Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
Protecting the Privacy of Customers of Broadband and Other Telecommunications Services	)	WC Docket No. 16-106

THE FREE STATE FOUNDATION[*]

REPLY COMMENTS TO OPPOSITIONS

I. Introduction and Summary

The Free State Foundation respectfully submits these Reply Comments to Oppositions to Petitions for Reconsideration of rules adopted by the Commission in its *Broadband Privacy Order* (2016). The Commission lacks legal authority for its new privacy rules. And the regime of intrusive regulation it imposes on broadband Internet service providers (ISPs) but not on other online service providers that collect personal information is arbitrary and will restrict the choices that ISPs offer consumers and the information available to consumers. The Commission should grant the Petitions and find that it is in the public interest to withdraw its new privacy rules in their entirety. Or, at the very least, the Commission should find it is in the public interest to amend its privacy rules to conform them to the Federal Trade Commission's (FTC) framework for privacy protections.

Section 222 jurisdiction is limited to the privacy of phone call length, numbers called, voice billing, and like information "made available to the carrier by the customer solely by virtue

[*] These reply comments express the views of Randolph J. May, President of the Free State Foundation, and Seth L. Cooper, Senior Fellow. The views expressed do not necessarily represent the views of others associated with the Free State Foundation. The Free State Foundation is an independent, nonpartisan free market-oriented think tank.

of the carrier-customer relationship." The Commission's privacy rules improperly purport to extend its Section 222 authority to broad information categories, including "any information that is linked or linkable to an individual" via the Internet.

The Commission's imposition of intrusive privacy rules on ISPs – but not on non-ISPs that also collect personal information and data, and much more of it – is contrary to the principle that laws should be applied equally to all, absent compelling reasons to the contrary. ISPs do not uniquely possess such information, as it is well known that Google, Amazon, and Microsoft, and numerous other edge providers collect personal information about users across multiple platforms. The Commission's privacy rules are even more problematic in view of evidence indicating non-ISPs possess and access much more information compared to ISPs, as an increasing percentage of Internet traffic is encrypted and inaccessible to ISPs. It is estimated that encryption technologies were used for as much as 70% of such traffic by the end of 2016. Moreover, the Order nowhere identifies any unique harm posed by ISPs that would warrant a departure from the principle of equal treatment.

By requiring ISPs to create an "opt in" policy regarding the collection of "any information that is linked or linkable to an individual," the Commission's privacy rules unfairly disadvantage ISPs by requiring them to obtain consent for access to data that non-ISPs presently collect without needing such consent. This will almost certainly confuse consumers and give the mistaken impression that ISPs are seeking consent for access to data for dubious reasons – when the reality is otherwise and when non-ISPs will continue routinely to access the same data without providing "opt in" notices. By virtue of such government-created confusion, consumers are more likely to be deprived of information that they would value.

The Commission's reservation of case-by-case review authority over so-called "pay for privacy" offerings such as discounts for use of personally identifiable information also will discourage ISPs from offering consumers targeted marketing deals or selling advertisements personally targeted to match consumer expectations. The privacy rules fail to clearly delineate factors for assessing the lawfulness of offers that contain financial incentives. The rules similarly fail to require the filing of formal complaints that describe with particularity the alleged violations and also fail to place the burden of proof on complaining parties.

Further, the Commission's default privacy regulatory regime for enterprise broadband services should be withdrawn. The rules exempt any contract that "specifically addresses the issues of transparency, choice, data security, and data breach; and provides a mechanism for the customer to communicate with the carrier about privacy and data security concerns." But this results in regulation-by-default and creates significant regulatory uncertainty as to whether a specific contract complies with its exemption terms – or with the Commission's as-applied interpretation of its exemption terms. Such regulation is unnecessary and wrongfully interferes with private contracting. Sophisticated business customers of enterprise broadband services can look after their own interests and negotiate terms. And no specific harm supports such regulation.

