission "need only to determine the probability of success on a single issue" to find that a stay is warranted.[20/] The instant petition satisfies each of the four factors.

I. PETITIONERS ARE LIKELY TO PREVAIL ON THE MERITS OF THEIR PETITIONS FOR RECONSIDERATION

Petitioners and other parties seeking reconsideration have shown that the broadband privacy, data breach, and data security rules adopted under Section 222 of the Communications Act and applied to ISPs are unlikely to be sustained upon reconsideration. The rules are deficient on both legal and policy grounds.

16/ *Florida Public Service Commission Request for Interpretation of the Applicability of the Limit on Change in Interstate Allocation, Section 36.154(f) of the Commission's Rules*, Order Granting Motion for Partial Stay, 11 FCC Rcd 14324, ¶ 3 (1996) ("*Florida Public Service Commission*").

17/ *Fed.-State Joint Bd. on Universal Serv.*, 20 FCC Rcd. 5167, 5168–69 ¶ 4 (2005) (citing *Washington Metropolitan Area Transit Commission*, 559 F.2d at 843).

18/ *Florida Public Service Commission*, 11 FCC Rcd 14324, at ¶ 3.

19/ *See, e.g.*, *Cuomo v. U.S. Nuclear Regulatory Commission*, 772 F.2d 972, 974 (D.C. Cir. 1985) ("Probability of success is inversely proportional to the degree of irreparable injury evidenced. A stay may be granted with either a high probability of success and some injury, or vice versa."); *Virginia Petroleum Jobbers Association*, 259 F.2d at 925 ("injury held insufficient to justify a stay in one case may well be sufficient to justify it in another, where the applicant has demonstrated a higher probability of success on the merits").

20/ *Comcast Cable*, 20 FCC Rcd 8217, at ¶ 4.

A. The Commission Lacks the Legal Authority to Adopt the Rules Under Section 222.

The Commission lacks the legal authority to adopt core elements of the rules. First, Section 222 does not authorize the Commission to regulate ISP use and sharing of BIAS customer data.[21/] Congress designed Section 222 to cover a discrete data set of telephone customer record information that it defined as CPNI, accessible by only a narrow and specific group of entities (voice telephony providers). But the *Order* untenably seeks to shoehorn into the statute virtually all data that can be associated with broadband users and their devices, a considerable amount of which is readily accessible by countless Internet entities.[22/]

Congress never intended for Section 222 to regulate use and sharing of customer data obtained from the provision of Internet access service. The text and structure of Section 222 are infused with statutorily-defined terms, including subscriber list information, telephone toll service, and telephone exchange service, that are relevant only in the voice telephony context.[23/] Rather than confront the boundaries on its authority imposed by these telephone-centric terms, the Commission violates basic tenets of statutory construction by discarding them altogether in the context of BIAS,[24/] and thereby impermissibly arrogates to itself the authority to redefine the scope of the statute.[25/] But the Commission cannot, as the *Order* seeks to do, exceed the limits of the statute by simply invoking its decision in the *Open Internet Order* to re-label ISPs as "telecommunications carriers" for purposes of Title II,[26/] because that constitutes an

---

21/ NCTA Petition at 4-6; WISPA Petition at 5-7.

22/ Dissenting Statement of Commissioner Michael O'Rielly ("Commissioner O'Rielly Dissent") at 1.

23/ *See* NCTA Petition at 5-6; ACA Petition at 4-5; CTIA Petition at 2-3; Commissioner O'Rielly Dissent at 2.

24/ NCTA Petition at 5; WISPA Petition at 5-6.

25/ *See Order*, ¶ 336; NCTA Petition at 5-6; ACA Petition at 12.

26/ *Order*, ¶ 335.

impermissible expansion of the scope of the statute beyond Congress's intent.[27/] The *Order's* failure to abide by the limits on the Commission's authority under Section 222 warrants reconsideration.

Second, the Commission erred by concluding that Section 222(a) empowers it to constrain ISP use and sharing of the PII of BIAS customers.[28/] As demonstrated in the Petitions, the *Order* finds authority in Section 222(a) only by ignoring both the plain language of that provision and the overarching structure of the statute. When Congress seeks to regulate PII in the Communications Act, it does so explicitly – as evidenced by the language of Sections 631 and 338.[29/] The *Order* never explains why Congress would choose to protect PII by expressly referencing it in two other provisions of the Communications Act – the Cable and Satellite Privacy Acts – but refrain from making any reference to the term PII in Section 222.[30/] This conclusion is supported by the legislative history, which makes clear that the focus of Section 222 is CPNI, *not* PII.[31/] Put simply, the *Order* never reconciles its assertion that the protection of PII is "at the heart of most privacy regimes"[32/] with the deliberate Congressional decision to refrain from using that term anywhere in Section 222.

The language of Section 222 further precludes the Commission from subjecting BIAS customer PII to the statute. Archetypal examples of PII – name, address, and phone number –

27/ NCTA Petition at 5, n.13; ACA Petition at 7-8; WISPA Petition at 8.

28/ NCTA Petition at 6-9; US Telecom Petition at 23-24; ACA Petition at 5-7; CTIA Petition at 3-6; ITTA Petition at 3-11; WISPA Petition at 12-14.

29/ *See* 47 U.S.C. §§ 551(b); 338(i)(3).

30/ NCTA Petition at 6-7; ANA Petition at 8 ("Had Congress intended proprietary information regarding customers to include PII, it would have used the term PII as it did in other statutes").

31/ Notably, the "Conference agreement" portion of the Conference Report for the Telecommunications Act stated: "the new section 222 strives to balance both competitive and consumer privacy interests *with respect to CPNI*." H.R. Rep. No. 104-458, at 205 (1996) (emphasis added).

32/ *Order*, ¶ 88.

are explicitly defined for *all* of Section 222 as "subscriber list information," a category of data excluded by the statute from the protections applied to CPNI.[33/] The Commission cannot take a category of information that Congress plainly defined in a specific manner for use throughout Section 222, and redefine it as something completely different using Section 222(a).[34/] The *Order* itself even goes on to acknowledge, but not distinguish, the Commission's prior finding "that names, addresses, and telephone numbers are *not* CPNI, *even when not published as subscriber list information*."[35/]

The structure of Section 222 also shows that Congress could not have intended Section 222(a) to serve as an independent constraint on PII use and disclosure.[36/] Section 222(e) imposes a duty on providers to enable third-party publishing of names, addresses, and phone numbers – subscriber list information – "notwithstanding subsections (b), (c), and (d)."[37/] If these categories of information were intended to be protected under subsection (a), then Congress would have needed to include subsection (a) in subsection (e)'s notwithstanding clause. Congress did not do this because Section 222(a) does *not* grant the Commission standalone authority to restrict the use and sharing of PII or other information not expressly covered by the statute as a whole.[38/]

33/ 47 U.S.C. § 222(h).

