BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, DC 20554

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

PETITION OF AMERICAN CABLE ASSOCIATION FOR RECONSIDERATION

Matthew M. Polka
President and Chief Executive Officer
American Cable Association
7 Parkway Center, Suite 755
Pittsburgh, PA 15220-3704
(412) 922-8300

Ross J. Lieberman
Senior Vice President of Government Affairs
American Cable Association
2415 39th Place, NW
Washington, DC 20007
(202) 494-5661

January 3, 2017

Thomas Cohen
Jameson J. Dempsey
Kelley Drye & Warren LLP
3050 K Street, NW, Suite 400
Washington, DC 20007
(202) 342-8518

Barbara S. Esbin
Cinnamon Mueller
1875 Eye Street, NW, Suite 700
Washington, DC 20006
(202) 872-6811

David S. Turetsky
Akin Gump Strauss Hauer & Feld LLP
1333 New Hampshire Avenue, NW
Washington, DC 20036
(202) 887-4074
Counsel to the
American Cable Association

TABLE OF CONTENTS

BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, DC 20554

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

PETITION OF AMERICAN CABLE ASSOCIATION FOR RECONSIDERATION

INTRODUCTION AND SUMMARY

American Cable Association ("ACA")[1] hereby petitions the Federal Communications Commission ("FCC" or "Commission") pursuant to section 1.429 of the Commission's rules to reconsider its October 27, 2016 *Privacy Order*.[2] Despite the Commission's claims that its decision balances the privacy and data security interests of consumers and broadband Internet

[1] ACA represents approximately 750 small and medium-sized cable operators, incumbent telephone companies, municipal utilities, and other local providers. In aggregate, these providers pass nearly 19 million homes and serve nearly seven million homes. The vast majority of ACA members have fewer than 5,000 subscribers, and half have fewer than 1,000 subscribers.

[2] *See In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, Report and Order, FCC 16-148 (rel. Nov. 2, 2016) ("Privacy Order"); 47 C.F.R. § 1.429.

service providers ("BIAS providers"), the *Privacy Order* goes off the rails because it makes material errors on the law, facts, and policy and thus warrants complete reconsideration.[3]

First, the *Privacy Order* contains material errors regarding the Commission's legal authority to adopt the rules in the Order.[4] The provisions on which the Commission relies for its authority—sections 201(b), 202(a), and 222 of the Communications Act of 1934 (the "Communications Act" or the "Act")—whether considered singly or in combination, do not permit the Commission to adopt the sweeping, prescriptive broadband privacy rules set forth in the Order or to apply its rules to categories of data beyond customer proprietary network information ("CPNI") as defined in the Act. Even assuming *arguendo* the Commission has authority to reach BIAS privacy practices, it lacks authority to apply such authority to BIAS or other telecommunications carriers with respect to information other than CPNI.

Second, even if the Commission has legal authority to adopt the rules contained in the *Privacy Order*, it fails to provide an evidentiary basis for its highly prescriptive rules in several respects. First, the Commission fails to base its rules on evidence of tangible and material harm to consumers. Second, the Commission fails to give virtually any weight to evidence that BIAS providers have been responsible stewards of their customers' information. Third, the

---

[3] Reconsideration is the most appropriate and expedient means of addressing the myriad, severe shortcomings in the *Privacy Order* before the most burdensome of the new rules take effect. Action via reconsideration is particularly justified with regard to this proceeding given the Commission takes a contorted and largely novel view of its legal authority that goes to the essence of whether it can adopt the new rules pursuant to the statutory provisions. Moreover, action on reconsideration is especially warranted given that the *Privacy Order* adopts applies highly prescriptive *ex ante* privacy rules for the first time to a class of providers not covered by the statute and there is no commitment to review the effect and value of these new rules at a later point.

[4] Nor does the Commission have the authority to classify BIAS as a Title II telecommunications service. *See* Joint Petition for Rehearing En Banc of Petitioners National Cable & Telecommunications Association and American Cable Association, *United States Telecom Ass'n, et al. v. FCC*, No. 15-1063 (D.C. Cir. July 29, 2016).

Commission fails to appreciate the harms that its rules would cause to providers and their customers. Most especially, the Commission erred by failing to meet its obligations under the Regulatory Flexibility Act ("RFA"), resulting in the imposition of disproportionate burdens on small providers that will raise their costs and inhibit their ability to innovate, while upending broadband customer expectations and creating confusion.

Third, the Commission in adopting new breach notification rules fails to consider, address, or appropriately balance arguments in the public interest, resulting in rules that overreach in key respects and are both burdensome on BIAS providers, especially smaller ones, and badly at odds with existing federal and state law. As just one example, the new breach notification requirements create a serious deterrent to cybersecurity information sharing under the Cybersecurity Information Sharing Act of 2015[5] ("CISA") and compound the burdens on small providers by requiring them to cope with new notification requirements on top of 47 state data breach notification laws.

Unfortunately, the *Privacy Order* is a train wreck that the Commission cannot just patch up and place back on the track. The Commission should reconsider its approach to privacy in its entirety, eliminating the rules adopted in the *Privacy Order*, and if it must, replace them with a proposed framework firmly grounded in the Federal Trade Commission's ("FTC's") successful and time-tested section 5 privacy regime to avoid again imposing requirements that are unlawful and do not reflect the record and the public interest.

[5] Cybersecurity Information Sharing Act of 2015, Pub. L. No. 114-113, 129 Stat. 2242, 2935 (2015).

