Before the

Federal Communications Commission

Washington, DC 20554

In the Matter of	**)**	
	)	
Restoring Internet Freedom	**)**	**WC Docket No. 17-108**
	)	
	)	

REPLY COMMENTS OF THE NATIONAL CONSUMERS LEAGUE

August 30, 2017

Executive Summary

The National Consumers League ("NCL") reiterates its opposition to the proposed Federal Communications Commission's ("FCC") rules that would reclassify Internet Service Providers ("ISPs") as Title I information services. Because this reclassification would result in a significant decrease in data security protections for consumers, NCL urges the FCC to retain both the Title II classification of ISPs and jurisdiction over data security and privacy matters.

In our reply comments, NCL responds to various statements in the record made by interested parties in response to the Commission's Notice of Proposed Rulemaking (NPRM) regarding "Restoring Internet Freedom."[1] We reiterate that the protection of consumers' data security has been, and should continue to be, one of the FCC's top priorities. Furthermore, we argue that the FCC is uniquely positioned with its civil penalty authority and its ability to promulgate *ex ante* regulations to achieve this goal. NCL firmly believes that the classification of ISPs under Title II is the correct classification and should remain in place.

Despite what some commenters claim, Title II is the best avenue for protecting consumer data security under the jurisdiction of the FCC. The lack of competition among ISPs in almost all areas of the country, and especially in rural and low-income areas, makes it practically impossible for market forces to have any meaningful impact on regulating ISPs privacy and data security practices.

We reiterate that a secure Internet is the only way for innovation and engagement to thrive. The protection of consumer data is a critical component in ensuring a maximization of economic and democratic participation of the Internet. As a unique player in this arena, ISPs are

[1] Restoring Internet Freedom, WC Docket No. 17-108, Notice of Proposed Rulemaking, FCC 25, (rel. Apr. 27, 2017), available at https://apps.fcc.gov/edocs_public/attachmatch/FCC-17-60A1_Rcd.pdf, *(Restoring Internet Freedom NPRM).*

privy to enormous amounts of consumers' most sensitive data.[2] Holding ISPs to a high standard in regards to their handling of this data is best accomplished by retaining the current Title II classification. A policy reversal would decimate the important progress that has been made in creating a safer Internet since the initial reclassification in 2015.

[2] Public Knowledge and Common Cause, *Comments of Public Knowledge and Common Cause in the Matter of Restoring Internet Freedom,* July 19, 2017, 90, https://ecfsapi.fcc.gov/file/1071932385942/PK%20CC%20Updated%20Comments%20with%20Appendices%20FINAL.pdf.

Introduction

The National Consumers League respectfully submits these reply comments to the Federal Communications Commission in the above captioned proceeding.[3] This issue has garnered unprecedented levels of public input, with over 16 million comments submitted to the FCC in the two month comment period. Commenters are overwhelmingly opposed to the proposed rules.[4] This level of public engagement underscores the importance not only of the open Internet, but of strong data security protections.

NCL is America's pioneering consumer advocacy organization. Since our founding in 1899, our nonprofit mission has been to promote social and economic justice for consumers and workers in the United States and abroad.[5] NCL is the home of Fraud.org, a website dedicated to giving consumers the information they need to avoid becoming victims of telemarketing and Internet fraud. NCL's #DataInsecurity Project is an advocacy campaign to raise consumer and policymaker awareness about the need for strong data security standards and a comprehensive national data breach notifications law.

NCL reiterates our belief in the need for the FCC to maintain Title II classification for Internet Service Providers. NCL's initial comments, and these reply comments, closely examine the data security and enforcement provisions of the NPRM. These issues are of great importance to our fraud prevention work as more than half of fraud losses occurring in 2016 came from data breach victims.[6] NCL believes that data security is a crucial component of privacy and fraud

---

[3] NCL wishes to acknowledge the invaluable contribution of NCL's Public Policy Manager Brian Young and Google Public Policy Fellow Rachel Gallagher (Washington and Lee University '18) in producing these reply comments.

[4] Ali Breland, *Dems press FCC to extend net neutrality comment period,* The Hill, August 3, 2017, http://thehill.com/policy/technology/345175-senate-dems-press-fcc-on-giving-public-more-time-to-comment-on-net.

[5] National Consumers League, *Mission,* http://www.nclnet.org/mission (last visited June 19, 2017).

[6] Javelin Research, *2017 Data Breach Fraud Impact Report: Going Undercover and Recovering Data*, June 14, 2017, https://www.javelinstrategy.com/coverage-area/2017-data-breach-fraud-impact-report-going-undercover-and-recovering-data.

prevention.[7] We believe that maintaining the Title II classification of ISPs is the best way to promote data security.

