MASSACHUSETTS
40 main st, suite 301
florence, ma 01062
tel 413.585.1533
fax 413.585.8904

WASHINGTON
1025 connecticut ave. nw, suite 1110
washington, dc 20036
tel 202.265.1490
fax 202.265.1489

freepress
www.freepress.net

March 14, 2016

Chairman Tom Wheeler
Federal Communications Commission
445 Twelfth Street SW
Washington, D.C. 20554

Dear Chairman Wheeler:

In 2015, the Commission returned to the proper interpretation of the Communications Act when it rightly reclassified broadband Internet access as a telecommunications service. Restoring the proper common carrier framework for broadband Internet access service, under Title II of the Communications Act, was a welcome and necessary step towards protecting Internet users' rights to just and reasonable service. That includes, but is by no means limited to, the right to reasonably nondiscriminatory service now enshrined in the Net Neutrality rules.

When it reclassified, the Commission also recognized carriers' serious "mandate" under the law to "to protect the confidentiality of [their] customers' proprietary information."[1] As the Commission explained, "[c]onsumers' privacy needs are no less important when [they] communicate over and use broadband Internet access" than when they use telephones or other telecom services.[2] And just as carriers have no right to block, degrade, or otherwise interfere with the information that their customers choose to send and receive, these carriers have no right to misuse for marketing or other purposes the private information they obtain through their provision of broadband service.

Free Press applauds the Commission's ongoing work to promulgate appropriate broadband privacy rules under Section 222 of the Act and related provisions in Title II.[3] The *Open Internet Order* declined to forbear from applying Section 222, but stipulated the commencement of a proceeding to implement rules specifically for broadband Internet access service.[4] Internet users want and need these kinds of updated safeguards in place to protect their private information from unauthorized disclosure and abuse.

---

[1] *Protecting and Promoting the Open Internet*, GN Docket No. 14-28, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601, ¶ 53 (2015) ("*Open Internet Order*").

[2] *Id.*, ¶ 54 (quoting *Appropriate Framework for Broadband Access to the Internet Over Wireline Facilities et al.*, CC Docket No. 02-33, Report and Order and Notice of Proposed Rulemaking, 20 FCC Rcd 14853, ¶ 148 (2005)).

[3] *See* "Chairman Wheeler's Proposal to Give Broadband Consumers Increased Choice, Transparency & Security With Respect to Their Data," Fact Sheet (rel. Mar. 10, 2016), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DOC-338159A1.pdf ("Fact Sheet"); *see also FCC Enforcement Advisory, Open Internet Privacy Standard*, Public Notice, DA 15-603 (rel. May 20, 2015).

[4] *See Open Internet Order*, ¶¶ 462-63.

However, the same broadband providers and their trade associations that continue fighting the *Open Internet Order* are also spreading confusion and misinformation about the Commission's obligation to protect consumer privacy under Section 222. While Free Press has joined letters submitted over the course of the last several weeks emphasizing the need and the popular support for such broadband privacy safeguards,[5] we write separately today to highlight several fundamental flaws in the industry's lobbying efforts.

On February 11, these broadband industry associations and allies sent your office a letter of their own, urging this Commission to adopt an FTC-style privacy framework focused on "prohibiting unfairness and deception" in order to "harmonize" FCC and FTC privacy enforcement.[6] Yet mimicking the FTC and drawing on another agency's authorizing statute instead of your own would accomplish neither of these objectives.

The ISP Letter urges far weaker rules than those for which this Commission has statutory authority, and it ignores Congress' stated aims in the Communications Act. It misleadingly conflates ISPs with edge providers to suggest this Commission has no role to play in protecting privacy for common carrier customers, while misreading several reports including the FCC's 2010 National Broadband Plan. And it misrepresents the FTC's complementary role in privacy enforcement with specialized agencies.

We write to refute these claims and encourage the FCC to move forward with strong privacy safeguards in keeping with its statutory mandate.

Congressional Mandate on Telecommunications Privacy

The ISP Letter glosses over the reason that this Commission must take strong action on communications privacy: Congress required it in the Communications Act. The Congressional directive to the FCC is unambiguous:

> Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information [CPNI] by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of [same].[7]

---

[5] *See* Letter from Access Now *et al.* to Chairman Tom Wheeler, Jan. 20, 2016, *available at* http://www.freepress.net/sites/default/files/resources/broadband_privacy_letter_to_fcc.pdf; Letter from American Civil Liberties Union *et al.* to Chairman Tom Wheeler, Mar. 7, 2016, *available at* https://www.democraticmedia.org/sites/default/files/field/public-files/2016/broadband_privacy_letter_to_fcc_3.7.16_final.pdf.

[6] Letter to Tom Wheeler, Chairman, FCC, from the American Cable Association, Consumer Technology Association, Internet Commerce Coalition, Competitive Carriers Association, CTIA, National Cable & Telecommunications Association, and U.S. Telecom Association, Feb. 11, 2016 ("ISP Letter").