I. THE ORDER CONTAINS MATERIAL ERRORS REGARDING THE COMMISSION'S LEGAL AUTHORITY TO ADOPT THE RULES IN THE *PRIVACY ORDER*

The Commission should reconsider the *Privacy Order* because it erred in finding that it has legal authority to impose the rules adopted. The *Privacy Order* relies on sections 222, 201, and 202 of the Communications Act as the basis for its legal authority.[6] However, sections 222, 201(b), and 202(a), either considered singly or in combination, fail to grant the Commission authority to impose privacy rules on BIAS.[7] Even assuming *arguendo* the Commission has authority to reach BIAS privacy practices, it lacks authority to apply such authority to BIAS or other telecommunications carriers with respect to information other than CPNI.

A. The Commission erred by imposing privacy and data security rules on BIAS pursuant to section 222

Contrary to the conclusions in the *Privacy Order*,[8] the statutory language of section 222 does not authorize the Commission to impose the adopted privacy rules on BIAS. Section 222 clearly focuses on the protection of information related to voice telephony services and not BIAS.[9] Indeed, the only potential link to the Internet in section 222 relates to IP-enabled voice

---

[6] *See Privacy Order*, ¶¶ 333-68.

[7] *See supra*, n. 4. The *Privacy Order* stems from the Commission's *2015 Open Internet Order*, in which it improperly reclassified broadband Internet access service as a telecommunications service under Title II of the Communications Act. *Protecting and Promoting the Open Internet*, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601 (2015), *aff'd sub nom., United States Telecom Ass'n v. FCC*, 825 F.3d 674 (D.C. Cir. 2016), *petitions for rehearing/petitions for rehearing en banc pending* (D.C. Cir., filed July 29, 2016) ("2015 Open Internet Order"). Several parties, including ACA, sought review of the *2015 Open Internet Order* in the D.C. Circuit. While the initial three-judge panel ruled 2-1 to uphold the *2015 Open Internet Order*, petitioners have filed for *en banc* review, a request that is pending. As a foundational matter, if the D.C. Circuit accepts the parties' petition for *en banc* review and vacates the Commission's reclassification, the Commission will not have authority under Title II—including sections 201, 202, and 222—to impose privacy and data security rules on BIAS.

[8] *See Privacy Order*, ¶ 334.

[9] *See* 47 U.S.C. § 222 (cabining key provisions with words such as "call," "call location information," and "telephone exchange service," with no reference to broadband service).

services, which are delivered over the Internet, a category that was added to the statute in 2008.[10] The fact that Congress saw the need to add a specific provision dealing with one specific form of Internet-delivered service—voice—demonstrates that it did not intend section 222 to apply to any other IP-enabled services, let alone an Internet access service such as BIAS. The lack of an explicit reference to the Internet or Internet access service in section 222 stands in stark contrast to section 230 of the Act, which explicitly addresses "the Internet" and "interactive computer services," a term which includes an information service such as BIAS.[11] In short, Congress knows how to include the terms "Internet" and "a service or system that provides access to the Internet" when it intends for a provision to apply to Internet-related services (*e.g.*, BIAS) and did not do so when it drafted section 222. The Commission errs in the *Privacy Order* by arrogating to itself the legislative authority to "adopt broader privacy protections to keep pace with the evolution of telecommunications services,"[12] beyond those carefully delineated by Congress in sections 222(b) and (c) concerning, respectively, carrier and customer proprietary network information.

The Commission's reliance on section 628 as an analogous provision providing it with authority to keep pace with industry developments is particularly inapposite.[13] There, Congress included a preamble setting forth a broad statutory "Purpose" in section 628(a), followed by a

---

[10] *See* NET 911 Improvement Act of 2008, Pub. L. No. 110-283, § 301(1) (2008).

[11] Section 230, for its part, limits the liability of providers and users of "interactive computer services"—i.e., "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet"—and applies to Internet content delivered over "packet switched networks," as opposed to telephone exchange services. *See* 47 U.S.C. § 230(f)(2) (emphasis added).

[12] *Privacy Order*, ¶ 347.

[13] *See id.*, ¶ 349.

specific statutory "Prohibition" on practices that would generally deny competitors access to cable-affiliated programming in section 628(b), and followed that with a provision calling for "Regulations Required" that sets forth in section 628(c) only the "Minimum Contents of Regulations." By setting forth a purpose and an express prohibition and then directing the Commission to enact regulations that at a *minimum* addressed specific, known types of behavior that would violate the statutory prohibition in section 628, Congress was expressly calling upon the Commission to keep pace with industry developments. This stands in sharp distinction to section 222, where Congress has taken it upon itself to establish the regulations required by enacting sections 222(b) and (c) without giving any indication that these were only the "minimum" required. The Commission resorts to pointing to case law permitting it under section 628(b) to prohibit "an anti-competitive practice that is only tenuously related to the 'minimum' requirements implemented under Section 628(c)"[14] as demonstrating the breadth of its authority to similarly impose specific privacy requirements on carriers under the general language of section 222(a). In the case of section 628(b), however, such an expansive interpretation was contemplated by Congress, given the degree of latitude it afforded the Commission to go beyond the minimum specified in adopting implementing regulations under section 628(c). Contrary to the reasoning of the *Privacy Order*, this case says nothing about the scope of the Commission's privacy authority because the latitude granted by Congress under section 628(c) to go beyond the "minimum contents of regulations" set forth in that provision is plainly lacking under section 222.

[14] *See id.* (citing *National Cable & Telecomms. Ass'n v. FCC*, 567 F.3d 659, 661 (D.C. Cir. 2009)).