I. The FCC is best situated to protect data security

The FCC's proposed rules contemplate "return[ing] jurisdiction over Internet service providers' privacy practices to the FTC," a move widely condemned by most major consumer advocacy organizations.[8] By relinquishing its authority in this space, "the FCC would not only turn a blind eye to its own expertise on communications networks but would also rob consumers of their sole privacy cop on the beat with that expertise."[9]

Many industry commenters laud the FTC as the expert agency in this arena. However, while the FTC is an admirable protector of consumers, this analysis fails to account for the FTC's limited resources and experience in the realm of data security regulation for ISPs.[10] Unlike the FCC, the FTC has no ability to preempt consumer harms by engaging in *ex ante* regulatory intervention. Instead, the FTC must stand by and watch as harms are committed, and work to address the harm after the fact. As stated in our initial comments, and echoed by the Center for Democracy & Technology, sensitive information such as Social Security numbers and

---

[7] National Consumers League, *Comments of The National Consumers League in the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services,* May 27, 2016, https://ecfsapi.fcc.gov/file/60002078689.pdf.

[8] Alina Selyukh, *Internet Companies Plan Online Campaign To Keep Net Neutrality Rules,* NPR, July 11, 2017, http://www.npr.org/sections/alltechconsidered/2017/07/11/535804285/internet-companies-plan-online-campaign-to-keep-net-neutrality-rules.

[9] Public Knowledge and Common Cause, *Comments of Public Knowledge and Common Cause in the Matter of Restoring Internet Freedom,* July 19, 2017, https://ecfsapi.fcc.gov/file/1071932385942/PK%20CC%20Updated%20Comments%20with%20Appendices%20FINAL.pdf.

[10] Center for Democracy & Technology, *Comments of the Center for Democracy & Technology in the Matter of Restoring Internet Freedom,* July 17, 2017, https://ecfsapi.fcc.gov/file/107172520302851/CDT%202017%20FCC%20NPRM%20Comment.pdf; Verizon, *Comments of Verizon in the Matter of Restoring Internet Freedom,* July 17, 2017, https://ecfsapi.fcc.gov/file/10717390819816/2017%2007%2017%20Verizon%20comments%202017%20Open%20Internet%20Notice.pdf; Comcast Corporation, *Comments of Comcast Corporation in the Matter of Restoring Internet Freedom,* July 17, 2017, https://ecfsapi.fcc.gov/file/10717906301564/AT%26T%20Internet%20Freedom%20Comments.pdf.

addresses, once lost, are "nearly impossible to regain exclusive control of."[11] The FCC's *ex ante* regulatory ability is essential to prevent this Pandora's box from being opened in the first place, as individuals who have their data compromised under a Title I regime may feel those lasting impacts indefinitely.[12]

Just as concerning, pending litigation continues to throw the FTC's authority in this sector into question.[13] *AT&T Mobility v. FTC*, which is currently being considered *en banc* before the U.S. Court of Appeals for the Ninth Circuit, may undermine the FTC's regulatory authority. If the Court finds in favor of AT&T, it "would effectively leave consumers with no federal remedy for violations of privacy by ISPs with common carrier services."[14] The impact of such an interpretation would be disastrous for consumer data security protection. We reiterate our concern regarding the effect of the proposed rules on small companies and individual consumers who do not have large financial reserves - making it practically impossible for individual complaints to be acted upon. An unfavorable court ruling, combined with the roll-back of Title II classification, threatens to create a gap in consumer protection.[15]

II. 'Privacy promises' do not safeguard consumer's privacy

The FCC, in suggesting that the FTC should be given sole authority over ISPs' data security practices, places great emphasis on the importance of companies' individual privacy

---

[11] Center for Democracy & Technology, *Comments of the Center for Democracy & Technology in the Matter of Restoring Internet Freedom,* July 17, 2017, https://ecfsapi.fcc.gov/file/107172520302851/CDT%202017%20FCC%20NPRM%20Comment.pdf.

[12] Stan Adams, *Why the FTC Shouldn't Be the Only "Cop On the Beat,"* Center for Democracy and Technology, May 18, 2017, https://cdt.org/blog/why-the-ftc-shouldnt-be-the-only-cop-on-the-beat/.

[13] Center for Democracy and Technology, *LabMD v. FTC: Tackling "Unfair" Data Security Practices in the Eleventh Circuit,* June 20, 2017, https://cdt.org/insight/labmd-v-ftc-tackling-unfair-data-security-practices-in-the-eleventh-circuit/.

