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

May 27, 2016

Re: WC Docket No. 16-106
In the matter of protecting the privacy of customers of broadband and other telecommunications services

Dear Ms. Dortch,

The undersigned organizations are providing these comments in support of the Federal Communications Commission (FCC) proposed rules referenced above. Broadband Internet access services have become essential to Americans' daily lives and providers of those services have a unique role in the online ecosystem. Their position as Internet gatekeepers gives them a comprehensive view of consumers' behavior. Consumers must be able to protect their personal information, and the FCC's authority to ensure that they have the rights and the tools to do so is clear. That is why a broad cross-section of groups representing consumers wrote to FCC Chairman Wheeler earlier this year urging him to move forward on this rulemaking.[1]

The Need for These Rules

Privacy and security are crucial if consumers are to have confidence in using communications services. We have long had protections for the privacy and security of our mail, telegraph and telephone services. There is a clear policy interest in encouraging Americans to avail themselves of broadband Internet services. That interest is undermined by consumers' concerns that their online communications will be exposed or subject to commercial surveillance and used in ways that they do not want or that would unfairly discriminate against them.[2]

---

[1] *See* January 20, 2016 letter from 59 consumer, privacy, and civil rights groups, http://consumerfed.org/wp-content/uploads/2016/01/1-20-16-Broadband-Privacy-Letter-to-FCC-1.pdf, March 8, 2016 letter from the American Library Association, Common Sense Kids Action, and the State Educational Technology Directors Association, https://d2e111jq13me73.cloudfront.net/sites/default/files/uploads/ltr_to_wheeler_school_library_broadband_privacy_3.8.16_1.pdf, and March 15, 2016 letter from Schools, Health & Libraries Broadband (SHLB) Coalition, http://shlb.org/uploads/Policy/Additional%20Policy/SHLB%20Privacy%20Letter%20-%20Final%20.pdf.

[2] *See* March 16, 2016 letter to FCC Chairman Wheeler from privacy and civil rights groups urging the agency to examine the impact that data collection and use could have on historically disadvantaged groups broadband privacy rule proceeding, https://static.newamerica.org/attachments/12815-oti-joins-coalition-urging-fcc-to-consider-civil-rights-principles-for-the-era-of-big-data/20160316%20-%20Broadband%20Privacy%20Letter%20FINAL.fc8649bd9d004e6b848237225e3d9833.pdf.

A recent survey[3] by the Pew Research Center revealed that:

- Ninety-one percent of adults believe that they have lost control of how personal information is collected and used by companies;
- Half of Internet users are worried about the amount of information available about them online;
- Few adults are confident that the records of their activities maintained by various companies and organizations, including phone companies, email providers and cable companies, will remain private and secure;
- Large majorities of adults view their Social Security numbers, the state of their health, the content of their phone conversations, emails and text messages, their physical locations over time, the numbers they have called or texted, their birth dates, their relationship histories, the websites they have visited, and the searches they have made as sensitive information;
- Seventy-four percent of adults say that it is very important for them to be able to control who gets information about them and 65 percent say it is very important for them to control who can collect information about them;
- Eighty-six percent of Internet users have taken steps to mask their digital footprints, and many would like to do more but are unsure how.

The Unique Role of Broadband Internet Access Service Providers

When consumers use broadband services, the data that is necessary to do what they want to do and go where they want to go must pass through their broadband Internet access service (BIAS) providers. BIAS providers can glean very personal information about their customers – their interests, their medical conditions, their financial status, their locations, and other sensitive data – from the websites they visit, the apps and other online services they use, and the messages they send across the Internet.[4]

This gives BIAS providers tremendous insight about their customers and the ability to use it to develop detailed profiles of them. The collection and use of this data is largely invisible to consumers and at present they have no effective control over it. While it is easy to switch the search engines, websites and apps they use, consumers have a relatively small number of BIAS providers to choose from and often get their email

[3] Lee Rainie, *The state of privacy in America: what we learned*, Pew Research Center, January 20, 2016, http://www.pewresearch.org/fact-tank/2016/01/20/the-state-of-privacy-in-america/.