Furthermore, the Commission plainly erred in finding that there is "no reason to depart from the definition of 'telecommunications carrier' in Section 3 of the Act" in construing the scope of the duties imposed by section 222[15] and in failing to adequately address arguments in the record that the text, structure, and legislative history of the provision do not support its extension to BIAS.[16] Only by erroneously reading significant limitations (*e.g.*, "subscriber list information," "including the publishing of directories")[17] that expressed Congressional intent to limit the scope of section 222 to telephony services out of the statute does the *Privacy Order* achieve its pre-determined conclusion that the statute applies to BIAS, thereby violating the basic canon of statutory construction that all words in the statute must be given effect.[18]

The Commission also makes a material error in concluding in the *Privacy Order* that it may expand the scope of its authority under Section 222 beyond that provided for by Congress in the 1996 Act to avoid a "gap in Congress' multi-statute privacy regime."[19] The Commission's erroneous decision in the *2015 Open Internet Order* to reclassify BIAS as Title II telecommunications services may have created an unfortunate "gap" in broadband consumer

---

[15] *See id.*, ¶ 334.

[16] *See, e.g.*, Comments of the American Cable Association, WC Docket No. 16-106, at 11-13 (May 27, 2016) ("ACA Comments"); Comments of the National Cable & Telecommunications Association, WC Docket No. 16-106, at 7-13 (May 27, 2016) ("NCTA Comments"); Comments of CTIA, WC Docket No. 16-106, at 16-23 (May 26, 2016). The failure to adequately address these arguments violates "the fundamental canon of statutory construction that the words of the statute must be read in their context and with a view to their place in the overall statutory scheme." *King v. Burwell*, 135 S.Ct. 475, (slip op., at 5) (2015), quoting *Util. Air Regulation Group v. EPA*, 134 S.Ct. 2427 (slip op., at 15) (2015).

[17] 47 U.S.C. § 222(g) (subscriber list information); 222(h)(3) (definition of subscriber list information); 222(c)(1)(B) (carriers may use CPNI derived from the provision of telecommunications services in the provision of "services necessary to, or used in the provision of, such telecommunications service, including the publishing of directories").

[18] *See, e.g.*, Larry M. Eig, Specialist in American Public Law, Congressional Research Service, "Statutory Interpretation: General Principles and Recent Trends," at 13-14 (Dec. 19, 2011).

[19] *See Privacy Order*, ¶¶ 334, 358.

privacy protection, but it changed nothing about the limited scope of section 222 that Congress intended in 1996 when the statute was drafted. The Commission's reliance on a "fill-the-gap" theory to expand its own statutory authority in the absence of any Congressional intent that it do so is clearly erroneous and further proves that the Commission lacks the statutory authority to regulate in this manner.

More to the point, the legislative history of section 222 demonstrates that Congress did *not* intend for that provision to apply to BIAS. As the Commission has recognized, section 222 was drafted to protect certain information to which telephone providers had *unique* access (excluding public and non-sensitive information[20]), while at the same time promoting competition in the telephone services market.[21] In the broadband context, on the other hand, "customer proprietary information" as the Commission has defined the recently invented term often is not uniquely available to BIAS providers.[22] This fact alone demonstrates that Congress did not intend section 222 to apply to BIAS because the thrust of statute is aimed precisely at information that the carrier uniquely possesses about the customer as a result of the carrier-customer relationship. Therefore, section 222 does not authorize the Commission to adopt the

---

[20] *See* 47 U.S.C. § 222(h)(1)(A).

[21] *See Implementation of the Telecommunications Act of 1996, Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as Amended*, CC Docket Nos. 96-115, 96-149, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061, ¶ 37 (rel. Feb. 26, 1998) ("1998 CPNI Order").

[22] Indeed, when consumers use the Internet, their information necessarily is shared with numerous entities throughout the Internet ecosystem, including edge providers, advertisers, and countless intermediaries. *See generally*, Peter Swire, *et al*., *Online Privacy and ISPs*, Working Paper, The Institute for Information Security & Privacy at Georgia Tech (Feb. 11, 2016), http://peterswire.net/wp-content/uploads/Online-Privacy-and-ISPs.pdf.

BIAS rules contained in the *Privacy Order*, and the Commission must reconsider its erroneous decision that section 222 applies by its terms to BIAS.

B. The Commission erred by creating a new category of information to be protected by both BIAS and other telecommunications service providers pursuant to section 222

Even if the Commission had authority to subject BIAS to section 222 requirements, section 222(a) does not provide authority to regulate the Commission-devised and much broader category of "customer proprietary information,"[23] as the *Privacy Order* maintains. The term "customer proprietary information" appears nowhere in the Act and the Commission lacks authority to create it. As ACA argued in an earlier challenge to the Commission's authority under section 222(a), the statutory language, structure, purpose, and legislative history of section 222 make clear that CPNI is the only customer data that section 222 protects, and the Commission's reading of section 222(a) as establishing broad privacy and data security obligations cannot be squared with the clear and more specific provisions of sections 222(b) and 222(c) of the statute.[24]

---

[23] ACA's use of the term "customer proprietary information" in these comments is solely for purposes of addressing the merits of the *Privacy Order* and is not intended to waive any of its legal challenges to the Commission's authority to establish its authority or promulgate rules pursuant to section 222, or to otherwise legitimize the term.

[24] *See* Comments in Support of Petition for Partial Reconsideration of the American Cable Association, *Lifeline and Link Up Reform and Modernization, et al.*, WC Docket Nos. 11-42, 09-197, 10-90, (Oct. 8, 2015) ("ACA Comments in Support of CTIA Petition"). ACA incorporates in full in the Petition for Reconsideration of the *Privacy Order* its comments in support of CTIA's Petition for Partial Reconsideration in the above-referenced proceedings, in which ACA in summary argued, "[n]othing in the Act suggests that the Commission has been delegated authority to impose customer data security regulations beyond those associated with the statutorily defined category of CPNI, and neither Section 222(a) nor the more general mandates concerning common carrier practices in Section 201(b) gives the Commission authority to impose customer data security requirements of any kind." *Id*. at 3. To the extent that ACA's arguments in those comments focused on data security obligations, ACA makes clear here that the Commission does not have authority under section 222(a) to impose *any* of its rules—privacy or data security—on non-CPNI "proprietary information."