[14] Center for Democracy & Technology, *Comments of the Center for Democracy & Technology in the Matter of Restoring Internet Freedom,* July 17, 2017, https://ecfsapi.fcc.gov/file/107172520302851/CDT%202017%20FCC%20NPRM%20Comment.pdf.

[15] Harold Feld, *Understanding the Ninth Circuit's Decision in AT&T Mobility v. FTC,* Public Knowledge, August 31, 2016, https://www.publicknowledge.org/news-blog/blogs/understanding-the-ninth-circuits-decision-in-att-mobility-v-ftc.

promises. Historically, the FTC's privacy policy enforcement actions involved cases of broken privacy promises, not cases in which privacy policies and practices were woefully inept at protecting consumers.[16]

Under the proposed reclassification, there would be a new, increased reliance on privacy promises. This is "a recipe for dismantling privacy protections, not enhancing them."[17] If ISPs can only be held accountable for the privacy promises they create for themselves, they may be incentivized to simply refrain from creating robust promises in order to avoid being held liable by the FTC for any failures to engage in adequate protection. This race to the bottom among privacy promises would mean that "the FTC may not be able to adequately protect the sensitive personal data of consumers through enforcement."[18]

NCL firmly believes that privacy promises alone are insufficient when compared to vigorous privacy protection rules enforced by the FCC. Although industry players like Verizon laud the FTC's ability to ensure standards are upheld "consistently across the Internet ecosystem," the opposite is in fact true.[19] Each ISP would be held to their own, personalized privacy promise, if they choose to make one. As they are currently written, these promises vary wildly by company and typically do not cover information such as browsing history that is not personally identifiable or app usage, location data, and other information that ISPs deems to be non-sensitive.[20] Given this fact, consumers would be worse off under sole FTC jurisdiction, as the FTC can only enforce privacy promises, not create new privacy rules.

---

[16] Public Knowledge and Common Cause, *Comments of Public Knowledge and Common Cause in the Matter of Restoring Internet Freedom,* July 19, 2017, https://ecfsapi.fcc.gov/file/1071932385942/PK%20CC%20Updated%20Comments%20with%20Appendices%20FINAL.pdf.

[17] Free Press, *Comments of Free Press in the Matter of Restoring Internet Freedom,* July 17, 2017, https://ecfsapi.fcc.gov/file/1071818465092/Free%20Press%20Title%20II%20Comments.pdf.

[18] Center for Democracy & Technology, *Comments of the Center for Democracy & Technology in the Matter of Restoring Internet Freedom,* July 17, 2017, https://ecfsapi.fcc.gov/file/107172520302851/CDT%202017%20FCC%20NPRM%20Comment.pdf.

[19] Verizon, *Comments of Verizon in the Matter of Restoring Internet Freedom,* July 17, 2017, https://ecfsapi.fcc.gov/file/10717390819816/2017%2007%2017%20Verizon%20comments%202017%20Open%20Internet%20Notice.pdf.

[20] Jeremy Gillula and Kate Tummarello, *Hallow Privacy Promises from Major Internet Service Providers,* Electronic Frontier Foundation, April 18, 2017, https://www.eff.org/deeplinks/2017/04/major-internet-service-providers-privacy-promises-ring-hollow.

Unlike the FCC, the FTC views privacy not as a right, but as "a commodity to be balanced against other considerations."[21] The FTC's view in this area fundamentally clashes with the value set of most consumers.[22] Consumers' practical inability to protect their own data, coupled with the intrinsic importance of Internet access in the 21st century, creates a strong case for the FCC to take a proactive role in protecting consumer data security.

III. Significant economic losses are attributable to data insecurity

In the absence of Title II regulations, the threat to consumers' data security will only increase. This will result in measurable economic losses. Companies lose a considerable amount of money when they must pay consumers to make amends for data breaches that occur on their watch. More broadly, as consumers grow weary of frequent data breaches, a growing number of consumers are simply opting to avoid electronic commerce. These impacts are not inconsequential, with an estimated $2.1 trillion in losses to the global economy by 2019 due to cybercrime.[23]

Another overlooked harm triggered by the proposed reclassification is the disproportional impact to low-income consumers, who acutely feel the dangers of data insecurity. 34% of those making under $30,000 annually report that they ceased Internet commerce following the breaches.[24] This disparity in confidence between high and low-income Americans is alarming, and stratifies the Internet in indefensible ways.