[4] These recent papers explain in detail the unique role of BIAS providers and the data about consumers available to them by virtue of that role: *The FCC's Role in Protecting Online Privacy*, New America's Open Technology Institute, January 2016, https://static.newamerica.org/attachments/12325-the-fccs-role-in-protecting-online-privacy/CPNI__web.d4fbdb12e83f4adc89f37ebffa3e6075.pdf; *Protecting Privacy, Promoting Competition*, Public Knowledge, February 16, 2016, https://www.publicknowledge.org/documents/protecting-privacy-promoting-competition-white-paper.

service and other bundled services from them, making switching less likely. Moreover, consumers' relationships with BIAS providers are different than the relationships that they have with "free" services." They are customers of broadband services and have a reasonable expectation that the personal information that their BIAS providers obtain by virtue of that relationship will not be abused.

The FCC has the Authority and Obligation to Protect Broadband Users

When Congress updated the Communications Act of 1996, with an overwhelming bipartisan majority in both chambers, it added Section 222, which required common carriers to protect the confidentiality of customers' private information and requires customers' opt-in approval, with very few exceptions, to use this information for reasons other than providing the underlying service. Having reclassified broadband as a telecommunications service, the FCC now has the authority to extend that protection to the private information that BIAS providers can obtain as a result of their function as telecommunications services.[5] To fail to do so would be a dereliction of its duty and leave a growing class of communications customers unprotected.

Arguments that the rules are not necessary because there are tools such as encryption and Virtual Private Networks (VPN) are misleading. Most web traffic is not encrypted, and even encrypted data can reveal detailed information about consumers' behavior. VPNs are usually paid services and their use is not likely to be widely adopted.[6]

The argument that the FCC's proposal is unfair because other kinds of businesses in the online ecosystem that collect and use consumers' personal data would not be covered by the rules ignores the unique position of BIAS providers and the vast expansion of their commercial surveillance, without having to give their customers meaningful control.[7] The result of heeding this argument would be a continued race to the bottom, where there are no limits for what anyone does except those set in voluntary privacy policies.[8]

The FCC does not need to find that others in the online ecosystem are also a threat, or a bigger threat, to act, nor must it harmonize its approach with the FTC, which does not

---

[5] The papers by New America's Open Technology Institute and Public Knowledge, *supra*, provide detailed explanations of the FCC's authority in this regard.

[6] *See* letter from Princeton Professor Nick Feamster, http://ftt-uploads.s3.amazonaws.com/fcc-cpni-nprm.pdf, and report from Upturn, https://www.teamupturn.com/reports/2016/what-isps-can-see, correcting inaccuracies and omissions in industry-funded report about the limitations of the personal information available to BIAS providers.

[7] *See Big Data is Watching: Growing Digital Data Surveillance of Consumers by ISPs and Other Leading Video Providers*, Center for Digital Democracy, March 2016, https://www.democraticmedia.org/sites/default/files/field/public-files/2016/ispbigdatamarch2016.pdf.

[8] *See* March 3, 2016 blog by Jay Stanley, Senior Policy Analyst, ACLU Speech, Technology and Privacy Project, https://www.aclu.org/blog/free-future/carriers-pushing-weak-arguments-against-fcc-privacy-protection.

have jurisdiction over common carriers.[9] It has the obligation to protect broadband customers' privacy and security. The states and the U.S. Congress should take action to ensure that consumers' privacy and security are adequately protected in areas that the FCC rules do not cover.

Opt-in is the Right Approach

We urge the FCC to prohibit BIAS providers from using customer data or sharing it with others, except to provide the broadband service or to offer upgrades to that service without specific opt-in permission from their customers. Customers' private information should not be used or shared for *any* other purposes without their express, affirmative consent.

Where the default lies matters; "opting out" puts the burden on consumers to take extra steps to avoid something that they do not want. Academics argue that consumers have difficulty exercising choice because they lack the same level of knowledge as the data holder about exactly how their personal information may be used; moreover, they may believe that they may make certain erroneous assumptions about their rights or companies' practices.[10]

It should be up to the BIAS provider to make a compelling argument for the benefits of opting in. Opting in should never be presented as a requirement to obtain service. The consequences of opting in should be clearly and completely explained and, on that basis, if customers want to receive information about other communications-related services or any other services they will agree. Consent must be verifiable and easy for customers to revoke at any time. BIAS providers should be obliged to comply fully with customers' choices.

