

KELLEY DRYE & WARREN LLP
WASHINGTON HARBOUR, SUITE 400
3050 K STREET, NW
WASHINGTON, D.C. 20007-5108

NEW YORK, NY
LOS ANGELES, CA
CHICAGO, IL
STAMFORD, CT
PARSIPPANY, NJ
BRUSSELS, BELGIUM

AFFILIATE OFFICES
MUMBAI, INDIA

(202) 342-8400

FACSIMILE
(202) 342-8451
www.kelleydrye.com

DIRECT LINE: (202) 342-8518

EMAIL: tcohen@kelleydrye.com

October 4, 2016

Via ECFS

Marlene Dortch, Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: *Ex Parte* Filing of the American Cable Association: *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106

Dear Ms. Dortch:

On September 30, 2016, Ross Lieberman and Mary Lovejoy, American Cable Association (“ACA”) and Counsel to ACA, Barbara Esbin, Cinnamon Mueller, David Turetsky, Akin Gump Strauss Hauer & Feld LLP, and Thomas Cohen, Kelley Drye & Warren LLP, met with Matthew DelNero, Lisa Hone, Daniel Kahn, and Melissa Kirkel (by telephone) from the Wireline Competition Bureau and Peter Shroyer (by telephone) from the Public Safety and Homeland Security Bureau. The purpose of the meeting was to discuss ACA’s views in the above-referenced docket.¹ ACA believes it is essential the Commission strike the proper balance between the interests of consumers in having their privacy protected and data secure and the interests of smaller Internet service providers (“ISPs”) in not being subjected to unreasonably burdensome regulations. For years, these smaller ISPs have been subject to extensive federal and state oversight of their practices to protect the confidentiality of their customers’ information, and they have a commendable track record.

Earlier this year, ACA joined with other ISPs to urge the Commission to adopt privacy and data security regulations consistent with the framework established by the Federal Trade

¹ *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). ACA represents approximately 750 smaller ISPs.

Marlene H. Dortch
October 4, 2016
Page Two

Commission (“FTC”).² Until the Commission’s adoption of the *2015 Open Internet Order*,³ ISP privacy and security practices were overseen by the FTC subject to its Section 5 authority and pursuant to an “unfair and deceptive acts or practices” standard. In general, the FTC regulatory regime was viewed as successful as it protected consumers’ privacy and security without imposing overly burdensome requirements on ISPs. Importantly, it provided oversight under the same standards for all firms operating in the Internet ecosystem and recognized that government requirements needed to adapt as services and market structure evolved. In addition, ACA filed extensive comments in the docket, detailing concerns of smaller ISPs and offering solutions to alleviate them.⁴

ACA representatives began the meeting by expressing appreciation for the Commission’s consideration of concerns raised by ISPs and especially for seeking solutions to concerns raised by smaller ISPs. Nonetheless, even if the Commission adopts rules consistent with the FTC’s framework and establishes a more reasonable and flexible regulatory regime than that proposed in the NPRM, any changes to the FTC’s approach in the Commission’s new *ex ante* privacy rules will impose substantial compliance burdens on smaller ISPs. For instance, these ISPs will need to review existing customer data security and marketing practices, upgrade various operating systems, train personnel, conduct additional risk assessments, revisit relationships with unaffiliated vendors, secure data, and maintain new records.⁵ As a result of this strain on the resources of smaller ISPs, the Commission should include in its order tailored relief for smaller ISPs, including the following, all of which will have at most minimal impact on protecting their customers’ privacy.

² See Letter from Matthew M. Polka, American Cable Association, Steven K. Berry, Competitive Carriers Association, Meredith Atwell Baker, CTIA, Michael Powell, National Cable & Telecommunications Association, and Walter B. McCormick, Jr., USTelecom, to the Honorable Tom Wheeler, Chairman, Federal Communications Commission (March 1, 2016). See also Comment of the Staff of the Bureau of Consumer Protection of Federal Trade Commission, WC Docket No. 16-106 (May 27, 2016).

