The Internet & Television Association
25 Massachusetts Avenue, NW | Suite 100
Washington, DC 20001
(202) 222-2300

Loretta Polk
Vice President &
Associate General Counsel
o (202) 222-2445 e lpolk@ncta.com

October 18, 2016

Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

Re: ***Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106**

Dear Ms. Dortch:

On October 15, 2016, Christi Barnhart of Charter Communications, Frank Buono and Rudy Brioché of Comcast Corporation, Jennifer Prime of Cox Enterprises, Christin McMeley of Davis Wright Tremaine, Christopher Harvie of Mintz Levin, and I met with Nick Degani, Legal Adviser to Commissioner Ajit Pai, to discuss the Commission's broadband privacy proceeding.

We discussed the need to harmonize the FCC's broadband privacy rules with the Federal Trade Commission's (FTC) privacy framework, particularly with regard to the scope and definition of sensitive information. We emphasized that the Commission should refrain from adding new categories of data to the definition of "sensitive information" beyond those already set forth in the FTC's 2012 privacy report. As other commenters in this proceeding have noted, the proposal to include Web browsing data and apps usage data as sensitive information would be especially counterproductive.[1] Consumers benefit from online advertising, individualized content, and product improvements based on this information, and those that wish to forego those benefits are free to opt out of having their data used for such purposes. There is no evidence of consumer harm arising from ISPs utilizing such data subject to opt-out approval when they were governed by the FTC privacy framework. The absence of any demonstrable harm associated with subjecting ISPs to the same choice mechanism for Web browsing and apps usage data as all other Internet entities raises substantial

[1] *See, e.g.*, Letter from Austin Schlick, Google, to Marlene Dortch, Secretary, FCC, WC Docket No. 16-106, October 3, 2016; Letter from Jim Halpert, Internet Commerce Coalition, to Marlene Dortch, Secretary, FCC, WC Docket No. 16-106, October 13, 2016; Letter from American Advertising Federation, American Association of Advertising Agencies, Association of National Advertisers, Direct Marketing Association, Interactive Advertising Bureau, Network Advertising Initiative, to Marlene Dortch, Secretary, FCC, WC Docket No. 16-106, October 10, 2016.

doubts about the lawfulness of the disparate treatment being proposed for that category of customer data.[2]

We also noted the need to exclude content-related exchanges and interactions between an ISP and its customers from being classified as sensitive information. While recognizing the intention of the proposed rules to cover as "sensitive" content of communications that are not intended for ISPs - such as items placed in an Amazon shopping cart or video selections on Netflix - but that are accessible to them in their capacity as providers of broadband access and connectivity, blanket treatment of all content of communications as sensitive information leads to unreasonable results. Customers intend for ISPs to make use of content-related conversations and interactions they have with their ISP – whether they take the form of an email from the customer to the ISP seeking information about a product or service feature, a placement of a modem into a shopping cart on an ISP-affiliated website, or the selection of songs for an ISP-affiliated music streaming service. Categorizing such first-party content-related conversations and interactions as "sensitive" information subject to opt-in consent would be unnecessary and disruptive. It also would interfere with ISPs' ability to employ recommendation engines based upon interactions and transactions with their customers, which the FTC's 2012 report expressly affirmed may be utilized without soliciting customer approval.[3]

Consistent with comments filed by NCTA, Charter, and Comcast, we also discussed the value of adopting an implied consent approach for first-party marketing and advertising activities by ISPs that parallels the FTC framework.[4]

During the meeting, we also expressed support for the three-part standard employed by the FTC for de-identification of information[5] and also argued that IP addresses and other persistent identifiers should not be automatically and categorically classified as CPNI or personally identifiable information.[6] In addition, we noted the importance of ensuring that the

---

[2] *See e.g.,* Supplemental White Paper: A Response to Arguments that the Commission's Proposed Broadband Privacy Rules Would Be Consistent with the First Amendment, Laurence H. Tribe and Jonathan S. Massey, WC Docket No. 16-106, at 5-6 (noting constitutional infirmities associated with FCC's unwarranted departure from FTC's effective and technology-neutral framework and highlighting additional First Amendment scrutiny arising from speaker- and/or content-related distinctions in proposed rules).

[3] Protecting Consumer Privacy in an Era of Rapid Change, FEDERAL TRADE COMMISSION, at 48 (2012) ("FTC Report")("[T]he Commission has previously noted that online retailers and services such as Amazon.com and Netflix need not provide choice when making product recommendations based on prior purchases").

[4] NCTA Comments at 72-74; *Charter Reply Comments at 7, 10;* Comcast Comments at 46-47; Comcast Reply Comments at 30-31. *See also FTC Report* at 40 (2012) ("[M]ost first-party marketing practices are consistent with the consumer's relationship with the business and thus do not necessitate consumer choice"); The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, at 17 (2012).

[5] *See* FTC Report at 21. *See also* FTC Comments at 9 (Scope of FCC's rules should "only include information that is 'reasonably' linkable to an individual" and stating that an unqualified linkable standard "could unnecessarily limit the use of data that does not pose a risk to consumers"); Letter from Jules Polonetsky, CEO, Future of Privacy Forum, to Marlene Dortch, Secretary, FCC, WC Docket No. 16-106, September 12, 2016).

[6] *See, e.g.,* NCTA Comments at 21-23; Comcast Comments at 77-81.

rules permit the use or disclosure of CPNI or PII in connection with monitoring networks for cybersecurity purposes and sharing cyber threat indicators as permitted under the Cybersecurity Information Sharing Act (CISA).

If you have any questions, please contact the undersigned.

Respectfully submitted,

/s/ Loretta Polk

Loretta Polk

cc: Nick Degani