34/ NCTA Petition at 7; WISPA Petition at 21-22.

35/ *Order*, ¶ 99 (emphasis added).

36/ NCTA Petition at 8-9; ACA Petition at 9-10; CTIA Petition at 5-6; ITTA Petition at 3-8; ANA Petition at 8; CCA Petition at 4-5.

37/ 47 U.S.C. § 222(e).

38/ The *Order's* attempt to avoid this conclusion suffers from an obvious internal contradiction – in paragraph 86, the *Order* asserts that customer proprietary information is information that "should not be exposed widely to the public," but then in paragraph 351 maintains that certain types of information the Commission seeks to classify as customer proprietary information (CPI) are "by definition… published and therefore… not confidential." *Compare Order*, ¶ 86 *with Order*, ¶ 351.

Third, Section 222 precludes the Commission from constraining ISP use and sharing of IP addresses, MAC IDs, and other device identifiers.[39/] The Commission's inclusion of IP addresses and MAC IDs within the definition of CPNI fails because CPNI is defined as proprietary information "made available to the carrier by the customer,"[40/] whereas IP addresses are assigned to the customer's device by the carrier.[41/] Nor can they be considered "proprietary" given their widespread availability to numerous entities throughout the Internet ecosystem.[42/] The Commission likewise cannot treat IP addresses and other device identifiers as PII (even assuming PII were covered by Section 222, which it is not) because, as the record demonstrates and as numerous courts have found,[43/] IP addresses and device identifiers on their own cannot identify an individual.

Fourth, the Commission lacks authority to constrain ISP use and sharing of the content of broadband customer communications in the manner set forth in the *Order*.[44/] In fact, the Commission had previously concluded that "call content information is not considered CPNI" and therefore falls outside the ambit of Section 222's restrictions.[45/] The *Order* fails to acknowledge this precedent or cite to any statutory basis in Title II in support of its contrary

---

39/ NCTA Petition at 9-11; WISPA Petition at 21-22.

40/ 47 U.S.C. § 222(h)(1)(A). *See* US Telecom Petition at 23; WISPA Petition at 12.

41/ NCTA Petition at 9-10; WISPA Petition at 21-22.

42/ NCTA Petition at 10; CTIA Petition at 4-5. *See also* ACA Petition at 8; WISPA Petition at 21.

43/ NCTA Petition at 10-11, nn.45, 48; US Telecom Petition at 20-21; Letter from Loretta Polk, NCTA, to Marlene H. Dortch, Secretary, Federal Communications Commission, WC Docket No. 16-106, at 10-11, nn.34-37 (Oct. 20, 2016) (citing cases).

44/ *Order*, ¶ 104. *See also* US Telecom Petition at 12-13 (showing that the Commission's definition of "Content" is so overbroad and "nebulous that it could be read to include almost any online activity").

45/ *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Networking Information and Other Customer Information*, Notice of Proposed Rulemaking, 11 FCC Rcd 12513, ¶ 47 (1996). *See also Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Networking Information; Use of Data Regarding Alarm Monitoring Service Providers*, 11 FCC Rcd 9553, n.18 (1996).

determination.[46/] Rather, the *Order* cites to other statutes *outside* Title II or the Communications Act that protect content,[47/] which merely bolsters the view that when Congress desires to regulate communications content, it does so explicitly.[48/]

B. Adoption of the Notice and Choice Rules was Arbitrary and Capricious.

The notice and choice rules adopted by the Commission are arbitrary and capricious in various respects. They are predicated upon a misreading of the record regarding ISP visibility into broadband customer data, unjustifiably depart from the FTC's long-standing and effective privacy framework, and lack an appropriate assessment of whether the costs and burdens of the rules outweigh any purported benefits, particularly with respect to small providers.

First, the Order is predicated upon the fatal misconception that ISPs have unique visibility into broadband customer information relative to other Internet entities.[49/] The record shows that the growth of encryption, virtual private networks, and consumer Internet access via multiple devices and platforms means that ISPs have no more – and increasingly have less – visibility into broadband customer data than non-ISPs.[50/] Professor Peter Swire's findings in his comprehensive study of information flow over the Internet, including that "non-ISPs often have

---

46/ NCTA Petition at 11-12. Indeed, Section 222 imposes constraints only on the use and sharing of CPNI, and the definition of that term is limited to information *about* a communication, and does not encompass the content of the communication itself – which is protected by other statutes outside Title II of the Communications Act. *See* 47 U.S.C. § 222(h)(1).

47/ *Order*, ¶ 104, n.261.

48/ *See* WISPA Petition at 10 (explaining why Section 705 cannot constrain ISP use and sharing of content, or other broadband customer data, in the manner set forth in the *Order*).

49/ Oracle Petition at 3-7; USTelecom Petition at 2 ("[T]he *Order* ignores the record facts when it predicates this scheme of asymmetric regulation on the premise that ISPs are nearly omniscient and have greater visibility into consumer data than any other Internet company. That premise is false, as Commissioners Pai and O'Rielly and many commenters have explained"); Dissenting Statement of Commissioner Ajit Pai ("Commissioner Pai Dissent") at 2 ("The volume and extent of personal data that edge providers collect on a daily basis is staggering").

50/ NCTA Petition at 13-16; US Telecom Petition at 9-11.

access to more and a wider range of user information than ISPs,"[51/] was affirmed by a broad cross-section of commenters.[52/] The *Order* fails to grapple with these findings, instead offering only conclusory and fallacious assertions, such as the claim that "edge providers only see a slice of any given consumer's Internet traffic."[53/] Even commenters inclined to support the adoption of the Commission's rules acknowledged that framing ISPs as a more significant risk than edge providers is incorrect and provides a tenuous foundation for the rules.[54/]

The *Order* also errs by finding that ISPs exercise a unique gatekeeper role that warrants special constraints on their use of BIAS customer information.[55/] The record demonstrates that most consumers access the Internet via multiple devices and over multiple networks operated by multiple broadband providers.[56/] ISPs face more significant competitive constraints than large edge providers in several market segments – including search, social media, operating system

---

51/ Peter Swire, Justin Hemmings, Alana Kirkland, *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others*, The Institute for Information Security & Privacy at Georgia Tech, at 4 (May 2016) (submitted in Docket No. WC 16-106).