---

[21] Center for Democracy & Technology, *Comments of the Center for Democracy & Technology in the Matter of Restoring Internet Freedom,* July 17, 2017, https://ecfsapi.fcc.gov/file/107172520302851/CDT%202017%20FCC%20NPRM%20Comment.pdf.
[22] Mary Madden and Lee Raine, *Americans' Attitudes About Privacy, Security and Surveillance,* Pew Research, May 20, 2015, http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.
[23] Juniper Research, *Cybercrime will cost businesses over $2 trillion by 2019,* Apr. 25, 2017, https://www.juniperresearch.com/researchstore/strategy-competition/cybercrime-security/enterprise-threats-mitigation.
[24] Elizabeth Weise and Jessica Guynn, *24% of Americans stopped buying online because of breaches,* USA Today, June 3, 2014, https://www.usatoday.com/story/tech/2014/06/03/internet-security-survey/9907947/.

Unfortunately, these economic losses have been completely overlooked by major industry players when evaluating the FCC's NPRM.[25] With more than half of American households reporting that they have "cut down on the number of Internet sites they use" due to Internet security concerns, this is not an insignificant oversight.[26] NCL calls on the FCC to strongly consider the adverse economic impacts that will come about as a result of reclassification. Under Title II, consumers' data is more secure, and consumers will thus utilize the Internet more. As such, a Title II world provides consumers with more economic opportunities.

IV. Current competition is insufficient for meaningful consumer choice

Industry commenters, through numerical gymnastics, have attempted to convince readers that there are choices aplenty in broadband Internet service, creating a protective barrier of competition between the consumer and the ISP.[27] Unfortunately, this is not the case. Lack of meaningful competition ensures that "most consumers cannot change providers if they are unhappy with their current provider's privacy practices."[28] This lack of competition ensures that ISPs have little incentive to respond to consumers' data security concerns absent regulatory intervention. Without the presence of meaningful competition, Title II classification is a critical check on the balance of power wielded by the ISPs, and serves as a key protective force for consumers.

---

[25] Comcast Corporation, *Comments of Comcast Corporation in the Matter of Restoring Internet Freedom,* July 17, 2017, https://ecfsapi.fcc.gov/file/10717906301564/AT%26T%20Internet%20Freedom%20Comments.pdf; Verizon, *Comments of Verizon in the Matter of Restoring Internet Freedom,* July 17, 2017, https://ecfsapi.fcc.gov/file/10717390819816/2017%2007%2017%20Verizon%20comments%202017%20Open%20Internet%20Notice.pdf; AT&T Services Inc., *Comments of AT&T Services Inc. in the Matter of Restoring Internet Freedom,* July 17, 2017, https://ecfsapi.fcc.gov/file/10717906301564/AT%26T%20Internet%20Freedom%20Comments.pdf.

[26] Elizabeth Weise and Jessica Guynn, *24% of Americans stopped buying online because of breaches,* USA Today, June 3, 2014, https://www.usatoday.com/story/tech/2014/06/03/internet-security-survey/9907947/.

[27] AT&T Services Inc., *Comments of AT&T Services Inc. in the Matter of Restoring Internet Freedom,* July 17, 2017, https://ecfsapi.fcc.gov/file/10717906301564/AT%26T%20Internet%20Freedom%20Comments.pdf.

[28] Public Knowledge and Common Cause, *Comments of Public Knowledge and Common Cause in the Matter of Restoring Internet Freedom,* July 19, 2017, https://ecfsapi.fcc.gov/file/1071932385942/PK%20CC%20Updated%20Comments%20with%20Appendices%20FINAL.pdf.

Under the National Broadband Plan, the FCC was given a clear goal by Congress of "maximizing the use of broadband" and ensuring that broadband use "create[d] value [for] consumers."[29] The FCC's authority under Section 706 of the Telecommunications Act of 1996 allows that, if the FCC determines broadband is not being "deployed to all Americans in a reasonable and timely fashion," they are to "take immediate action to accelerate deployment of such capability."[30] Industry players claim that this mission has been fulfilled, even citing FCC statistics claiming that "97% of census blocks with housing units have at least two providers offering fixed broadband services with a minimum of 10 Mbps downstream and 1Mbps upstream."[31] This analysis fails to mention that in 2015, the FCC updated the "broadband benchmark speeds to 25 megabits per second (Mbps) for downloads and 3 Mbps for uploads."[32] Under the FCC's own definition, 10% of Americans lack access to broadband Internet entirely and "only 24% of census blocks housed two or more providers of fixed broadband."[33]

Clearly, the FCC has a great amount work left to do in order to fulfill its Section 706 mandate. This goal cannot be achieved if consumers are fleeing the Internet due to legitimate data security concerns. As stated in the FCC's NPRM "[t]he Internet became an ever-increasing part of the American economy, offering new and innovative changes in how we work, learn, receive medical care, and entertain ourselves."[34] Consumers should not be put in the position of choosing between Internet access, a service now ingrained in all aspects of 21st Century life, and their own data security - a choice forced upon consumers in a world without Title II protections.