Moreover, while Congress has often used the terms "personal information" or "personally identifiable information" in its statutes,[25] it used the term "proprietary information" in section 222 to serve a different and more limited purpose—preventing incumbent carriers from leveraging CPNI already in their possession to control CPNI derived "in one market to perpetuate their dominance as they enter other service markets."[26] The *Privacy Order* impermissibly ignores Congress' choice of terminology, incorrectly conflating "proprietary information" as used in section 222(a) with "personally identifiable information," a term that is relevant only to the separate category of statutorily protected information, CPNI.[27] Because Congress purposely cabined the application of section 222 privacy safeguards to CPNI, the Commission cannot now expand its interpretation of the statute to cover information that Congress clearly did not intend it to address.[28]

C. The Commission's reliance on sections 201 and 202 for authority to impose its adopted privacy and data security rules is also erroneous

Nor do sections 201 and 202 confer upon the Commission the authority it claims in the *Privacy Order*.[29] As ACA has argued, section 201(b) neither imposes privacy or data security

---

[25] Provisions in the Communications Act include section 631, protecting the privacy of cable subscribers' "personally identifiable information," 47 U.S.C. § 551, and a similar provision, section 338(i), protecting the privacy of satellite subscribers' "personally identifiable information," 47 U.S.C. § 338(i).

[26] *1998 CPNI Order*, ¶ 37.

[27] Although the *Privacy Order* argues its interpretation of "proprietary information of, [or] relating to … customers" as broader than CPNI, it fails to justify its categorization of "personally identifiable information" within its definition of "customer PI" and does not address its deviation from Congress' singular use of the term as it pertains to CPNI. *Privacy Order*, ¶ 355.

[28] The Supreme Court has made clear that "[a]n agency has no power to 'tailor' legislation to bureaucratic policy goals" by interpreting a statute to create a regulatory system "unrecognizable to the Congress that designed" it. *Util. Air. Regulatory Grp.* at 2444 (citing Prevention of Significant Deterioration and Title V Greenhouse Gas Tailoring Rule, 75 Fed. Reg. 31514, 31555 (June 3, 2010)).

[29] *See Privacy Order*, ¶¶ 368-70.

requirements on carriers nor gives the Commission authority to impose them.[30] Had Congress granted the Commission authority under section 201(b) broad enough to reach privacy and data security practices of common carriers, it would not have needed to subsequently enact the very detailed set of prescriptions over this same subject matter in section 222. The fact that it did so alone suggests the Commission overreaches in attempting to broadly regulate customer privacy and data security under section 201(b). Indeed, not only did the enactment of section 222 in 1996 itself indicate Congressional recognition that the Commission lacked authority under section 201(b) over privacy and data security, Congress again confirmed the lack of such broad authority under section 201(b) when it later added "location" to the definition of CPNI, explaining that had it not done so, "there [would have been] no protection for a customer's location information."[31]

Section 202, similarly, cannot be read so broadly as to impose privacy and data security requirements on BIAS providers, and in fact, the *Privacy Order* makes no serious attempt to do so.[32] Section 202 prohibits carriers from "mak[ing] any unjust or unreasonable discrimination;" "mak[ing] or giv[ing] any undue or unreasonable preference or advantage;" or "subject[ing] any particular person, class of persons, or locality to any undue or unreasonable prejudice or disadvantage."[33] These provisions have nothing to do with privacy and data security obligations. ACA is unaware of a single prior instance in which the Commission has ever used section 202 in an enforcement action involving alleged privacy or data security violations.

---

[30] *See* ACA Comments in Support of CTIA Petition at 7-9.

[31] *See* Floor Statement Concerning the Wireless Communications and Public Safety Act of 1999, 145 Cong. Rec. H9861 (Oct. 12, 1999) (statement of Rep. John Shimkus).

[32] *See Privacy Order*, ¶¶ 368-370.

[33] *See* 47 U.S.C. § 202(a).

Ultimately, the Commission's authority under sections 201 and 202 cannot overcome the later and more specific limitations on its authority under section 222. Such a limitless view of the Commission's authority would render much of the rest of Title II, with its minutely detailed statutory provisions and related rules, exceptions, and exemptions, largely if not completely superfluous.[34] Indeed, the Commission has long viewed section 222 as a "comprehensive" privacy framework.[35]

Also unavailing is the *Privacy Order*'s attempt to bootstrap the Commission's statutory authority under sections 201(b) and 202(a) to its Open Internet "General Conduct Standard" to give ballast to an interpretation of its sections 201(b) and 202(a) authority that would allow it to reach "'practices that fail to protect the confidentiality of end users' proprietary information' [as] potential carrier practices that are 'unlawful if they unreasonably interfere with or disadvantage end-user consumers' ability to select, access, or use broadband services, applications or content.'"[36] To reach this conclusion, the *Privacy Order* explains that the Commission's "enforcement of sections 201(b) and 202(a) in the context of BIAS finds expression in the 'no unreasonable interference/disadvantage' standard adopted in the *2015 Open Internet Order*."[37]

---

[34] Further, the Commission's suggestion that section 222(a) is designed to serve as a privacy and data security catch-all renders section 201(b) wholly duplicative.

[35] *See Implementation of the Telecommunications Act of 1996, Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as Amended*, CC Docket Nos. 96-115, 96-149, Order on Reconsideration and Petitions for Forbearance, FCC 99-223, ¶ 152 (rel. Sept. 3, 1999) ("the specific consumer privacy and consumer choice protections established in [S]ection 222 supersede the general protections identified in sections 201(b) and 202(a)"); *1998 CPNI Order* ¶ 14 ("Congress established a comprehensive new framework in section 222, which balances principles of privacy and competition in connection with the use and disclosure of CPNI and other customer information [i.e., subscriber list information and aggregate customer information].").