Petitioners have offered ample reasons to justify the Commission's reconsideration of the Order, and, as discussed below, the arguments of those opposing the Petitions are not persuasive. The Commission should use its discretionary authority to reconsider its misguided and harmful privacy rules. It should grant the Petitions and find that it is in the public interest to withdraw its new privacy rules in their entirety. Or at the very least, the Commission should amend its privacy rules to conform them with the Federal Trade Commission's (FTC) privacy framework – at least until such time as the FTC's privacy jurisdiction over ISPs is restored. The FTC has extensive

experience addressing online privacy and should serve as the common enforcer of a common set of privacy protections for all consumers online, regardless of the technology platform, service, or application being used.

II. The Commission's Sweeping Privacy Rules Lack Legal Authority

Section 222, the primary claimed basis for the Commission's authority for its new privacy rules, is limited to customer proprietary network information (CPNI) – a category specific to voice communications. In their mistaken claims that Section 222 authorizes the Commission's privacy rules, Oppositions filed in this proceeding emphasize the Commission's Title II reclassification of broadband as a "telecommunications service."[1] Yet, from the mere fact of Title II reclassification, it does not follow that Section 222 automatically authorizes the Commission's privacy rules. Section 222 includes terms specific to telephony. CPNI involves collection and use of subscriber information about the time and length of calls, phone numbers called, and billing information that "is made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[2] ISPs, however, have access to wider varieties of user information that are also accessible to non-ISPs.

As Petitioners have persuasively explained, regulation of data privacy and security involving broadband ISPs is beyond the scope of Section 222 and therefore beyond the Commission's jurisdiction.[3] The new categories of information established in the Order – "customer proprietary information" (customer PI) and "personally identifiable information" (PII) – are significantly and impermissibly broader than the narrow category of CPNI over which the

[1] *See, e.g.,* Public Interest Commenters Opposition, at 4; Center for Democracy & Technology Opposition, at 6.
[2] 47 U.S.C. § 222(h)(1)(A).
[3] *See, e.g.,* American Cable Association (ACA) Petition, at 4-8; National Cable & Telecommunications Association (NTCA) Petition, at 4-12;

Commission has been granted authority.[4] The Commission's reliance on additional statutory authorities for its privacy rules – such as Sections 201(b), 202(a), 303(b), and Telecommunications Act Section 706 – is similarly misplaced.[5]

III. The Commission's Privacy Rules Arbitrarily Subject Only One Group of Market Providers to Stringent Restrictions

The Commission's imposition of more stringent regulations on ISPs' collection and use of personal information compared to edge providers is arbitrary and capricious because ISPs do not uniquely possess such information. The privacy rules fail to account for the diversity of Internet traffic and personal data collection that takes place in an ecosystem inhabited by operating systems, web browsers, search engines, social media platforms, and countless other web apps and edge provider services.

Indeed, the Commission's privacy rules are even more problematic in view of evidence indicating non-ISPs have access to much more information compared to ISPs. Scholars have found that "ISPs have neither comprehensive nor unique access to information about users' online activity," and that "the most commercially valuable information about online users, which can be used for targeted advertising and other purposes, is coming from other contexts such as social networks and search."[6] Growing use of encryption technologies for Internet traffic – which has been estimated to reach 70% by the end of 2016 – will increasingly restrict ISP access to personal information related to non-ISP services.[7]

---

[4] ACA Petition, at 9-10.
[5] *See, e.g.*, CTIA Petition, at 22-24.
[6] Peter Swire, Justin Hemmings, and Alana Kirkland, "Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others," *A Working Paper of the Institute for Information Security & Privacy at Georgia Tech* (May 2016), available at: http://peterswire.net/wp-content/uploads/Online-Privacy-and-ISPs-1.pdf.
[7] *See* Sandvine, Press Release: "Sandvine: 70% Of Global Internet Traffic Will Be Encrypted In 2016" (February 11, 2016), available at: https://www.sandvine.com/pr/2016/2/11/sandvine-70-of-global-internet-traffic-will-be-encrypted-in-2016.html.

Opponents miss the mark in making claims that the findings of Peter Swire and his colleagues regarding access to consumer data and encryption have been refuted.[8] In fact, Opponents essentially concede Swire's main point – that ISPs do not have access to the growing volume of *encrypted* Internet data traffic. Reiterating the undisputed fact that ISPs have access to and collect unencrypted data neither undermines Swire's findings nor establishes that ISPs are unique possessors of personal information that should be uniquely subject to stringent rules.