³ See *Protecting and Promoting the Open Internet*, GN Docket No. 14-28, Report and Order on Remand, Declaratory Ruling, and Order, FCC 15-24 (rel. Mar. 12, 2015).

⁴ See Comments of the American Cable Association, WC Docket No. 16-106 (May 27, 2016) (“ACA Comments”); Reply Comments of the American Cable Association, WC Docket No. 16-106 (July 6, 2016) (“ACA Reply Comments”).

⁵ See ACA Comments at 22-39.

Marlene H. Dortch
October 4, 2016
Page Three

Small ISP Privacy and Data Security Proposals⁶

Proposed Data Security Requirements (Proposed Rule 64.7005)

ACA representatives explained that smaller ISPs work to protect their businesses and their customers' personal information and that virtually all of them have encountered and withstood a variety of cyber exploits. However, unlike large ISPs, smaller providers have few resources and limited staff and expertise.⁷ Instead, to protect against these threats, smaller ISPs often outsource much of their cyber defense and make use of and depend on large managed services providers for security and certain other business needs. As a result, for example, smaller providers should not be expected to do risk assessments that include a detailed review of a large managed service provider. In addition, smaller providers might not have the resources to address promptly any weakness revealed by an assessment. It is reasonable for smaller businesses, consistent with the National Institute of Standards and Technology ("NIST") Cybersecurity Framework and well-established risk management principles, to use their limited resources to concentrate first and foremost on protecting the "crown jewels" and not spread their limited resources everywhere there may be a weakness of lower priority. ACA representatives noted that the other specific requirements listed in the proposed rule pertaining to topics other than risk assessments also are problematic for smaller businesses as discussed in ACA's Comments filed in this matter.⁸

For these and other reasons, any data security rule should be based on "reasonableness" rather than strict liability. Any such rule should state clearly that the resources and size of the ISP will be taken into account in determining reasonableness, and this point should also be included in any discussion about reasonable implementation, whether in the text of the order or in the rule. In addition, the Commission should not include "minimum" "requirements" in the rule, which raise special problems for smaller ISPs because of their limited resources and capabilities. Rather, it should develop guidance or best practices, which permit flexible

⁶ In addition to the proposals discussed herein, the Commission should not require smaller ISPs to deploy a privacy "Dashboard" or encrypt customer personal information. *See* ACA Comments at 26-27, 38-39, 46. Any new rules also should not apply to information received from business customers. *See* ACA Reply Comments at 20-23.

⁷ The Commission's Communications Security, Reliability and Interoperability Council has recognized that smaller ISPs have resource constraints, which can affect their risk management, including allocation of available resources and establishment of priorities as reflected in its March, 2015 report applying the NIST Cybersecurity Framework for this sector. This recognition is also reflected by the Commission's development of the "Small Biz Cyber Planner."

⁸ *See* ACA Comments at 23-28.

Marlene H. Dortch
October 4, 2016
Page Four

compliance by providers of different sizes. By taking an approach that provides guidance based on the different sizes of ISPs and recognizes the relevance of such differences, the Commission would adopt a measure that better comports with sound principles of risk management to lower risks for smaller ISPs and their customers and would reduce unwarranted litigation.

Proposed Breach Notification (Proposed Rule 64.7006)

Data breach notification can be complex and costly for smaller ISPs, especially amidst the challenge of developing an understanding of the event, possibly dealing with a managed services provider, analyzing the genesis of technical issues and other security flaws, and grappling with the existing maze of notice requirements. A recent NIST paper noted that to provide notice, the cost to small businesses is a minimum of \$130 per person or \$130,000 per thousand as reported.⁹ It also is important for the Commission to factor in that 47 state laws already require notice pursuant to a variety of standards and that adding new federal regulatory requirements of consumer notification on top of state laws could be superfluous or confusing to smaller providers and their customers.