52/ NCTA Petition at 13, n.61; CTIA Petition at 7; WISPA Petition at 15; Oracle Petition at 4.

53/ *Order*, ¶ 30.

54/ *See* Memorandum, *FCC Communications Privacy Rulemaking*, Electronic Privacy Information Center, 1-2 (Mar. 18, 2016), *available at* https://epic.org/privacy/consumer/EPIC-Draft-FCC-Privacy-Rules.pdf ("Agencies engaged in rulemaking actions have a duty to accurately frame the problem they seek to address. The current description of the problem presents ISPs as the most significant component of online communications that pose the greatest threat to consumer privacy. This description is inconsistent with the reality of the online communications ecosystem, incorrectly frames the scope of communications privacy issues facing Americans today, and is counterproductive to consumer privacy."); *id.* at 1 ("[M]any of the largest email, search, and social media companies exceed the scope and data collection activities of the ISPs"); Consumer Watchdog Comments, WC Docket No. 16-106, at 3 ("As the Pew results demonstrate, it is not just [ISPs] that prompt people's privacy concerns. It is the entire Internet ecosystem."). *See also* Oracle Petition at 7.

55/ NCTA Petition at 15-16; USTelecom Petition at 11-12.

56/ CTIA Petition at 7; NCTA Petition at 15 and n.68. In addition, the Commission itself stated in the *Order* that small ISPs, some of which provide Internet access to the nation's most underserved and rural customers, "tend to collect and use customer data, including sensitive information, far less extensively" than other providers may. *Order*, 113-114, ¶ 268; WISPA Petition at 17. This statement cannot be reconciled with the Commission's unsubstantiated conclusions that ISPs have unique access to customer information.

platforms, browsers, and online advertising – that are subject to more flexible restrictions on use and sharing of broadband consumer data.[57/]

Second, the Order's asymmetric divergence from the FTC's technology-neutral framework is arbitrary and capricious, particularly in light of the Commission's failure to provide any evidence of harm to consumers from that approach.[58/] The *Order* departs dramatically from the FTC's long-standing and effective privacy framework by treating all BIAS customer Web browsing and app usage data as sensitive and subject to opt-in consent when accessed by ISPs, even though most of that information remains non-sensitive and subject to opt-out consent when accessed by non-ISPs.[59/] The *Order* compounds this unwarranted regulatory disparity by subjecting most first-party marketing activities of ISPs to either opt-in or opt-out consent, even though non-ISPs generally are permitted by the FTC framework to use customer data to market other products and services they offer based on implied consent.[60/] The FTC itself noted that applying different rules for the same information is "not optimal," and reaffirmed the wisdom and utility of applying a consistent set of privacy obligations for the same data set.

The *Order* adopts these departures without citing any evidence that broadband customers were harmed when ISPs were treated the same as non-ISPs with respect to use and sharing of

---

57/ NCTA Petition at 15 and n.69; WISPA Petition at 15. *See also* Commissioner Pai Dissent at 2 ("[D]ue to the FCC's action today, those who have more insight into consumer behavior (edge providers) will be subject to more lenient regulations than those who have less insight (ISPs)").

58/ NCTA Petition at 16-19; ACA Petition at 14-19; CTIA Petition at 8; CCA Petition at 6-7; WISPA Petition at 16, *quoting* Commissioner O'Rielly Remarks Before the Catholic University School of Law Technology Institute Panel, "Protecting Consumer Privacy and Promoting Innovation in the Internet Era" (Nov. 2, 2016) at 3 ("There is very little real evidence in the record that ISPs have or are planning to dissect the consumer traffic that they carry to a degree that would result in consumer harm").

59/ CTA Petition at 4 (by classifying Web browsing and app usage data as sensitive, *Order* "undermines . . . 'customer and business expectations" by departing from the FTC's framework and existing consensus regarding what information should be considered sensitive"); WISPA Petition at 20.

60/ US Telecom Petition at 14-15.

Web-browsing and app usage data, or with regard to first-party marketing.[61/] The Commission's failure to align its notice and choice rules with the demonstrably effective FTC framework constitutes an "overarching error[]" that by itself warrants reconsideration.[62/] While the *Order* asserts that consumers have different privacy expectations of their ISPs than edge providers, the record shows the opposite – that consumers trust their data with ISPs *more* than most other Internet entities and that consumers favor a consistent and uniform set of privacy obligations governing use of their data across the Internet.[63/]

Third, the *Order* fails to acknowledge or adequately grapple with the substantial costs and burdens caused by its significant departures from the status quo, and hence never assesses whether those costs can be deemed to outweigh the purported benefits of the rules.[64/] The disparate constraints on ISP use and sharing of BIAS customer data will, *inter alia*, put upward pressure on retail subscription prices, limit the ability of ISPs to provide data-driven services and capabilities to their customers, increase consumer confusion by applying different privacy regimes to the same set of consumer data, thwart the emergence of competition in the online advertising market, and needlessly hinder the digital economy.[65/] The *Order* also failed to comply with the RFA, which requires the Commission to provide an in-depth analysis of how

---

61/ *See* NCTA Petition at 16-18; CTIA Petition at 7; CTA Petition at 5 (*Order* departs from FTC and other privacy regime precedent regarding treatment of Web browsing and app usage data "without adequate justification"); *id.* at 7 (*Order* fails to acknowledge, let alone explain adequately, "its departure from FTC precedent and staff recommendations"); USTelecom Petition at 14 (Noting Commissioner's O'Rielly's observation that "there is no rational reason" to depart from the FTC's treatment of first-party marketing); ACA Petition at 15.

62/ USTelecom Petition at 2-3.

63/ NCTA Petition at 18; ACA Petition at 15-16.

64/ CTA Petition at 12-15; NCTA Petition at 19-21; WISPA Petition at 18-19. *See also* Commissioner O'Rielly Dissent at 8 ("Had the Commission conducted a cost-benefit analysis, which it committed to do but failed to live up to once again, it would have been unable to justify adopting these significant additional restrictions").