[7] 47 U.S.C § 222 (c)(1); *see also id.* § 222(a) (requiring carriers to protect the confidentiality of other proprietary customer information in addition to CPNI); *id.* § 201(b) (requiring that all carrier practices be just and reasonable).

In the statute, Congress outlines how CPNI and other private information ought to be used by telecommunications carriers: via an opt-in approach that limits the use of such information to provision of the service, with few exceptions.

When the FCC restored its Title II authority, that action rightly brought broadband Internet access service providers under Section 222's ambit. The question before the FCC is about defining the scope of CPNI and other proprietary information in the context of broadband Internet access – not whether the FCC should do so, but how. The need for such bright-line rules is not just a policy judgment for this Commission to make – least of all by weighing whether ISPs have purportedly greater or lesser access to private information on the Internet than do other entities. The command to protect the privacy of carriers' customers is well established by Congress in the operative statutes.

ISPs in the "Internet Ecosystem"

Broadband Internet access service providers continually compare themselves to websites, apps, and over-the-top services, lumping themselves in with such so-called "edge providers" in order to obfuscate their unique position within the "Internet ecosystem." It may well be true that these ISPs are part of the same personal information market in which many edge providers take part. They often sell consumer information to the same data brokers, and the ISPs' use of such data implicates many of the same privacy concerns as the edge providers' use does.[8] However, ISPs' role as gatekeepers to the Internet and the lack of competition in the market subjects them to a higher standard, per Congress's mandate that the FCC protect common carrier customers' privacy.

As the *Open Internet Order* explains, "[b]roadband providers function as gatekeepers for both their end user customers who access the Internet, and for various transit providers, CDNs, and edge providers attempting to reach the broadband provider's end-user subscribers."[9] And as the Commission's preliminary Fact Sheet for this proceeding reiterates, "[a] consumer's relationship with her ISP is very different than the one she has with a website or app," because "[a]n ISP handles all of its customers' network traffic."

Consumers have little choice when it comes to their broadband service provider. When choosing which search engine, e-mail service, or social media to use, people can make some conscious decisions to access those that reflect their privacy preferences. Absent strong privacy protections for ISPs, privacy-conscious consumers lose all agency when trying to protect their privacy online – even if they use encryption and other measures that shield some but by no means all information and CPNI from ISPs' view. [10]

---

[8] Stacey Higginbotham, "ISPs really, really want to be able to share your data," *Fortune*, April 28, 2016, *available at* http://fortune.com/2015/04/28/isps-share-your-data/.

[9] *Open Internet Order*, ¶ 78.

[10] *See* Upturn, "What ISPs Can See: Clarifying the Technical Landscape of the Broadband Privacy Debate" (Mar. 2016), *available at* https://www.teamupturn.com/reports/2016/what-isps-can-see.

Thus the question before this Commission is not whether Internet users also deserve protections from privacy-invasive edge providers, nor whether cable and telecom companies are better or worse on privacy than search engines and social media sites. The question is how the FCC can fulfill its mandate to protect CPNI and other proprietary information collected and used by ISPs.

Any comprehensive federal data privacy framework must begin with broadband providers, over whose practices the FCC has clear jurisdiction. Future FTC action or joint FCC/FTC actions make little sense if broadband providers with access to detailed customer information are selling CPNI and other proprietary information to data and ad brokers. The fact that ISPs may be an integral part of the same questionable enterprise as edge providers is a reason to fulfill Congress's mandate for FCC regulation of carriers, not a reason to engage in a regulatory race-to-the-bottom on American privacy protections.

The Role of the FTC

As Public Knowledge and others have documented, the FTC and FCC have complementary roles in privacy protection.[11] Public Knowledge argued that while federal privacy policy may operate with the FTC at the center, other agencies properly regulate specific industries like healthcare and finance. Complementary rules between sectors of the banking and finance "ecosystem" serve to enhance consumer privacy, not weaken it.

The FCC-FTC Memorandum of Understanding ("MOU") on consumer protection[12] recognizes this dynamic and the differing jurisdiction in each agency's governing statute. The MOU promises that the agencies will work together in joint actions to best protect consumers, not to simply harmonize their approaches and cater to industry as requested by the ISP Letter. And as FTC Commissioner Brill has rightly recognized, there is plenty for the FTC to do in safeguarding people's privacy against the purveyors of "apps, edge services, ad networks, advertisers, publishers, data brokers, analytics firms, and the many other actors whose data practices" impact Internet users.[13]

In a follow-up letter on March 1, the industry associations doubled down on urging the FCC to adopt an "unfairness and deception" regulatory model and recommended that the FTC and FCC avoid duplicative oversight.[14] Despite the industry

[11] Public Knowledge, Protecting Privacy, Promoting Competition, A Framework for Updating the Federal Communications Commission Privacy Rules for the Digital World, Feb. 2006, *available at* https://www.publicknowledge.org/documents/protecting-privacy-promoting-competition-white-paper.

