BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, DC 20554

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

COMMENTS OF THE INTERNET COMMERCE COALITION

Sydney M. White
Jim Halpert
500 8th Street, NW
Washington, D.C. 20004
(202) 799-4441

March 6, 2017

I. Introduction

The Internet Commerce Coalition (ICC), a coalition of major Internet companies, including both ISPs and edge providers, files these comments in support of the Petitions for Reconsideration filed by the American Cable Association, Competitive Carriers Association, CTIA, ITTA – The Voice of Mid-Sized Communications Companies, NCTA – The Internet & Television Association, NTCA – The Rural Broadband Association, United States Telecom Association, the Wireless Internet Service Providers Association, and WTA – Advocates for Rural Broadband, of the Commission's privacy, data breach, and security rules for broadband ISPs[1] (" Broadband Privacy Rules").[2] The Broadband Privacy Rules depart significantly from the FTC's tested, tech-neutral privacy and security framework, which should apply consistently to the same customer information. The ICC urges the Commission to modify the Broadband Privacy Rules and align them fully with the FTC privacy and security regime, which reflects the varying sensitivity of individual data elements.

II. The Rules Reflect an Overly-Expansive Interpretation of Sensitive Data

Privacy and security protection for data should be sensitivity-based and consistent with the FTC's framework across the Internet ecosystem, rather than varying based solely upon regulatory jurisdictional distinctions. The FTC framework limits sensitive information to defined categories, such as financial information, health information, Social Security numbers,

---

[1] *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Report and Order, WC Docket No. 16-106, FCC 16-148, (rel. Nov. 2, 2016) ("Privacy Report and Order").

[2] Many of the points made herein in support of the Petitions for Reconsideration also highlight why the Commission was right to grant the interim stay of new section 64.2005 and should grant the stay petitions in full.

precise geo-location information, and information pertaining to children.[3] The FCC has departed from the FTC's approach, however. The Broadband Privacy Rules recognize those categories of data as sensitive, but go much further.

Specifically, in addition to this truly sensitive data, the Broadband Privacy Rules categorize all web browsing and app usage as sensitive information, which means that a weather update or sports score, or data about the number of times a device used an app is subject to the same approval ("opt-in") and breach notice requirements as a user's health information or Social Security Number. By vastly expanding the categories and quantities of sensitive information, the Broadband Privacy Rules would force ISPs to utilize the same approval requirement for a wide expanse of data, and to devote critical security resources to provide unnecessarily high levels of protection for consumer data that are not sensitive, drawing resources away from protecting data that truly merits enhanced protection, such as financial information, while also harming competition and innovation. This runs counter to the long-standing understanding that data security is best done in a manner that accounts for the sensitivity of the data being protected as outlined in the FTC Start With Security report.[4]

The FCC Broadband Privacy Rules would invent a very different regulatory paradigm for ISPs than the regime that applies to the rest of the Internet ecosystem.[5] Notably, ISPs recently

---

[3] FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers* at 59 (Mar. 2012) ("FTC Privacy Report").
[4] FTC, *Start with Security: A Guide for Businesses* (June 2015), at 23 https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[5] Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106, at 8 (May 27, 2016) ("FTC Comments") imposing different rules is "not optimal". See also FTC Bureau of Consumer Protection Director

announced that they adhere to a voluntary set of privacy and data security principles that are consistent with the time-tested FTC framework.[6] The principles include specific policies on transparency, consumer choice, security and data breach notification. This too counsels in favor of granting the petitions.

III. The Rules Apply an Overly Broad Opt-in Requirement

One of the primary implications of the FCC's overly-expansive interpretation of "sensitive data" is that the Broadband Privacy Rules require ISPs to provide notice and obtain opt-in consent for all web browsing and app usage data regardless of the sensitivity of the data.[7] In contrast, the FTC reserves opt-in consent only for contexts that involve sensitive information.[8] The FTC's framework does not categorically treat all web browsing and app usage data as sensitive information subject to an opt-in consent requirement. Further, the FTC framework does not even suggest that any choice is appropriate for first party data collection and use involving non-sensitive data. In fact, this is the approach that applies throughout the Internet ecosystem today.

The FCC Broadband Privacy Rules would regulate ISPs with an expansive opt-in requirement for Internet advertising, which would apply to *all* customer web browsing and app

---

Jessica Rich, *Keeping up with the Online Advertising Industry*, (April 21, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-online-advertisingindustry raising the concern that departing from the sensitivity approach does not align with consumer expectations.

[6] *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Joint Petition for Stay filed by American Cable Association, Competitive Carriers Association, CTIA, ITTA, NCTA, NTCA, US Telecom Association, the Wireless Internet Service Providers Association, and WTA WC Docket No. 16, (Jan 27, 2017) Appendix A ("ISP Privacy Principles").

[7] 47 C.F.R. § 64.2004(c).

[8] FTC Privacy Report at 47.

usage information an ISP obtains, regardless of the sensitivity of the data.[9] This is an anomaly. No other U.S. regulatory or self-regulatory privacy framework takes this position.

We agree with petitioners that this significant departure provides no consumer benefit since it applies only to a very small portion of the companies holding the data, would create consumer confusion,[10] increase costs,[11] and hamper innovation and ISP choices for consumers,[12] all contrary to long-standing public policy goals reflected in FTC guidance and the 2012 White House privacy report.[13]

IV. Security and Breach Notice Requirements Must Be Commensurate with the Risk of Harm and Based on Reasonableness

Leading ISPs have committed to maintaining privacy and security protections that are consistent with the FTC's effective privacy framework. The FTC has emphasized the need for flexibility in data security, focusing on the most sensitive data, explaining that its approach gives "businesses the flexibility to tailor their programs to their particular circumstances."[14] The Rule instead requires securing an overly broad set of data[15] and requires breach notice for breaches of web browsing and app usage data that are not sensitive.[16] State privacy laws continue to apply to ISPs and states generally have not required breach notice for non-sensitive information. The

---

[9] 47 C.F.R. § 64.2004(c).
[10] Petition for Reconsideration of NCTA – The Internet & Television Association, WC Docket No. 16-106 (filed Jan. 3, 2017) at 2, fn 56 citing to Dissenting Statement on *Privacy Report and Order* of Commissioner Ajit Pai at 3.
[11] Petition for Reconsideration of United States Telecom Association, WC Docket No. 16-106 (filed Jan. 3, 2017) at 2.
[12] Petition for Reconsideration of NCTA at 19-20.
[13] Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (Feb, 2012), https://www.whitehouse.gov/sites/default/files/privacy-final.pdf.
[14] FTC Comments at 27.
[15] 47 C.F.R. § 64.2005.
[16] 47 C.F.R. § 64.2006.

FCC should refine its data breach notification requirement so it is targeted at incidents that are likely to cause consumer harm. As the FTC appropriately observed, overbroad data breach notifications cause consumer fatigue and distract from incidents that warrant a consumer response.[17]

V. Conclusion

The FCC should grant the pending Petitions for Reconsideration to align any requirements with the time-tested FTC privacy and security framework.

Respectfully submitted,

/s/ Sydney M. White

Sydney M. White
Jim Halpert
Counsel to the Internet Commerce Coalition
DLA Piper LLP (US)
500 8th Street, NW
Washington, D.C. 20004
(202) 799-4441

[17] FTC Comments at 31.