65/ NCTA Petition at 19-21; USTelecom Petition at 4-9; CTIA Petition at 10-11; CTA Petition at 13-14; WISPA Petition at 18, 25-26.

proposed rules will impose a significant economic impact on small providers, including an assessment of cost burdens versus benefits.[66/] The *Order* never weighs these substantial costs against the putative incremental benefit to privacy associated with the rules which, as then-Commissioner Pai correctly pointed out, is limited at best since "[n]othing in these rules will stop edge providers from harvesting and monetizing your data."[67/] As CTA notes, the "FCC's failure to conduct a cost-benefit analysis for its unproven approach – particularly in light of the evidence of the clear costs in the record and illusory nature of purported benefits – falls short of rational rulemaking."[68/]

C. The Broadband Privacy Rules Are Impermissible Under the First Amendment

The rules adopted by the Commission cannot pass constitutional muster. The *Order* inarguably constrains the First Amendment rights of ISPs, and fails to do so in a way that meets the exacting constitutional standards necessary to be upheld in light of those restrictions.[69/] The unique restrictions imposed upon ISPs with respect to Web browsing and app usage data, as well as first-party marketing activities, create speaker-based distinctions among similarly-situated

---

66/ CCA Petition at 16-17, *citing* 5 U.S.C. § 603, *and* Letter from Darryl L. DePriest, Chief Counsel for Advocacy, SBA Office of Advocacy, and Jamie Belcore Saloom, Assistant Chief Counsel, SBA Office of Advocacy, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 at 2, 4 (filed June 27, 2016), *and* Letter from Steve Chabot, Chairman, U.S. House of Representatives Committee on Small Business, and Nydia Velazquez, Ranking Member, U.S. House of Representatives Committee on Small Business, to Hon. Tom Wheeler, Chairman, FCC (Aug. 25, 2016). For instance, the Initial Regulatory Flexibility Analysis ("IRFA") attached to the *Privacy NPRM* did not, as required, describe and assess the significant economic impact of the Commission's proposals on small entities, nor did the IRFA discuss alternative rules that might reduce burdens to small providers. Instead, the Commission merely estimated the number of small BIAS providers that would be forced to comply with the rules. Although the Commission's Final Regulatory Flexibility Analysis ("FRFA") was more robust, the Commission never acknowledges its earlier compliance failures or attempts to quantify costs. Rather, in the FRFA, the Commission opted to describe the extent to which it had backed down from many proposals in the *NPRM*. *See Order*, Appendix B. In short, the *Order* fails to grapple with the manner in which small BIAS providers absorb and implement new, demanding agency rules.

67/ Commissioner Pai Dissent at 2. *See also* NCTA Petition at 20; WISPA Petition at 18.

68/ CTA at 15.

69/ NCTA Petition at 21-23; US Telecom Petition at 22.

entities in the Internet ecosystem concerning the use and disclosure of the same customer information. While such speaker-based distinctions are subject to heightened scrutiny,[70/] the *Order* does not even acknowledge, let alone satisfy, the exacting standard created by its establishment of those distinctions.[71/]

Even if subject to the intermediate scrutiny standard of *Central Hudson*, the rules would still fail.[72/] Not only are they under-inclusive because similarly situated entities are excluded from their ambit, but they also are over-inclusive because they improperly classify certain non-sensitive information as sensitive and impose stringent privacy protections on data elements such as IP addresses and other device identifiers that are widely available throughout the Internet and do not, by themselves, identify individuals.[73/] As ANA notes, the *Order* also is constitutionally infirm because it makes "no attempt to demonstrate that the [rules are] narrowly tailored to serve the privacy interests that [they] assert[]," and fails to show that the choice mechanisms available under the FTC framework for Web-browsing/app usage data and first-party marketing "would be insufficient to protect privacy."[74/]

70/ *Sorrell v. IMS Health, Inc.*, 564 U.S. 552, 570-71 (2011).

71/ NCTA Petition at 21-22; Laurence H. Tribe and Jonathan S. Massey, *The Federal Communications Commission's Proposed Broadband Privacy Rules Would Violate The First Amendment*, at 23 (May 27, 2016) ("[T]he speaker specific nature of the FCC's proposal – the singling out of ISPs – raises separate concerns under First Amendment equal protection principles"); Laurence H. Tribe and Jonathan S. Massey, *Supplemental White Paper: A Response to Arguments That The Commission's Proposed Broadband Privacy Rules Would Be Consistent With The First Amendment*, at 2, 10 (Sept. 13, 2016).

72/ NCTA Petition at 22-23; CTIA Petition at 12-15.

73/ NCTA Petition at 22-23; USTelecom Petition at 22.

74/ ANA Petition at 10. *See also* CTIA Petition at 14-15; NCTA Petition at 23.

D. The Flaws in the *Order's* Data Breach and Data Security Obligations Warrant Reconsideration

Petitioners are also likely to succeed on the merits of their arguments that the data breach and data security obligations established in the *Order* should be reconsidered.[75/]

First, the notification obligations can be triggered by unauthorized access to a broad swath of data that is inherently non-sensitive and unlikely to cause harm.[76/] Moreover, the *Order* unjustifiably presumes that any breach of sensitive data results in harm.[77/] The end result is that ISPs will be forced to investigate every instance where there is a possibility of unauthorized access to common customer data elements like IP addresses and MAC IDs, and may, depending upon how the rule is interpreted, be presumptively required to notify law enforcement and consumers any time, for example, Web-browsing data associated with an IP address is accessed "without authorization."[78/] This is the case even though mere access without use or disclosure is highly unlikely to cause harm, and thus the risk of notice fatigue will hinder the ability of consumers to focus on those instances in which they are subject to tangible harm.

Second, a key flaw of the data breach rules is that the timeframe for notification starts upon reasonable determination of a breach, rather than upon determination on the likelihood of harm.[79/] Although the Commission adopted a harm trigger to determine whether notice is required, the very short deadlines for breach notices (especially for large breaches involving 5,000 or more customers) likely will not provide adequate time in many instances to determine

---

75/ NCTA Petition at 23-25; CTIA Petition at 19-21.

76/ CTIA Petition at 20; CCA Petition at 18-19; WISPA Petition at 20.

77/ *Order*, ¶ 267. *See* WISPA Petition at 19-20; CCA Petition at 20.

78/ *See Order*, ¶ 261 ("We define a breach as any instance in which a person, without authorization or exceeding authorization, has gained access to, used, or disclosed customer proprietary information").

79/ *Order*, ¶ 278.

whether there was customer harm, especially for mere unauthorized access to CPI that is readily available on the Internet. This undermines the efficacy of the harm trigger adopted in the *Order* and lead to a substantial over-notification problem.[80/] As CTIA notes, it is far more consistent with consumer expectations – and with the goal of minimizing unnecessary alarm – to "require notification only when a provider determines that 'harm' is reasonably likely to occur as a result of the breach."[81/] The problem is exacerbated by the Commission's decision to define harm to include a variety of vague, non-economic impacts, such as "emotional" harm, reputational damage, and embarrassment, which will complicate harm determinations and thereby cause significant over-notification problems.[82/]

Third, while the *Order* appropriately adopts a "reasonable measures" standard for the data security obligations in the rules,[83/] the scope of information that would be held to the identical standard of what would be considered "reasonable" is impermissibly broad due to the wide scope of data defined as CPI and the wide scope of data characterized as sensitive.[84/] Further, though highlighting the importance of consistent application of that standard across the Internet,[85/] the *Order* undermines that objective by failing to ensure that the "reasonable measures" standard will be applied consistently with the FTC. To the contrary, the *Order* expressly states that the Commission will look beyond the FTC's interpretation of that standard and take into account the requirements of other privacy regimes such as the Health Insurance

---

80/ NCTA Petition at 23-24; ACA Petition at 17-18; USTelecom Petition at 18; WISPA Petition at 20.