[12] FCC-FTC Consumer Protection Memorandum of Understanding, Nov. 16, 2015, https://www.ftc.gov/system/files/documents/cooperation_agreements/151116ftcfcc-mou.pdf.

[13] Commissioner Julie Brill, "Net Neutrality and Privacy: Challenges and Opportunities," Speech to Georgetown Institute for Public Representation and Center for Privacy and Technology, at 4 (Nov. 19, 2015), https://www.ftc.gov/system/files/documents/public_statements/881663/151119netneutrality.pdf.

[14] Letter to Tom Wheeler, Chairman, FCC, from the American Cable Association, Competitive Carriers Association, CTIA, National Cable & Telecommunications Association, U.S. Telecom Association (March 1, 2016).

associations' insistence on the success of the FTC's enforcement model, merely providing consumers with notice of a company's intent to sell their information does little to provide them with real protection. Relying solely on the unfairness and deception regime ignores the disparate impacts that data collection and targeted advertising can have on disadvantaged populations.[15]

Prior FCC Reports and Related Recommendations

In a last-ditch effort to bolster their case, the ISP Letter incorrectly cites several government reports that supposedly support their FTC/FCC harmonization claims. But these claims find no support in these reports. For instance, the 2010 National Broadband Plan recognized several unique harms that broadband providers pose in regards to consumer privacy. As the Plan stated, the "[i]ncreased use of personal data raises material privacy and security concerns" for broadband users.[16] It recognized the anti-competitive nature of customer data collection in the broadband market[17] and acknowledged that privacy concerns can be a "barrier to the adoption and utilization of broadband."[18]

Far from supporting the type of harmonization of FTC and FCC rules imagined by the ISP Letter, however – or the weakening of FCC rulemaking authority inherent in any such "harmonization" efforts – the National Broadband Plan recommended maintaining and clarifying the agencies' dual roles to protect consumer privacy. It noted that the FCC "typically works with the providers of broadband access to the Internet – phone, cable and wireless network providers – and the Communications Act contains various provisions outlining consumer privacy protections," and expressed concerns about "ISPs operating in an unregulated environment."[19]

Fortunately, the FCC has now clarified that broadband Internet access service is indeed a telecom service, and that it does not fall into an unregulated twilight zone. While the Plan recommended that "[t]he FCC and FTC should jointly develop principles to require that customers provide informed consent before broadband service providers share certain types of information," that suggestion was offered up in a time when each of these agency's jurisdiction over broadband Internet access service remained unclear. The *Open Internet Order* and reclassification decision remove that uncertainty.

---

[15] Federal Trade Commission, "Big Data a Tool for Inclusion or Exclusion," (January 2016), *available at* https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.

[16] Federal Communications Commission, *Connecting America: The National Broadband Plan,* 17 (Mar. 17, 2010), *available at* http://download.broadband.gov/plan/national-broadband-plan.pdf.

[17] *Id.* at 53.

[18] *Id.*

[19] *Id* at 54.

Likewise, the White House 2012 Privacy Report[20] emphasizes individual control, transparency, and respect for context when it comes to regulating online privacy. None of these approaches suggest ignoring the plain reading of the Communications Act and using arbitrarily weaker privacy regulations. And while the FTC may be well suited for other Internet user privacy issues, its authority to protect against "unfair and deceptive" practices cannot proactively provide this kind of user control.

Conclusion

Again and again, the ISP Letter states that broadband providers are committed to their customers' privacy. However, there are ongoing privacy abuses by such providers that undermine that simple assertion. First, the privacy policies of nearly all broadband providers acknowledge that certain personally identifiable information and CPNI is shared with marketers and other entities, without necessarily first obtaining broadband users' consent, thus raising serious privacy concerns. Secondly, there have been concrete abuses of privacy by ISPs. Just last week, the FCC found the Verizon "super cookie" to be a serious violation of consumer privacy requiring remedies under Section 222.[21]

As a matter of policy, harmonizing FCC and FTC enforcement only would serve to weaken enforcement. Industry has consistently lobbied to weaken the FTC's enforcement power and preclude that agency from gaining more ability to engage in rulemaking. Broadband providers are content to muddy the waters, misstate facts, and seek a weak regime that allows them to expand their use of private information.

Under a common carriage framework, the FCC's course of action is clear. Abide by the congressional mandate to protect CPNI and other private information by commencing a strong rulemaking, starting with an opt-in approach for using consumer data for any purpose other than providing broadband service. Charting a better course on Internet privacy must begin by dealing with the broadband gatekeepers to whom consumers are particularly vulnerable, and against whom consumers have the least power to effectuate their privacy preferences in the marketplace.

Respectfully submitted,

/s/ Gaurav Laroia
Policy Counsel
202-265-1490
glaroia@freepress.net

[20] The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (Feb. 2012), *available at* https://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[21] *In the Matter of Cellco Partnership, d/b/a Verizon Wireless*, Consent Decree, DA 16-242 (rel. Mar. 7, 2016), http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0307/DA-16-242A1.pdf.