In the proposed rule, the Commission is proposing several new notification standards, one requiring companies to provide notice to two parts of the government in different circumstances, *i.e.*, the Commission and law enforcement, and another for providing notice to consumers. This array of notice requirements will tax smaller ISPs, particularly because the proposal requires that notice be given to the Commission on a highly expedited basis (7 days) of a breach of even a single consumer record. In contrast, the Commission is proposing that ISPs provide notice to law enforcement in the same seven days but only if a breach involves 5000 records. As a reference point, the President has proposed a national breach notification standard that would preempt state provisions and was pegged at 30 days. Thus, in a number of respects the Commission is proposing more onerous requirements, yet, it is unlikely to preempt state laws. As a result, in the middle of trying to analyze the genesis and fallout from a breach, smaller ISPs would need to scramble to provide notice to different parts of the government on different but aggressive timetables.

Because of these concerns, ACA representatives suggested alternative notice requirements for smaller ISPs.¹⁰ First, the Commission should be notified by ISPs of breaches only involving a more significant number of records. In other circumstances where the

⁹ Richard Kissel, Hyunjeong Moon, "Draft NISTIR 7621 Rev 1, Small Business Information Security: The Fundamentals," National Institute of Standards and Technology, U.S. Department of Commerce (December 2014).

¹⁰ In addition to adopting ACA's proposals, the Commission should narrow its definition of breach to circumstances where there is actual or a reasonable likelihood of harm.

Marlene H. Dortch
October 4, 2016
Page Five

Commission collects data about important problems, such as outages reportable under the Network Outage Reporting System (NORS), it sets a threshold for reporting that eliminates expedited reporting of small outage events but still enables it to receive ample information to meet its needs.¹¹ Similarly, the Department of Health and Human Services does not require expedited reporting to it of breaches of smaller numbers of records under HIPAA (which potentially involves much more sensitive personal that is of a much higher value on the dark web).¹² ACA representatives proposed that the Commission require smaller ISPs to notify the Commission of a breach only when it involves at least 5,000 records, which is the same threshold it proposes to use as the trigger for providing notice to law enforcement. Second, if the Commission really needs notice of breaches involving fewer than 5,000 records, it could more reasonably require that notice be provided to it at the same time providers give notice to customers (30 days), rather than much earlier. Both of these proposals would simplify and reduce the number of requirements the FCC was proposing for smaller ISPs and permit them to focus on vital issues rather than regulators when it first learns of a breach, but would still enable the FCC to gain information to track trends and understand areas that may need attention.

Effective Date for Smaller ISP Compliance

As discussed above, smaller ISPs share concerns expressed by all ISPs about the burdens associated with the proposed rules, including the proposed notices, customer approval processes, and security requirements, and join their call for the Commission to adopt rules that properly balance the many competing interests, including by reflecting the FTC's framework. Yet, even if the Commission strikes this proper balance, smaller ISPs will have unique compliance issues. First, smaller ISPs will find compliance with the notice, approval, and security requirements to be particularly burdensome. They will need to work with a variety of vendors and consultants to understand the requirements, enter into new agreements, and then, deploy or upgrade systems. Second, because smaller ISPs often use unaffiliated consultants and vendors that need access to customer personal information – including for sales/marketing, billing, installation, and help-desk functions – any new rules should neither prohibit sharing information with these parties nor place burdensome requirements on such sharing and use. ACA representatives proposed the Commission address these concerns by giving smaller ISPs more time to comply with the notice, approval, and security requirements and by enabling smaller ISPs to share information with unaffiliated parties, including vendors, serving as their agents so long as the unaffiliated parties agree to be bound by the rules to the same extent ISPs are bound.

¹¹ 47 C.F.R. § 4.9; Public Safety and Homeland Security Bureau, *NORS*, Federal Communications Commission, <http://transition.fcc.gov/pshs/services/cip/nors/nors.html>.

¹² See “Breach Notification Rule,” U.S. Department of Health and Human Services, www.hhs.gov/hipaa/for-professionals/breach-notification/.