[36] *See Privacy Order*, ¶ 368.

[37] *See id.*

While it is unclear what is meant by the concept of "finds expression" in the context of statutory interpretation, the Commission either has authority over carrier privacy practices under sections 201(b) and 202(a) or it does not. The Commission's speculation in the *2015 Open Internet Order* that these provisions would support an application of the General Conduct Standard in an enforcement action concerning BIAS privacy practices does not itself alter the scope of sections 201(b) and 202(a), and neither confers *any* authority additional to that granted the Commission in section 222 to adopt BIAS privacy rules. The fact that the Commission does not engage in any *ex ante* prohibition of practices involving financial incentives to surrender privacy rights that could potentially run afoul of this standard, apart from the prohibition on "take it or leave it" offerings, as the *Privacy Order* declares, cannot save its BIAS privacy rules from exceeding its statutory authority under sections 201(b) and 202(a) in the first instance.[38] That the Commission exceeded that authority only minimally rather than maximally is beside the point.

Finally, the *Privacy Order's* resort, yet again, to the "gap avoidance" theory of jurisdiction with respect to its sections 201(b) and 202(a) authority fares no better in this section of the order[39] than it did in the sections discussing its section 222 authority.

II. EVEN IF THE COMMISSION HAS AUTHORITY TO ADOPT THE RULES IN THE *PRIVACY ORDER*, THE COMMISSION ERRED BY FAILING TO PROVIDE AN EVIDENTIARY BASIS FOR ITS NEW RULES, DISREGARDING CONTRARY EVIDENCE IN THE RECORD AND FAILING TO CONDUCT A REASONABLE ECONOMIC ANALYSIS OF THE IMPACT OF ITS RULES ON SMALL PROVIDERS

Even if the Commission has legal authority to adopt its new privacy and data security rules, the Commission should reconsider the *Privacy Order* because it fails on several counts to

[38] *See id.*

[39] *See id.*, ¶ 369.

provide an evidentiary basis for its highly prescriptive rules. First, the Commission fails to base its rules on evidence of tangible and material harm to consumers. Second, the Commission fails to give virtually any weight to evidence that BIAS providers have been responsible stewards of their customers' information. Third, the Commission fails to appreciate the harms that its rules would cause to providers and their customers. The result of the Commission's multiple errors will fall hardest on small BIAS providers and their customers, raising costs, inhibiting innovation, and upending consumer expectations.

A. The Commission fails to reasonably consider and weigh evidence (or lack thereof) in the record and instead forges a path based on conjecture without analysis of the harms to consumers and providers

In response to the *Privacy NPRM*,[40] various parties filed data and other evidence demonstrating that many of the Commission's proposed rules lacked factual support.[41] Unfortunately, the *Privacy Order* fails to correct these error by reasonably considering and weighing empirical evidence in the record that many of its rules are unnecessary and would be harmful for consumers and providers alike. In the *Privacy Order*, the Commission assumes that BIAS providers "hold a unique position in the Internet ecosystem" that necessitates prescriptive rules to "bolster consumer trust."[42] However, the Commission, despite having a voluminous record, unreasonably gives little weight, if any, to the lack of evidence of actual consumer harm

[40] *See Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, Notice of Proposed Rulemaking, FCC 16-39 (rel. Apr. 1, 2016) (the "NPRM" or the "Privacy NPRM").

[41] *See, e.g.*, NCTA Comments at 54; Letter from Howard Beales, Professor of Strategic Management and Public Policy, George Washington University Regulatory Studies Center, WC Docket No. 16-106, at 3 (May 27, 2016); Comments of the Association of National Advertisers (ANA), WC Docket No. 16-106, at 9 (May 27, 2016); Comments of T-Mobile, WC Docket No. 16-106, at 11 (May 27, 2016).

[42] *See Privacy Order*, ¶¶ 36-37.

or of evidence that adopting rules that depart from a uniform privacy framework (reflective of Section 5 of the FTC Act) would bolster consumer trust. Instead, the Commission over-weights submissions in the record about provider incentives that make generalized, speculative assumptions that "consumers fearful of the loss of privacy may be less likely to use broadband connectivity."[43] Even worse, the Commission fails to attribute even these unsupported and sweeping suggestions of consumer fear about privacy to the actions of BIAS, as opposed to edge, providers or other players in the Internet ecosystem. Such "unreasoned" analysis makes any decision legally infirm, but it is not surprising since supporters of the *Privacy Order* failed to offer evidence of consumer mistrust or harm that would warrant the new, heavy-handed rules.[44]

At the same time, the Commission fails to give reasonable weight to evidence in the record contradicting its assumptions. Many commenters provided evidence demonstrating that BIAS providers are good stewards of their customers' data. As NCTA explained, for example, BIAS providers have "heightened incentives to safeguard customer data" to preserve trust.[45] Indeed, as the record reflects, most BIAS providers lack the incentives or resources to engage in the sorts of sophisticated analytics that the Commission fears.[46] For example, Comcast noted in

---

[43] See *id.* ¶ 36, n. 62 (citing various commenters).

[44] *See, e.g.*, "Protecting Privacy, Promoting Competition: A Framework for Updating the Federal Communications Privacy Rules for the Digital World, (Feb. 2016) attached to Comments of Public Knowledge et al., WC Docket No. 16-106 (May 27, 2016); Comments of New America's Open Technology Institute, WC Docket Nos. 16-106 and 13-306 (May 27, 2016); Comments of the Center for Democracy and Technology, WC Docket No. 16-106 (May 27, 2016). These key proponents of the Commission's approach proffer no compelling evidence of consumer harm.

[45] *See* Reply Comments of the National Cable & Telecommunications Association, WC Docket No. 16-106, at 26, n. 132 (July 6, 2016) ("NCTA Reply Comments") (citing T-Mobile Comments at 9-10; Comcast Comments at 38-39; CenturyLink Comments at 28).