81/ CTIA Petition at 19-20.

82/ NCTA Petition at 24; CTIA Petition at 20; ACA Petition at 17-18; USTelecom Petition at 19-20; WISPA Petition at 19-20; CCA Petition at 19.

83/ *See e.g., Order*, ¶ 238.

84/ *See supra* pp. 11-13. *See also* NCTA Petition at Section I.B and I.C.

85/ *Id.*, ¶ 246.

Portability and Accountability Act (HIPAA) and the Gramm Leach Bliley Act (GLBA),[86/] thereby substantially widening the uncertainty and compliance burdens imposed upon ISPs relative to all other Internet entities and heightening the risks of different interpretations.[87/] For these reasons, the *Order's* treatment of the data breach and data security rules for BIAS customer data also is likely to be reconsidered.

II. ISPs WILL SUFFER IRREPARABLE HARM ABSENT A STAY

Absent a stay, Petitioners' member companies will experience irreparable harm. As an initial matter, as described above, Petitioners' members will suffer a violation of their First Amendment rights,[88/] which itself constitutes an irreparable harm justifying a stay.[89/]

Moreover, Petitioners will be forced to bear substantial costs and burdens complying with rules that are unsustainable as a matter of law and sound policy.[90/] The economic losses that

---

86/ *Id.*, ¶ 250.

87/ NCTA Petition at 25. Further, the *Order* sets forth a recommended set of data security practices that the Commission believes "provide a solid foundation for data security," *Order*, ¶ 249, some of which may not be employed today by companies represented in Petitioners' filings. *See id.*, ¶¶ 250-54. The Commission's recommendations include potential changes to a company's internal organizational structure, customer authentication methods, as well as the institution or expansion of data minimization measures. While some recommendations are not mandated by the *Order*, companies may consider adopting them in order to ensure that they are compliant, particularly since the Commission signals in the *Order* that its administration of the "reasonable measures" standard will draw in unspecified ways from a variety of other privacy statutes and privacy frameworks.

88/ *See supra* Section I.C.

89/ *Elrod v. Burns*, 427 U.S. 347, 373 (1976) (citing *New York Times Co. v. United States*, 403 U.S. 713 (1971)). *See also Field Day, LLC v. County of Suffolk*, 463 F.3d 167, 181 (2d Cir. 2006); *Connection Distrib. Co. v. Reno*, 154 F.3d 281, 288 (6th Cir. 1998)("[T]o the extent that [movant] can establish a substantial likelihood of success on the merits of its First Amendment claim, it also has established the possibility of irreparable harm").

90/ *State of Texas v. United States Environmental Protection Agency*, 829 F.3d 405 (5th Cir. 2016)(Regulatory compliance costs suffice to establish irreparable injury where no mechanism exists to recover such costs should the challenged rule be invalidated); *National Medical Care v. Shalala*, 1995 U.S. Dist. LEXIS 10074, *9 (D.D.C. 1995)(Given likelihood of plaintiffs' success on the merits, compliance costs constitute irreparable injury because "it would be absurd" to impose such costs on plaintiffs); *Central Valley Chrysler Plymouth v. California Air Resources Board*, 2002 U.S. Dist. LEXIS 20403, *21 (E.D. CA 2002) (Finding of irreparable injury may be based on the excessive costs of compliance when coupled with the inability to recoup those should the challenge to the regulation ultimately be successful); *In the Matter of Hickory Tech Corporation and Heartland Telecommunications Company, Petition for Waiver of Section 69.605(c)*, 13 FCC Rcd 22085, ¶ 3 (1998) (Finding irreparable injury in circumstance where denial of stay would cause expenditure of "substantial resources that would be unnecessary – and unrecoverable – if Petitioners later were to succeed in their Application for Review"). *See also In the Matter of*

ISPs will imminently face in preparing to implement regulatory obligations that will likely be invalidated or revised are non-recoverable and thus also constitute irreparable harm under the law and Commission precedent.[91/] These non-recoverable costs will be especially harmful to small providers, who rely on limited capital and personnel to provide competitive BIAS services.[92/]

The notice and choice provisions will require ISPs to devote considerable costs and resources toward operationalizing the new constraints on data collection, use, and sharing established by the *Order*. The *Order* itself recognizes that this will be a costly and resource-intensive process and therefore provides ISPs with twelve months to come into compliance with those requirements.[93/] To meet that deadline, ISPs will need to incur substantial costs immediately so as to have compliant technical safeguards and internal business procedures in place by the rules' effective date.[94/] As the Commission acknowledged, "our new notice and choice rules may 'represent a significant shift in the status quo' for carriers… [ISPs will need to] analyze the new, harmonized privacy rules as well as coordinate with various business segments

Charter Communications Entertainment I, LLC, 22 FCC Rcd 13890, ¶ 4 (2007) ("If a petitioner makes a strong showing of likely success on the merits, it need not make a strong showing of irreparable harm").

91/ *Thunder Basin Coal Co. v. Reich*, 510 U.S. 200, 220-21 (1994) (Scalia, J., concurring in part and in the judgment ("[C]omplying with a regulation later held invalid almost always produces the irreparable harm of non-recoverable compliance costs"); *Sottera, Inc. v. FDA*, 627 F.3d 891, 898 (D.C. Cir. 2010) (injury to business that could not be remedied constitutes irreparable harm); *Comcast Cable*, 20 FCC Rcd 8217 (2005) (granting temporary stay where success on review was possible on at least one of petitioner's claims and where petitioner faced non-recoupable economic harm); *Brunson Communications, Inc.*, 15 FCC Rcd 12883, at ¶ 3 (granting stay because, barring stay, petitioner would incur "costs that will not be recoverable should it prevail on review"); *Heritage Cablevision, Inc. d/b/a TCI of Central Iowa Petition for Stay of Local Rate Order of City of Des Moines, Iowa*, Order, 13 FCC Rcd 22842 (1998) (granting stay where petitioner faced irreparable harm in the form of non-recoverable economic losses).