---

[29] FCC, *America's Plan Executive Summary,* March 17, 2010, https://transition.fcc.gov/national-broadband-plan/national-broadband-plan-executive-summary.pdf.
[30] 47 U.S. Code § 1302 – Advanced telecommunications incentives.
[31] AT&T Services Inc., *Comments of AT&T Services Inc. in the Matter of Restoring Internet Freedom,* July 17, 2017, https://ecfsapi.fcc.gov/file/10717906301564/AT%26T%20Internet%20Freedom%20Comments.pdf.
[32] Federal Communications Commission, *2015 Broadband Progress Report,* February 4, 2015, https://www.fcc.gov/reports-research/reports/broadband-progress-reports/2015-broadband-progress-report.
[33] Jonathan Sallet, *Better Together: Broadband deployment and broadband competition,* The Brookings Institution, March 15, 2017, https://www.brookings.edu/blog/techtank/2017/03/15/better-together-broadband-deployment-and-broadband-competition/.
[34] See, e.g., Aaron Smith, Pew Research Center, Searching for Work in the Digital Era at 2 (2015), http://www.pewinternet.org/files/2015/11/PI_2015-11-19-Internet-and-Job-Seeking_FINAL.pdf (detailing the importance of the Internet for job seekers); Lifeline & Link Up Reform & Modernization, Order on Reconsideration, 31 FCC Rcd 3962, 3967, para. 16 (2016) (discussing the benefits of telemedicine).

Conclusion

The FTC is not adequately positioned to safeguard consumers data security, as the FTC can only engage in *ex post* regulatory intervention and enforce privacy promises made to consumers. Given the lack of competition in the Internet ecosystem, ISPs have every incentive to create privacy policies that protect themselves from FTC enforcement, not consumers from data breaches. The rapid rise of data breaches has not only drained millions from the economy, but has caused many Americans to reduce or cease usage of the Internet. Bringing more Americans online is a core tenant of the FCC's work, highlighted by its Section 706 mandate. The FCC's ability to craft *ex ante* regulations makes them the correct agency to be tasked with ISP regulation.

The failure by industry players to meaningfully acknowledge the significant data security impacts triggered by reclassification is very troubling. Buried within filings spanning hundreds of pages, most industry members spent just a few lines breezily addressing data security and privacy ramifications, with Comcast referring to this critical question merely as an "ancillary benefit" of reclassification.[35] Not only do we firmly believe that handing sole jurisdiction over privacy to the FTC would be a net-loss to consumers data security rather than a benefit, it certainly should not be considered an "ancillary" effect.

Such a view of the importance of consumer data security serves to highlight exactly why NCL is concerned with putting such a critical component in the hands of the FTC and industry privacy promises instead of the current Title II classification. NCL firmly believes that these alternatives fall short of equaling the level of protection afforded to consumers under the current Title II regime, and are unacceptable. The unique position of ISPs "comes with a responsibility

[35] Comcast Corporation, *Comments of Comcast Corporation in the Matter of Restoring Internet Freedom,* July 17, 2017, https://ecfsapi.fcc.gov/file/10717906301564/AT%26T%20Internet%20Freedom%20Comments.pdf.

to protect" the information with which they are entrusted, and this important responsibility should be seen as consumer right, not simply as a privilege.[36]

As these reply comments demonstrate Title II classification for ISPs provides the strongest legal framework for the protection of consumers' data security. A decision by the FCC to reclassify under Title I of the Communications Act would significantly weaken the data security of all consumers.[37] NCL urges the FCC to refrain from reclassification and continue to promote strong data security for ISPs.

Respectfully submitted,

/S/

John D. Breyault
Vice President of Public Policy, Telecommunications and Fraud
National Consumers League

[36] Center for Democracy and Technology, *Setting the Record Straight on Broadband Privacy -- Myths and Facts,* June 19, 2017, https://cdt.org/insight/setting-the-record-straight-on-broadband-privacy-myths-facts/.
[37] Restoring Internet Freedom, WC Docket No. 17-108, Notice of Proposed Rulemaking, FCC 26, (rel. Apr. 27,2017), available at https://apps.fcc.gov/edocs_public/attachmatch/FCC-17-60A1_Rcd.pdf, *(Restoring Internet Freedom NPRM).*