[46] *See, e.g.*, *Ex Parte* Letter from Patricia Cave, Director Government Affairs, WTA, to Marlene H. Dortch, Secretary, Federal Communications Commission, WC Docket No. 16-106 at 2-3 (Aug. 22, 2016); *see also* Reply Comments of the Rural Wireless Association, Inc., WC Docket No. 16-106 at 2 (July 6. 2016); Comments of WTA, WC Docket No. 16-106, at 19 (May 27,

its comments that "extensive survey data from reputable independent organizations" demonstrates that "consumers consistently trust ISPs with their private information more than other companies in the Internet ecosystem with that information."[47] NCTA, the Electronic Transactions Association, and Consumers' Research all offered additional evidence showing that consumers trust their providers *as much or more* than other players in the Internet ecosystem.[48] Further, contrary to the Commission's unsupported assumption that privacy concerns hinder broadband adoption, NTIA has explained that only a fraction of one percent of consumers cite privacy as the primary reason for non-adoption of broadband.[49]

Not only does the Commission ignore or undervalue this evidence without serious analysis, it also fails to appreciate the harms that its new rules will cause providers and their customers. For example, the *Privacy Order* eliminates providers' ability to rely on implied consent to use "sensitive" customer proprietary information for first-party marketing purposes without reasonably weighing the absence of evidence that such uses fall outside of consumer expectations.[50] As a result, voice and broadband providers will need to incur substantial costs to draft new customer approval forms, redesign customer approval tracking systems, train staff on the new rules, review and potentially renegotiate vendor and third-party agreements to ensure compliance with the new rules, and obtain new customer approvals where the grandfathering

---

2016); Comments of Competitive Carriers Association, WC Docket No. 16-106, at 33 (May 27, 2016); Comments of NTCA, WC Docket No. 16-106, at 1 (May 27, 2016); ACA Comments at 5.

[47] *See* Comments of Comcast Corporation, WC Docket No. 16-106, at 34 (May 27, 2016).

[48] *See* NCTA Reply Comments at 28 (citing ETA Comments at 3; Consumers' Research at 7, 15-16).

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

[50] *See Privacy Order*, ¶¶ 166-234.

exemption does not apply. It also will undermine consumer expectations by requiring opt-in consent in situations where both the FCC and FTC have long argued that consent is implied (*e.g.*, the use of CPNI for first-party marketing).[51] Further, these restrictions on first-party marketing will inhibit broadband investment, undermining a central justification for the new rules.[52] The Commission does not reasonably weigh these harms in adopting its prescriptive rules.

In addition, the Commission fails to reasonably consider that its harm-based data breach notification rule is so vague that it will invariably lead to over-notification by providers and notice fatigue for consumers. The *Privacy Order* adopts a rule under which a carrier must notify affected customers of any data breach "unless the telecommunications carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach."[53] While harm-based triggers may find support in the record, the Commission's definition of harm is so broad as to be essentially unbounded, encompassing "financial, physical, and emotional harm."[54] By including emotional harm as sufficient to trigger a breach notification, the Commission requires providers to engage in needless subjective analysis. Providers will consequently defer toward notification rather than risking enforcement for failure to notify. As a result, providers and customers will be left in the same position as if there were no harm-based

---

[51] *See, e.g.*, *Ex Parte* Letter from Loretta Polk, Vice President & Associate General Counsel, NCTA to Marlene H. Dortch, Secretary, Federal Communications Commission, WC Docket No. 16-106 at 7-8 (Oct. 20, 2016); *Ex Parte* Letter from Jennifer Hightower, Senior Vice President and General Counsel, Cox Communications Inc., to Marlene Dortch, Secretary, FCC, WC Docket No. 16-106 (Oct. 20, 2016); *Ex Parte* Letter from James Talbot, Executive Director-Senior Legal Counsel, AT&T, to Marlene Dortch, Secretary, FCC, WC Docket No. 16-106 (Oct. 17, 2016).

[52] *See, e.g., Ex Parte* Letter from James Talbot, Executive Director-Senior Legal Counsel, AT&T, to Marlene Dortch, Secretary, FCC, WC Docket No. 16-106, at 3 (Oct. 4, 2016) ("AT&T Oct. 4, 2016 *Ex Parte*").

[53] *See Privacy* Order, App'x A (47 C.F.R. § 64.2006(a)).

[54] *See Privacy Order*, ¶ 266.

trigger at all, subjected to an unduly burdensome notification regime unmoored from necessity, precedent, or common sense.

Moreover, the *Privacy Order* errs in assuming that the harm-based data breach notification trigger will "substantially reduce[] the compliance burdens on small carriers."[55] As noted above, the ambiguity of the Commission's harm-based data breach notification trigger is more likely to lead smaller providers, which often lack in-house legal and compliance personnel to conduct regulatory analyses, to notify customers for any breach regardless of potential harm. Not only is this costly for small providers, it raises the specter of notice fatigue and decreased vigilance among customers, which will significantly increase the risk of a breach. As such, this is another error in the Commission's judgment warranting reconsideration.

Ultimately, the rigid, prescriptive framework of the *Privacy Order* is unfortunate because the record offered the Commission a proven, working model for broadband privacy that would have harmonized privacy rules across the Internet ecosystem while minimizing disruptions and harms to providers and their consumers. In advance of and during this proceeding, ACA and others proposed a framework built on the successful "unfair or deceptive acts or practices" standard of section 5 of the FTC Act, which has served as a uniform and flexible framework for the Internet ecosystem for over a decade. The Industry Proposal would ensure a consistent framework for all players in the Internet ecosystem, would offer BIAS providers flexibility to evolve their practices and procedures with changes in the market, and would meet consumers' privacy needs and expectations. Indeed, the record demonstrates that consumers expect their data will be subject to consistent privacy standards based upon a uniform standard regardless of

[55] *Privacy Order*, App'x B, Final Regulatory Flexibility Analysis ("FRFA"), ¶ 71.

which entity in the Internet ecosystem uses that data.[56] Despite receiving broad support in the record, however, the Industry Proposal receives no meaningful discussion in the *Privacy Order*. Because the Commission did not consider the evidence in the record and instead forged a path based on conjecture without analysis of the harms to consumers and providers, it should reconsider the *Privacy Order*.