92/ CCA Petition at 17, n.55.

93/ *Order*, ¶ 312. Further, small ISPs were afforded 24 months to come into compliance, thereby further underscoring the complexity and resource-intensiveness of conforming business practices to the new rules.

94/ CCA Petition at 17.

and vendors, and update programs and policies," as well as "engage in consumer outreach and education."[95/]

But that only skims the surface of the technical, operational, and business steps that must be performed between now and the rules' effective date.[96/] ISPs will need to take substantial technical measures – which will entail significant changes to current network hardware and software assets – to reconfigure data collection and use protocols. They will need to establish new internal business rules regarding use and sharing of a significantly larger swath of information, including data elements such as IP addresses and MAC IDs that are a fundamental component of basic network operations – and they will need to revise and update company operating manuals to reflect those changes. Employee training programs will need to be modified and many thousands of company personnel trained. Some companies, such as small rural providers, must hire additional employees or procure the services of third parties to manage each facet of the transition to the new rules. Companies also will be forced to review and analyze their contracts with vendors and other third parties to ensure that any provisions relevant to handling customer data are compliant with the new rules, and may be required to renegotiate certain provisions.

Further, ISPs will need to revise all customer-facing communications materials that address use and sharing – and the requisite permissions therefor – of broadband data. To be in compliance by the rules' effective date, ISPs will need to revise and send notices, and obtain opt-

---

95/ *Order*, ¶ 312. The process of analyzing the impact of the rules on current business practices itself imposes particular harm on small providers' customers. CTA Petition at 13; USTelecom Petition at 4, 7. Small providers are unable to absorb the immense administrative costs necessary to navigate regulations as complicated as the *Order*, and the costs of hiring outside attorneys and staff must ultimately be passed on to the customers themselves. WISPA Petition at 17.

96/ ACA Petition at 20-21 (describing the costs associated with compliance and the Commission's failure to conduct an economic analysis of those costs).

in for the use of app usage and Web browsing data, and offer either opt-in or opt-out consent for most first-party marketing activities they undertake today. This will also require technical and administrative data-handling systems for tracking and ensuring compliance with a substantially larger and more varied set of customer consents.

As noted, the Commission's establishment of special rules applicable solely to ISP treatment of broadband consumer is inherently confusing for consumers. Even if consumers withhold consent from their ISPs, they likely will not realize that various other online companies will continue to collect and use their data. It will be particularly confusing for consumers if ISPs begin to implement these policy changes and the FCC then modifies or eliminates the rules, which would necessitate an additional round of changes to customer-facing notices and policies.

The application of either an opt-in requirement (applicable to use of Web browsing and app usage data) or opt-out consent (for all "non-sensitive" data) prior to using customer information for engaging in most first-party marketing of an ISP's other products and services represents a sea change from the status quo. This will hinder the ability of customer service representatives to recommend products and services to BIAS customers that could meet their needs, which they have come to expect and value under the long-standing FTC regime – thereby impairing customer goodwill.[97/] The rules' constraints on data-driven advertising and marketing also will raise the costs of advertising and marketing campaigns and produce greater waste by limiting the ability of companies to target such activities to those customers most likely to be responsive.

97/ *See Ferrero v. Associated Materials, Inc.*, 923 F.2d 1441, 1449 (11th Cir. 1991) ("[T]he loss of customers and goodwill is an irreparable injury"); *Ross-Simons of Warwick, Inc. v. Baccarat, Inc.*, 217 F.3d 8, 13 (1st Cir. 2000) (courts "often find" injuries to "goodwill and reputation" to be irreparable).

The costs and burdens associated with undertaking these dramatic changes from long-standing business practices and data-handling routines will be unrecoverable. ISPs already are incurring costs associated with analyzing the myriad changes to their network operations and business practices that will be necessitated by the new rules, and many will soon be forced to begin (if they have not started already) to bear the costs of implementing these changes. Compliance on day one requires a significant investment of time and resources in the months leading up to the rules' effective date. For example, technical changes need to be designed and tested well in advance to ensure safe and smooth network operations, and employee training requires substantial lead time. And to the extent the Commission ultimately decides to withdraw – or substantially revise – the rules adopted in the *Order*, these implementation costs will be unrecoverable, and will be compounded by additional costs associated with reverting back to protocols and practices permitted prior to establishment of the vacated obligations.

The new rules also will inflict considerable damage on data-driven revenue streams and new product initiatives, due to the well-documented disparities in approval rates between opt-in and opt-out consent regimes.[98/] In relation to other Internet entities with which they compete, ISPs will have a more difficult time developing and offering data-driven services, products, and capabilities, thereby impeding their ability to attract customers to their products and platforms and to differentiate their offerings from competitors' products. Similarly, the rules' restrictions on data use will hurt ISPs' ability to offer discounts and incentives to customers, which, in turn, will negatively impact subscriber retention, business growth, and customer goodwill. In addition, the rules will severely hamper the ability of ISPs to enter and compete in the digital

98/ NCTA Petition at 21; *id.* at n.94.

advertising marketplace against large entrenched incumbents.[99/] By dampening revenue from data-driven services and markets, the rules also will inhibit investment. The loss of these business opportunities and the adverse impact of the rules on subscriber growth and retention, customer goodwill, broadband deployment, and market share relative to non-ISPs cannot be adequately recouped in the future and thus also constitute irreparable harm.[100/]

Beyond the harms that will be incurred due to the *Order's* new notice and choice rules, the new data security and data breach requirements will cause their own set of irreparable harms. Given that these rules currently are slated to take effect potentially as early as March 2, 2017 and June 2, 2017, respectively, the harm to Petitioners from failing to grant a stay is even more immediate. As discussed above,[101/] while the "reasonable measures" standard governing the Commission's data security rules itself is not objectionable, an extraordinary breadth of information is potentially subject to that standard, including a considerable amount of data that is non-sensitive because it cannot, on its own, identify an individual. Further, the *Order* states that it will be construed in accordance with "implementation of data security requirements under HIPAA, GLBA, and other relevant statutory frameworks."[102/] These changes represent a substantial departure from the status quo, in which ISPs have operated under the FTC's interpretations of the FTC Act's Section 5 prohibition against unfair or deceptive acts or practices. ISPs must immediately devote resources to assessing the interplay between these other

---

99/ WISPA Petition at 18, *citing* Reply Comments of Competitive Carriers Association, WC Docket No. 16-106 (filed July 6, 2016) at 32 ("[The] rules will create a chilling effect by giving 'a clear competitive advantage to edge providers that already dominate the digital advertising market").

