March 7, 2016
Tom Wheeler
Chairman
Federal Communications Commission
445 12th St., SW
Washington, D.C. 20554

Re: Broadband Privacy Rulemaking

Dear Chairman Wheeler:

On March 1, 2016, five large trade associations for broadband Internet service providers ("ISPs") proposed a framework for the Federal Communication Commission's ("FCC") forthcoming rulemaking on broadband privacy.[1] While it is encouraging that ISPs now appear willing to engage on this issue and to recognize the importance of FCC data security and data breach regulations, the proposed framework fails to provide consumers with the robust protections needed in light of ongoing ISP information collection practices. We therefore submit this letter reviewing the collection practices of ISPs across multiple platforms (including their video offerings), and urging the FCC to adopt rules that will provide meaningful protections for broadband consumers.

ISPs currently play a leading role in the complex ecosystem of online behavioral advertising and related forms of data-driven, targeted marketing. These companies are showing an increased interest in monetizing the data they collect about their customers, and they are leveraging their position as gatekeepers to the Internet to harness this data in powerful and invasive ways.

Verizon, for example, has in place powerful data-driven tracking and targeting infrastructure for multiple platforms and devices, including mobile phones. Verizon's acquisition of both AOL and Millennial Media in 2015, as well as its advertising partnership with Microsoft, provide the company with extraordinary capabilities for data gathering, analysis, and monetization of subscriber information.[2]

---

[1] Letter of American Cable Association, Competitive Carrier Association, CTIA, NCTA and USTelecom to Tom Wheeler, Chairman, Federal Communications Commission (Mar. 1, 2016).

[2] Center for Digital Democracy, *Big Data That Watches You Across Platforms* (forthcoming Mar. 2016) [hereinafter "CDD Report"]; Rich McCormick, *Verizon Will Share Your Browsing Habits With AOL's Massive Ad Network*, THE VERGE (Oct. 6, 2015), http://www.theverge.com/2015/10/6/9468025/verizon-will-share-your-browsing-habits-with-aols-massive-ad-network; *AOL to Deepen its Programmatic Leadership with Agreement to Acquire Millennial Media*, MILLENNIAL MEDIA (Sept. 3, 2015) http://www.millennialmedia.com/press/aol-to-deepen-its-programmatic-leadership-with-agreement-to-acquire-millennial-media.

Last year, Comcast announced it would share viewer data collected by its cable set-top boxes with its NBCUniversal media division.[3] As a result, Comcast is now actively involved in the race to build advanced data collection technologies into broadband networks and multi-screen video systems. Through its "Spotlight" advertising service, Comcast provides "multi-screen" targeting, including on mobile devices.[4] In addition to its own intensive research and development efforts, Comcast has also acquired a number of leading advanced advertising and data-targeting companies.[5] Comcast is able to harvest "terabytes of unstructured data" from the set-top boxes it controls, which it then enriches with demographic information to provide data "more meaningful to advertisers," including those targeted via "Comcast's IP-based systems."[6]

Cox Communications offers data-driven, cross-device targeting on television, Internet, and mobile devices. Its targeting capabilities "[l]everage household demographics, like income, ethnicity and home ownership."[7] And through "data partnerships" and related online targeting techniques, Cox gathers additional information about consumers to create highly detailed behavioral profiles.[8]

These consumer tracking and targeted advertising practices are exacerbated by the position of ISPs as gatekeepers to the Internet, which can provide them with a highly detailed and comprehensive view of their subscribers' online communications, personal habits, and daily lives. Moreover, ISPs have access to additional information by virtue of their business relationship with subscribers, such as home addresses, financial information, and credit ratings.

As of April 2015, sixty-five percent of Internet traffic in North America was unencrypted,[9] thereby allowing ISPs expansive access to the content of subscribers' online communications. However, even as websites increasingly adopt encryption to protect privacy, this measure does not eliminate ISP data collection capabilities. Most forms of encryption

---

[3] Shalini Ramachandran & Suzanne Vranica, *Comcast Seeks to Harness Trove of TV Data*, WALL ST. J. (Oct. 20, 2015), http://www.wsj.com/articles/comcast-seeks-to-harness-trove-of-tv-data-1445333401.

[4] *Ad Solutions*, COMCAST SPOTLIGHT, http://www.comcastspotlight.com/ad-solutions/overview.

[5] CDD Report, *supra*; Suzanne Vranica, *Comcast Has Agreed to Acquire Ad Tech Firm Visible World*, WALL ST. J. (June 4, 2015), http://blogs.wsj.com/cmo/2015/06/04/comcast-has-agreed-to-acquire-ad-tech-firm-visible-world; Ryan Lawler, *Comcast is Acquiring Video Ad Company FreeWheel for $320 Million*, TECHCRUNCH (Mar. 1, 2014), http://techcrunch.com/2014/03/01/comcast-freewheel/.

[6] *Comcast Uses MapR for New Advertising Platform That Provides Real-Time Targeted Ads*, MAPR, https://www.mapr.com/resources/comcast-uses-mapr-new-advertising-platform-provides-real-time-targeted-ads.

[7] *Cox Digital Ad Network Solutions*, COX MEDIA, http://www.coxmedia.com/products-and-services/online/cox-digital-ad-network-solutions.aspx.