B. The Commission fails to conduct an adequate economic analysis in crafting its rules which prevented it from considering means to mitigate disproportionate harms to small BIAS providers

While the *Privacy Order* will unduly burden all BIAS providers, the Commission's failure to reasonably consider and weigh evidence in the record and conduct and account for a reasoned economic analysis will result in disproportionate burdens on small providers and their customers. The Office of Advocacy for the Small Business Administration lamented that the Commission's NPRM "failed to comply with the Regulatory Flexibility Act's requirement to quantify or describe the economic impact that its proposed regulations might have on small entities," and "[t]he FCC has provided no estimate of the paperwork hours required to comply with the regulations."[57] Instead, "the FCC simply describe[d] compliance requirements and [sought] comment on compliance costs, without making any attempt to explain what kinds of costs small BIAS providers might incur in order to comply, and without any discussion of how those costs might be disproportionately burdensome for small entities."[58] The *Privacy Order* fares no better.

---

[56] *See, e.g.*, AT&T Oct. 4, 2016 *Ex Parte* (noting that "the expectations of broadband customers are no different from consumer expectations for any other actor in the Internet ecosystem.").

[57] *See* Letter from Darryl L. DePriest, Chief Counsel for Advocacy, U.S. Small Business Administration Office of Advocacy, to Marlene H. Dortch, Secretary, Federal Communications Commission, WC Docket No. 16-106, at 1-2 (June 27, 2016).

[58] *See id.*

As with the NPRM and Initial Regulatory Flexibility Analysis ("IRFA"), the FRFA does not provide a quantifiable/numerical description of the costs of its regulations or suggest that quantification was not practicable or reliable. Neither the text of the *Privacy Order* nor the FRFA even attempt to quantify the costs of the adopted rules, despite the overwhelming evidence in the record that prescriptive rules would be extremely burdensome for small providers.[59] The Commission also fails to estimate the paperwork hours required to comply with its rules. The *Privacy Order* devotes two paragraphs to its FRFA analysis, and nowhere does it meaningfully analyze the burden of the new rules or consider alternative, less burdensome approaches.

The Commission's failure to conduct an adequate impact analysis with respect to small providers creates a stark mismatch between its unfounded assumptions and the reality for small BIAS providers and their customers. For example, the Commission assumes that its choice framework will not be burdensome because "[t]he choice rules are also significantly harmonized with existing rules, with which most small providers currently comply."[60] However, the Commission ignores the fact that the *Privacy Order* significantly modifies its existing choice framework by adopting a sensitivity-based regime, heightening consent requirements and removing existing exemptions. As a result, the changes to the consent rules will require modifications to a BIAS provider's existing consumer choice policies, employee and vendor training materials, and systems for obtaining and tracking customer choices, all at substantial

[59] *See* Reply Comments of American Cable Association, WC Docket No. 16-106, at 7-16 (July 6, 2016).

[60] *See Privacy Order*, ¶ 396.

cost and disruption to providers' business operations.[61] The new rules also will create confusion and frustration among consumers, who will be faced with a new privacy regime out of step with their expectations and a deluge of new consent forms.

Similarly, the Commission assumes that its "reasonableness" approach to data security will mitigate small provider concerns about the cost of the data security requirements.[62] However, while the Commission will consider the size of a BIAS provider when analyzing whether its data security practices are reasonable, as explained above, many small providers will expend even more significant resources—including internal and external legal, compliance, and technical personnel—on an abbreviated timeline to adopt the Commission's "exemplary practices" or face an increased risk of enforcement.

Because of all these FRFA related flaws, the Commission should reconsider its decision to account for the burdens placed on smaller providers by its prescriptive rules and to consider and take steps to mitigate those unreasonable obligations.

III. THE COMMISSION ERRED IN NOT PROPERLY ALIGNING ITS BREACH NOTIFICATION RULES WITH PROVISIONS OF FEDERAL AND STATE LAW

In adopting the breach notification rules, the Commission failed to consider, address, or appropriately balance arguments in the public interest, resulting in rules that overreach in key respects, are burdensome on BIAS providers, especially smaller ones, and are at odds with federal and state law. Accordingly, the Commission should reconsider these rules to at least take the actions identified below.

---

[61] The Commission purports to grandfather customer approvals received before the rules go into effect; however, existing approvals must align with the new rules, which often will not occur.

[62] *See Privacy Order*, ¶ 323.

Despite claims that its rules do not prohibit or impose any constraint on lawful threat information sharing under CISA[63] and that the Commission encourages providers to consider engaging in established information sharing practices,[64] the *Privacy Order* fails to consider and reasonably weigh arguments in the record that its policy choices would establish a significant deterrent to cybersecurity information sharing by BIAS providers and undermine CISA.[65] CISA sought to provide incentives for more and faster cybersecurity information sharing by assuring companies, including BIAS providers, that they would be protected from liability and regulatory enforcement even in certain circumstances where the company inadvertently included unnecessary personal information of its customers in cybersecurity information it shared. The Commission's new rules, however, undermine this goal by requiring BIAS providers to report to regulators and consumers every incident of breach affecting even one person and providing no exception for the inadvertent inclusion of personal information in cybersecurity information that is shared and would entitle the provider to receive liability protection under CISA. The incentives CISA provides to BIAS providers will be much less likely to result in an expansion of cybersecurity information sharing where these providers know that if they undertake the risk of information sharing and make a mistake, they will be required to engage with the Commission on every incident of sharing personal information they did not know was included, even if the Commission is restricted under CISA on what action it can take against them in those

---

[63] *See Privacy Order*, ¶ 246.