100/ *Multi-Channel TV Cable Co. v. Charlottesville Quality Cable Operating Co.*, 22 F.3d 546, 552 (4th Cir. 1994) ("[W]hen the failure to grant preliminary relief creates the possibility of . . . the loss of goodwill, the irreparable injury prong is satisfied."); *Novartis Consumer Health, Inc. v. Johnson & Johnson-Merck Consumer Pharmaceuticals Co.*, 290 F.3d 578, 596 (3d Cir. 2002) ("[L]oss of market share constitutes irreparable harm").

101/ *See supra* Section I.D.

102/ *Order*, ¶ 250.

privacy regimes and their existing data security practices – which apply in contexts far removed from ISPs' current businesses – and potentially institute technical and operational measures to alter those practices to accord with these other regimes.

To the extent companies opt to ensure compliance by implementing the set of recommended practices set forth in the *Order*[103/] – a measure that may have particular appeal given the *Order's* intention of drawing upon other privacy frameworks and statutes – they would need to allocate additional costs and resources toward such an effort. These recommended practices include changes to a company's internal business structure, potential modifications to its customer authentication methods,[104/] and changes to its information handling practices in order to implement data minimization measures that would be acceptable to the Commission. In a competitive marketplace, forcing companies to devote additional costs and resources toward implementation of requirements that may never become operative is particularly wasteful, and is also counterproductive from the standpoint of consumer welfare because those funds would be better spent developing new offerings or upgrading networks.[105/]

Likewise, the data breach rules will impose additional unrecoverable costs on ISPs. The vast scope of data subject to the FCC's new breach notification obligation due to unauthorized access by third parties is considerably broader than the status quo.[106/] For example, the data breach rules cover commonly shared data elements such as IP addresses and MAC IDs. In addition to being shared with third parties as a matter of course for purposes of basic Internet functionality, these are often broadcast "in the clear" when broadband customers access the

---

103/ *See supra* n.87.

104/ The prospect of having to implement new authentication practices is fraught with risk to customer goodwill, since customers typically find such changes to be inconvenient, unnecessary, and frustrating.

105/ WISPA Petition at 15.

106/ *See, e.g.*, CTIA Petition at 20-21; WISPA Petition at 24.

Internet from WiFi hotspots. The Commission's rules require notice of a breach to the Commission and law enforcement within seven days (and to consumers within 30 days) of reasonably determining the existence of a breach, irrespective of whether or not a determination of harm has been made. In many instances, one (and sometimes both) of those time frames will be insufficient to gather all the facts necessary to ascertain whether or not harm has occurred, particularly because of the breadth of data covered by the obligation and the vagueness of the harm definition.[107/] As a result, prior to the rules going into effect, ISPs will need to establish internal business protocols for identifying, capturing, and assessing any potential unauthorized sharing of *any* CPI data elements with any third party – which may entail software and other technical modifications as well as new monitoring and audit procedures – as well as for rendering a determination as to whether a notification obligation might be triggered. This requires a substantial and immediate devotion of resources, particularly given the broad swath of data covered by the breach notification rules, the numerous situations in which certain data elements are commonly disclosed, and the rules' requirement to notify the FCC and consumers even before a full and accurate assessment can be completed.

If the data breach rules go into effect, there is a substantial risk of over-notification to both government authorities and consumers of breaches that ultimately are deemed not to have caused any harm.[108/] A notice stating that a customer's IP address, MAC ID, or other device identifier was accessed by a third-party without authorization – a potentially frequent occurrence given the scope of the data covered by the rules and the potential breadth of the breach definition – is apt to be of little value to consumers, and more likely to be annoying and confusing. The

---

107/ *See supra* Section I.D.

108/ *See id*.

FTC's comments in the rulemaking proceeding highlighted the negative consumer impact of over-notification,[109/] which also will subject ISPs to unnecessary costs and damage to their goodwill and customer relationships. Both ISPs and consumers will suffer injury from over-notification that leads to notice fatigue. For example, consumers may disregard a notice of breach in a circumstance of real harm, due to being inundated with excessive and unnecessary notices on prior occasions. These concerns are exacerbated by the rules' expansive conception of harm,[110/] as well as their broad definition of sensitive information (which includes app usage data and Web browsing history), combined with the presumption that a breach of sensitive data is harmful. Each of these changes substantially raises the likelihood of over-notification, thereby increasing the costs to ISPs and imposing attendant harms on consumers.[111/]

III. A STAY WILL NOT INJURE OTHER PARTIES AND WILL FURTHER THE PUBLIC INTEREST

The final two factors addressed in evaluating a petition for a stay – harm to the opposing party and the public interest – "merge when the Government is the opposing party."[112/] Grant of a stay will not harm any other party. Instead, it will maintain a status quo that has been in place *for nearly two years* since the Commission adopted the *Open Internet Order* and reclassified BIAS as a telecommunications service, thereby removing ISPs from the purview of the FTC privacy and data security framework. ISPs continue to adhere to privacy policies predicated upon the FTC's core principles of transparency, choice, and security, as well as comply with a

---

109/ Comments of FTC Staff, WC Docket No. 16-106, at 31-32.

110/ *See* US Telecom Petition at 19-20 (noting that a breach can trigger reporting and notification requirements even if it threatens no financial harm and raises only a risk of "emotional harm"); WISPA Petition at 19-20.

111/ *See Order*, ¶ 272 ("We share [commenters'] general concern about the risk of over-notification—it is costly to providers, without corresponding benefit to consumers, and can lead to notice fatigue and possibly consumer de-sensitization").

112/ *Nken v. Holder*, 556 U.S. 418, 435 (2009).

myriad of federal and state privacy- and security-related laws, such as the Children's Online Privacy Protection Act (COPPA), the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act, the Electronic Communications Privacy Act (ECPA), the Stored Communications Act (SCA), and numerous state privacy and data breach laws. Further, ISPs have released a voluntary set of privacy and data security principles that are consistent with the FTC's long-standing framework, and have committed to continue adhering to these obligations regardless of whether the Commission's broadband privacy rules are stayed, thereby further minimizing the risk of harm to other parties.[113/]

The public interest also favors a stay.[114/] The rules effectuate substantial changes to a successful and well-established set of obligations applicable to ISPs under the FTC framework that effectively balanced the interest in safeguarding consumer privacy with the objective of promoting competition, innovation, new services, and growth in the digital economy while also ensuring a consistent and uniform set of privacy obligations across the Internet. Deferring the repudiation of that demonstrably effective approach pending further reconsideration of the lawfulness and wisdom of the dramatic departures from the framework adopted in the *Order* furthers the public interest.[115/]

In addition, there is no public benefit to forcing ISPs to incur substantial costs and burdens in order to begin implementing privacy rules that are unsustainable on both legal and

---

113/ *See* Appendix A.