Standardized formats for providing consumers with the information they need to make informed decisions about whether to opt in would be helpful. The challenges of providing effective privacy notices have been studied extensively and we urge the FCC to consult with experts in this regard.[11]

---

[9] *See* March 14, 2016 letter to FCC Chairman Wheeler from Free Press, http://www.freepress.net/sites/default/files/resources/section_222_common_carrier_principles_and_industry_reply_march_14_2016_final.pdf.

[10] *See* Chris Jay Hoofnagle and Jennifer M. Urban, Berkeley Law, *Alan Westin's Privacy Homo Economicus*, 19 Wake Forest L. Review 261 (2014), http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=3399&context=facpubs.

[11] *See* for instance Florian Shaub, Carnegie Mellon University; Rebecca Belabako, Rand Corporation; Adam L. Durity, Google; Lorie Faith Cranor, Carnegie Mellon University, *A Design Space for Effective Privacy Notices*, USENIX Association 2015 Symposium on Privacy and Security, https://www.usenix.org/system/files/conference/soups2015/soups15-paper-schaub.pdf.

The FCC should make clear that the opt-in requirement applies to BIAS providers, their affiliates and their business partners in regard to the use of customers' data that is collected by the BIAS providers by virtue of providing broadband services to those customers. Use of data that is collected from other sources would not be covered by these rules.

Consumers should not Pay for Privacy or Agree to Put Certain Data at Risk

Notice, even if done well, is not enough, however. There are some practices that simply should not be allowed. Because consumers' Social Security numbers are the keys to their identities and the harm that can be caused if that information is compromised is so great, BIAS providers should not be allowed to ask for Social Security numbers or share them except as necessary to provide the broadband services that the consumers have requested.

Consumers also should not be asked to pay to protect their privacy. A recent survey showed that most Americans do not feel that trading their privacy for a discount is a fair deal.[12] It is not. Tempted by the lure of a bargain, consumers may not take the time to understand and consider the consequences of opting in. Furthermore, for consumers who are struggling financially, it is not really a free choice. Pay-for-privacy would create a two-tier system in which consumers who can afford privacy will get it, and those who cannot will not. It is runs contrary to the public policy goals of inclusion and bridging the digital divide.

Broadband Customers' Data Must be Secure

Strong security protections are crucial to protecting consumers' data from breaches. Given the inherently sensitive nature of communications data, BIAS providers must be required to follow strict rules to safeguard customer information from unauthorized use or disclosure and to take full responsibility for the protection of customer information when it is shared with third parties.

Since, as with privacy, the U.S. lacks a comprehensive legal framework on data security, it is incumbent on the FCC to use its rulemaking authority to ensure that BIAS providers analyze their data security risks, implement data security systems, train the appropriate staff, regularly perform tests, designate responsible personnel, have a breach response in place, and notify customers promptly if a breach occurs.

---

[12] Joseph Turow, Ph.D., Annenberg School of Communication, University of Pennsylvania; Michael Hennessy, Ph.D., Annenberg Public Policy Center; Nora Draper, Ph.D., University of New Hampshire, *The Tradeoff Fallacy*, June 2015 https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf.

We applaud the FCC for its thoughtful analysis of the issues and the many questions that it has posed in this proceeding, to which some of us will be responding in greater detail in further comments. We strongly urge the FCC to continue to move forward as expeditiously as possible to put in place meaningful privacy protections and control for broadband Internet users.

Signed by the following organizations:

Access Humboldt
Access Sonoma Broadband
Ashbury Community Services, Inc. (dba) Ashbury Senior Computer Community Center
Benton Foundation
Coalition for Transparency, Clarification & Simplification of Regulations Pertaining to American Broadcasting
Consumer Federation of America
Consumer Federation of California
Demand Progress
Massachusetts Consumers Council
National Consumer Law Center (on behalf it its low income clients)
National Consumers League
National Digital Inclusion Alliance
Online Trust Alliance
Privacy Rights Clearinghouse
U.S. PIRG
Virginia Citizens Consumer Council
World Privacy Forum
X-Lab