[8] *Digital VideoX*, COX MEDIA, http://www.coxmedia.com/products-and-services/online/digital-videox.aspx.

[9] *See* Sandvine, *Global Internet Phenomena Spotlight: Encrypted Internet Traffic* 3 (May 8, 2015) https://www.sandvine.com/downloads/general/global-internet-phenomena/2015/encrypted-internet-traffic.pdf.

obscure the content of communications, but the packet headers remain visible.[10] Thus, ISPs would still have access to this metadata, which includes information regarding the time, size, origin, and destination of the communication.[11] HTTPS also does not prevent ISPs from seeing the websites to which a user navigates. Such information can reveal intimate details of the user's lifestyle. Moreover, communications via devices connected to the Internet of Things are largely unencrypted, allowing ISPs access to the information these devices are reporting on their users.[12]

Regardless of encryption, ISPs still receive data related to the frequency, timing, location, and volume of a user's Internet access. This information can reveal intimate details about the subscriber, such as when a user has recently become employed or given birth to a child.

While use of a "virtual private network" ("VPN") also provides additional privacy protections, Americans who utilize free broadband access cannot rely on VPNs to protect their privacy. This is particularly true with respect to low-income Americans and children who use access points maintained by E-Rate recipients, since E-Rate recipients are required to filter for adult content.[13] Moreover, many Internet users do not even know what VPNs are, much less how to use them. Consumers should not be forced to pay for extra precautions to protect their privacy.[14] Privacy should not be reserved for the privileged, and no American should have to choose between Internet access and their privacy.

The invasive and ubiquitous tracking practices of ISPs underscore the imperative for the FCC to exercise the full extent of its rulemaking authority to protect consumer privacy. As it stands, the Federal Trade Commission is simply not equipped to provide meaningful protections for consumer privacy for numerous reasons.

---

[10] *See* Ctr. for Democracy & Tech., *Applying Communications Act Consumer Privacy Protections to Broadband Providers* (Jan. 20, 2016), https://cdt.org/insight/applying-communications-act-consumer-privacy-protections-to-broadband-providers/.

[11] *Id*.

[12] *See* Nick Feamster, *Who Will Secure the Internet of Things?*, FREEDOM TO TINKER (Jan. 19, 2016), https://freedom-to-tinker.com/blog/feamster/who-will-secure-the-internet-ofthings/ (noting several Internet of Things devices transmitting video, ZIP codes, and other sensitive data without encryption); Lorenzo Franceschi-Bicchierai, *Nest Thermostat Leaked Zip Codes Over the Internet*, VICE: MOTHERBOARD (Jan. 20, 2016), http://motherboard. vice.com/read/nest-thermostat-leaked-home-locations-over-the-internet ("Some smart devices have such little computing power that they couldn't perform the necessary encryption processes even if their creators wanted them to . . . .").

[13] *See* 47 U.S.C. § 254(h)(5)(B).

[14] *See* Marc Rotenberg, *Privacy Guidelines for the National Research and Education Network*, NCLIS (1992) ("Users should not be required to pay for routine privacy protection. Additional costs for privacy should only be imposed for extraordinary protection.") *reprinted in* ANITA L. ALLEN & MARC ROTENBERG, PRIVACY LAW AND SOCIETY 762 (2016); *see also* Marc Rotenberg, *Communications Privacy: Implications for Network Design,* 36 Communications of the ACM 61-68 (Aug. 1993).

The FTC's emphasis on the "notice and choice" approach to privacy protections fails to effectively protect consumer privacy. Research shows that consumers rarely read privacy policies; when they do, these complex legal documents are difficult to understand. Moreover, emphasizing notice or disclosure favors the interests of businesses over consumers and fails to establish meaningful privacy safeguards. Nor can industry self-regulatory programs provide meaningful privacy protections when they are not supported by enforceable legal standards.

Even when the FTC reaches a consent agreement with a privacy-violating company, the Commission rarely enforces the Consent Order terms.[15] Moreover, the Commission rarely incorporates public comments into its proposed settlements, which is contrary to public policy and the interest of American consumers. Fundamentally, the FTC is not a data protection agency. Without regulatory authority, the FTC is limited to reactive, after-the-fact enforcement actions that largely focus on whether companies honored their own privacy promises.

Because the United States currently lacks comprehensive privacy legislation or an agency dedicated to privacy protection, there are very few legal constraints on business practices that impact the privacy of American consumers. The FCC has the opportunity to fill this void. In light of the increasingly pervasive tracking practices of ISPs, it is imperative that the FCC take this opportunity to exercise the full extent of its rulemaking authority to protect consumer privacy.

Thank you for your continuing commitment to consumer privacy protection. We look forward to working with you to develop rules to provide meaningful and much-needed protections in this field.

Sincerely,

American Civil Liberties Union
Center for Digital Democracy
Common Sense Kids Action
Consumer Action
Consumer Federation of America
Consumer Federation of California
Consumer Watchdog
Electronic Privacy Information Center
Free Press
New America's Open Technology Institute
Privacy Rights Clearinghouse
Public Knowledge

[15] *See* Compl., *EPIC v. FTC*, 844 F. Supp. 2d 98 (D.C. Cir. 2012) (No. 12-206).