[64] *See id.*, ¶ 254.

[65] As ACA warned, but the Commission failed to mention or much less weigh, the Commission could undermine cybersecurity information sharing and, therefore, security, by requiring BIAS providers, especially smaller providers, to disclose to the Commission that they shared personal information where they have liability protection under CISA, and by imposing new requirements on top of state law by requiring a provider to notify consumers of such disclosures even in circumstances where the provider is protected from liability by CISA. *See, e.g.*, ACA Comments at 32-34.

circumstances. Because the Commission undermines the goals of CISA and creates disincentives to cybersecurity information sharing, it should reconsider its decision.

Should the Commission persist in adding new layers of breach notification requirements, there are at least three steps it should take on reconsideration to solve this CISA-related problem and address other public interest problems with its data breach notification rules. First, the Commission should include in its rules a specific exception to new requirements for notification to the Commission and affected consumers for unauthorized access to personal information that a BIAS provider believes in good faith is subject to CISA liability protection. Second, the Commission has insufficient basis to require BIAS providers to report to the Commission breaches that may affect as little as one individual, and, in any event, reporting at that level is outweighed by the associated burdens on providers.[66] Accordingly, the Commission should increase the threshold and should exempt incidents involving a small number of consumers, a strategy that also would reduce the probability that a BIAS provider would ever need to disclose under the new rules the inadvertent inclusion of personal information in threat indicators that it shares under CISA because this is unlikely to affect more than a few consumers in any instance, if it occurs at all. Third, the Commission should reconsider its decision to impose on BIAS providers a new federal consumer notification regime in addition to that imposed under 47

[66] As ACA noted, to the extent the Commission wants to identify, monitor, and address significant trends and vulnerabilities, it can require reporting above a reasonable threshold, not every incident affecting one consumer – a policy it has pursued in other areas, such as outage reporting. *See* ACA Comments at 34, n. 67 (discussing NORS). In contrast, in the *Privacy Order*, the Commission simply asserts that "[W]e expect that this notification data will facilitate dialogue between the Commission and telecommunications carriers and will prove extremely valuable to the Commission in evaluating the efficacy of its data security rules, as well as identifying systemic negative trends and vulnerabilities that can be addressed with individual providers or the industry…" *Privacy Order*, ¶ 276. Neither the Commission nor industry has sufficient resources for, nor do the benefits warrant, a discussion about every incident of unauthorized access affecting a single customer – an issue the *Privacy Order* does not address.

different state laws, especially one that includes new consumer notification requirements even where a BIAS provider has liability protection under CISA. The Commission seems to suggest that any concern about multiple government requirements can be readily addressed by Commission preemption of state laws on a case-by-case basis. But, the Commission ignores that this unrealistic and impractical approach creates significant burdens and confusion for BIAS providers and their customers. These harms will fall hardest on smaller providers, since the cost of engaging in such individual proceedings is very high and the timetable for providers to reconcile state and federal law in the event of a breach is too brief. At a minimum, the Commission should establish clear, easy to apply grounds for the expedited preemption of state laws to satisfy the public interest, reduce confusion, avoid needlessly burdening providers, and to enhance consistency with CISA. In sum, the Commission's burdensome and overreaching requirements are at war with the objectives of CISA, the Congress, the President and even the Commission's own expressed interest in fostering information sharing under CISA.[67]

CONCLUSION

This proceeding went awry from the beginning; the final *Privacy Order*, despite limited attempts to correct the initial flaws, suffers from the same errors that plagued the *NPRM*. It makes material errors on the law. It fails to consider and reasonably weight evidence or acknowledge contrary evidence in the record and does not undertake a reasoned economic and

[67] By failing to harmonize the *Privacy Order* with existing laws, the Commission also sends BIAS providers and the public mixed messages that the President's Commission on Enhancing National Cybersecurity warned against and that has concerned private groups as well. *See* "Report on Securing and Growing the Digital Economy," Commission on Enhancing National Cybersecurity, at 5 (Dec. 1, 2016). *See also, e.g.,* "Dear 45: Let's Make Strides Towards Better Cybersecurity," U.S. Chamber of Commerce (Oct. 18, 2016) *available at* https://www.uschamber.com/above-the-fold/dear-45-lets-make-strides-towards-better-cybersecurity.

FRFA analysis, particularly with respect to impacts on small BIAS providers. It fails to adopt reasonable data breach notification rules that are in sync with other federal government policies and practices. For these reasons, the Commission should reconsider the entire *Privacy Order*, eliminate the adopted rules, and start afresh.

Respectfully submitted,

AMERICAN CABLE ASSOCIATION

Matthew M. Polka
President and Chief Executive Officer
American Cable Association
7 Parkway Center, Suite 755
Pittsburgh, PA 15220-3704
(412) 922-8300

Ross J. Lieberman
Senior Vice President of Government Affairs
American Cable Association
2415 39th Place, NW
Washington, DC 20007
(202) 494-5661

Thomas Cohen
Jameson J. Dempsey
Kelley Drye & Warren LLP
3050 K Street, NW
Suite 400
Washington, DC 20007
(202) 342-8518

Barbara S. Esbin
Cinnamon Mueller
1875 Eye Street, NW, Suite 700
Washington, DC 20006
(202) 872-6811

David S. Turetsky
Akin Gump Strauss Hauer & Feld LLP
1333 New Hampshire Avenue, NW
Washington, DC 20036
(202) 887-4074

Counsel to the
American Cable Association

January 3, 2017