Marlene H. Dortch
October 4, 2016
Page Six

In regard to delaying the effective date of the new rules, ACA has proposed the Commission require smaller ISPs to comply one year after large ISPs are required, which would be after the Office of Management and Budget approves the data collection pursuant to the Paperwork Reduction Act and the Commission posts notice in the *Federal Register*. This will enable smaller ISPs to examine how large ISPs comply and then work with their outside vendors, contractors, and counsel to change their systems. ACA representatives explained that customer privacy would not be put at risk during this period because smaller ISPs are and will remain subject the statutory duty placed on all carriers to protect the confidentiality of proprietary information of, and relating to, their customers and other carriers and equipment manufacturers.¹³ Among other things, ACA suggested that the Commission consider grandfathering customer approvals gained by small ISPs through an opt-out procedure for any customer information deemed to be subject to an opt-in approval process in the new rules during the compliance delay period. ACA representatives noted that the Commission could also provide additional guidance for small ISP compliance with Section 222 by reiterating that its enforcement policy during this period will remain as articulated in the Enforcement Bureau's May 20, 2015 Open Internet Privacy Standard Enforcement Advisory: "broadband providers should take reasonable, good faith steps to protect consumer privacy" and "should employ

¹³ 47 U.S.C. § 222(a). Accordingly, during the period of delayed compliance, the Commission would remain free to use its discretion to initiate an enforcement action if it believes a smaller ISP has violated the statutory commands, regardless of whether the action of the smaller ISP would also violate the new rules. To address the possibility of smaller ISPs being subject to complaints filed by subscribers for violations of the statutory obligations and/or the new rules, ACA representatives suggested that the Commission make clear in the order in this proceeding what standards would guide its review in such cases. Presumably, the Commission would not entertain claims that a small ISP had violated the new rules during the delayed compliance period, but would be required to judge claims for violation of the statute according to some agreed upon interpretation of the statute as applied to the facts of the case. For this reason, the Commission should take care not to suggest in the Order that its interpretation of how Section 222 applies to the provision of broadband Internet access service is the only reasonable interpretation, but rather that it is an interpretation that appropriately furthers "consumer privacy interests and competition, as well as the principle of consumer control," as it has in the past when interpreting the statute for the purpose of developing customer approval requirements. See, e.g., *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, ¶ 87 (rel. Feb. 26, 1998) (interpreting the term "approval" in section 222(c)(1) to be ambiguous and choosing among three separate views in the record as to how to implement the customer approval requirement for use, disclosure or access to CPNI in the Commission's rules).

Marlene H. Dortch
October 4, 2016
Page Seven

privacy protections in line with their privacy policies and core tenets of basic privacy protections.”¹⁴

This letter is being filed electronically pursuant to Section 1.1206 of the Commission’s rules.

Sincerely,



Thomas Cohen
Kelley Drye & Warren, LLP
3050 K Street N.W.
Washington, DC 20007
202-342-8518
tcohen@kelleydrye.com
Counsel for the American Cable Association

cc: Matthew DelNero
Lisa Hone
Daniel Kahn
Melissa Kirkel
Peter Stroyer

¹⁴ Public Notice, FCC Enforcement Advisory, Open Internet Privacy Standard, “Enforcement Bureau Guidance: Broadband Providers Should Take Reasonable, Good Faith Steps to Protect Consumer Privacy,” (rel. May 20, 2015). ACA representatives noted that each BIAS provider is required under the Open Internet Transparency Rule to disclose privacy policies; most ISPs provide brief descriptions of the privacy-related information described in the 2010 Open Internet Order as well as links to their privacy policies in their Open Internet disclosures. *See Preserving the Open Internet*, GN Docket No. 09-151, *Broadband Industry Practices*, WC Docket No. 07-52, Report and Order, 25 FCC Rcd 17905 (2010) (“2010 Open Internet Order”) (Commercial Terms – “Privacy Policies: For example, whether network management practices entail inspection of network traffic, and whether traffic information is stored, provided to third parties, or used by the carrier for non-network management purposes”). Importantly, the Enforcement Advisory affirmed that during the period between the effective date of the Open Internet Order and the adoption of new broadband privacy rules, “the Enforcement Bureau intends to focus on whether broadband providers are taking reasonable, good-faith steps to comply with Section 222 rather than focusing on technical details.” *See 2010 Open Internet Order*, ¶ 2. This approach has been successfully employed for nearly a year and a half, and has provided both useful guidance for providers and adequate protection for consumers.