114/ A stay also is consistent with the recent "Regulatory Freeze" memorandum from the President's Chief of Staff, requesting that agencies "temporarily postpone" the effective date of recently-promulgated rules that have been published in the Federal Register but are not yet operative, "for the purposes of reviewing questions of fact, law, and policy they raise." *See* Memorandum For The Heads of Executive Departments and Agencies, January 20, 2017.

115/ *Cf. Iowa Utilities Bd. v. FCC*, 109 F.3d 418, 427 (8th Cir. 1996) (Finding a stay in the public interest because it would "preserve the continuity and stability of this regulatory system — a system that has initially proved to be successful").

policy grounds. Further, the prospect of the Commission revisiting Title II reclassification also militates in favor of a stay, since the relief requested here would permit the Commission to defer the operative effect of the broadband privacy rules until the issue of BIAS reclassification is definitively resolved. It is not in the public interest to compel ISPs to initiate the process of complying with the arbitrary and unconstitutional broadband privacy rules, especially given that the tenuous legal predicate for their adoption is likely to be revisited by the Commission.[116/] As with the relief requested here, revisiting the decision to reclassify BIAS as a Title II service would benefit consumers by restoring the application of consistent and uniform privacy and data security obligations across the Internet.

116/ *See supra* n.11.

CONCLUSION

For the foregoing reasons, the Commission should stay the rules adopted in the *Order* in the manner suggested herein, pending final resolution of the Petitions for Reconsideration of the *Order*.

Respectfully submitted,

/s/ Rick Chessen*

Rick Chessen
Senior Vice President, Law & Regulatory Policy
NCTA - The Internet & Television Association
25 Massachusetts Avenue, NW, Suite 100
Washington, DC 20001

Joshua Seidemann
Vice President, Policy
NTCA – The Rural Broadband Association
4121 Wilson Boulevard, Suite 100
Arlington, VA 22203

Jonathan Banks
Senior Vice President – Law & Policy
United States Telecom Association
14th Street, NW, Suite 400
Washington, DC 20005

Stephen E. Coran
Wireless Internet Service Providers Association
4417 13th Street, #317
St. Cloud, FL 34769

Derrick Owens
Vice President of Government Affairs
WTA – Advocates for Rural Broadband
400 7th Street, NW, Suite 406
Washington, DC 20004

Ross J. Lieberman
Senior Vice President, Government Affairs
American Cable Association
2415 39th Place, N.W.
Washington, D.C. 20007

Rebecca Murphy Thompson
EVP & General Counsel
Competitive Carriers Association
805 15th Street NW, Suite 401
Washington, DC 20005

Tom Power
Senior Vice President & General Counsel
CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036

Michael J. Jacobs
Vice President, Regulatory Affairs
ITTA – The Voice of Mid-Sized Communications Companies
1101 Vermont Avenue, NW, Suite 501
Washington, DC 20005

January 27, 2017

**Authorized to file on behalf of all Petitioners*

APPENDIX A

ISP Privacy Principles

ISPs understand the trust our customers place in us, and we are committed to protecting our customers' privacy and safeguarding their information. For 20 years, we have implemented policies and practices that are consistent with the FTC's widely respected and effective privacy framework and other federal and state privacy laws. This framework helped drive the success of today's Internet ecosystem by balancing consumer protection with the flexibility necessary to innovate. We understand the importance of maintaining our customers' trust. That is why we will continue to provide consumer privacy protections, while at the same time meeting consumers' expectations for innovative new product solutions to enhance their online experiences. Regardless of the legal status of the FCC's broadband privacy rules, we remain committed to protecting our customers' privacy and safeguarding their information because we value their trust. As policymakers evaluate the issues, we will maintain consumer protections that include the following:

- ***Transparency***. ISPs will continue to provide their broadband customers with a clear, comprehensible, accurate, and continuously available privacy notice that describes the customer information we collect, how we will use that information, and when we will share that information with third parties.

- ***Consumer Choice***. ISPs will continue to give broadband customers easy-to-understand privacy choices based on the sensitivity of their personal data and how it will be used or disclosed, consistent with the FTC's privacy framework. In particular, ISPs will continue to: (i) follow the FTC's guidance regarding opt-in consent for the use and sharing of sensitive information as defined by the FTC; (ii) offer an opt-out choice to use non-sensitive customer information for personalized third-party marketing; and (iii) rely on implied consent to use customer information in activities like service fulfillment and support, fraud prevention, market research, product development, network management and security, compliance with law, and first-party marketing. This is the same flexible choice approach used across the Internet ecosystem and is very familiar to consumers.

- ***Data Security***. ISPs will continue to take reasonable measures to protect customer information we collect from unauthorized use, disclosure, or access. Consistent with the FTC's framework, precedent, and guidance, these measures will take into account the nature and scope of the ISP's activities, the sensitivity of the data, the size of the ISP, and technical feasibility.

- ***Data Breach Notifications***. ISPs will continue to notify consumers of data breaches as appropriate, including complying with all applicable state data breach laws, which contain robust requirements to notify affected customers, regulators, law enforcement, and others, without unreasonable delay, when an unauthorized person acquires the customers' sensitive personal information as defined in these laws.

These principles are consistent with the FTC's privacy framework, which has proved to be a successful privacy regime for many years and which continues to apply to non-ISPs, including social media networks, operating systems, search engines, browsers, and other edge providers that collect and use the same online data as ISPs. That framework has protected consumers' privacy while fostering unprecedented investment and innovation. The principles are also consistent with the FCC's May 2015 Enforcement Advisory, which applied to ISPs for almost two years while the FCC's broadband privacy rules were being considered.

The above principles, as well as ISPs' continued compliance with various federal and state privacy laws, will protect consumers' privacy, while also encouraging continued investment, innovation, and competition in the Internet ecosystem.

Altice USA
American Cable Association
AT&T
Charter Communications
Citizens Telephone and Cablevision
Comcast
Cox Communications
CTIA
Dickey Rural Networks
Inland Telephone Company d/b/a Inland Networks
ITTA – The Voice of Mid-Sized Communications Companies
NCTA – The Internet & Television Association
Northeast Louisiana Telephone Co., Inc. (NortheastTel)
NTCA – The Rural Broadband Association
SCTelcom
T-Mobile
USTelecom
Verizon
VTX1 Companies
Wheat State Telephone, Inc.
Wireless Internet Service Providers Association
WTA – Advocates for Rural Broadband