It is also overly simplistic and misleading when Opponents characterize ISPs as gatekeepers deserving stricter restrictions when the same term could be applied to different types of edge services.[9] For instance, a user may have different ISPs depending on whether they are using a mobile device or a PC or are working at home or at their office – but rely on the same Internet search engine or web-app across multiple devices.

Subjecting only ISPs to its new privacy rules is contrary to the principle that laws should be applied equally to all. Certainly, the privacy rules violate the principle that regulations should be neutrally applied to all technologies,[10] absent strong reasons exist for treating them differently. In adopting its privacy rules, the Commission failed to offer any reasons to justify the disparate regulatory treatment of ISPs. The Commission has offered no evidence of consumer harm from ISP privacy practices that justify uneven and more intrusive restrictions being placed on them.[11] And it declined to justify its rules based on any cost-benefit analysis.[12]

Opponents claim that identification of ISP-specific harms is not needed to support the Commission's privacy rules.[13] Even if one assumes this is true of raw exercises of bureaucratic

[8] Public Interest Commenters Opposition, at 3; Free Press Opposition, at 10.
[9] Consumers Union Opposition, at 3; New America's Open Technology Institute, at 6.
[10] NCTA Petition, at 13, 19.
[11] ACA Petition at 14-19; Competitive Carriers Association Petition, at 6-7; NCTA Petition, at 16-19.
[12] NCTA Petition, at 19-21.
[13] Free Press Opposition, at 9.

power, sound policymaking should require evidence of market sector-specific or segment-specific harms before adopting rules that apply more stringently to that sector or segment of the market.

IV. The Commission's Privacy Rules Reduce Choice and Harm Consumers

By requiring ISPs to create an "opt in" policy regarding the collection of "any information that is linked or linkable to an individual," the Commission's privacy rules unfairly disadvantage ISPs by requiring them to obtain consent for access to data that non-ISPs will be able to collect without needing to obtain such consent. This disparate treatment of ISPs almost certainly will confuse consumers, since consumers do not make artificial distinctions among online providers collecting information the way that the Commission's rules do. The opt-in requirement will likely give many consumers a mistaken impression that ISPs are seeking consent for access to data for dubious reasons that should give them heightened concern. It is unlikely consumers would perceive that the opt-in requests are not based on privacy standards applicable to all online providers but based on the preferences of the Commission and Opponents to arbitrarily single out ISPs for more stringent consent requirements. And by virtue of such confusion, consumers are more likely to be deprived of information that they otherwise would value.

The Commission's ban on so-called "take it or leave it" offers and its reservation of case-by-case review authority over so-called "pay for privacy" offers such as discounts for use of PII will discourage ISPs from offering consumers targeted marketing deals or selling advertisements to personally design consumer experiences. As a result, consumers will have reduced choice for free or inexpensive services.

While there is certainly a role for case-by-case adjudication in enforcing the Communications Act and FCC regulations, the privacy rules fail to clearly delineate the factors that it will consider in assessing the lawfulness of offers and plans that contain financial incentives. The Commission's case-by-case approach to "pay for privacy" arrangements is similarly unconstrained by sensible procedural requirements. More carefully crafted procedural rules would require the filing of a formal complaint which addresses, with particularity, the factors delineated by the Commission and which addresses the claimed market failure and consumer harm allegedly connected with the practice at issue. The complainant should bear the burden of proof in an on-the-record evidentiary proceeding.

For targeted advertising and other business models, personal information, not money, is the source of value that consumers provide in exchange for services. Restricting arrangements in which consumers opt to pay for equivalent services rather than provide personal information is a form of price control. Such restrictions are based on the mistaken assumption that consumers are not competent to decide what form of payment they are willing to make for services. The critical point is that the choice should be up to consumers. Unfortunately, the Commission's privacy rules arbitrarily and unduly restrict ISP practices and thereby restrict consumer choice.

V. Consumer Online Privacy Should Be Protected by Equal Rules Under One Enforcer

In view of the legal and policy shortcomings of its privacy rules, the Commission should find that it is in the public interest to withdraw its new rules in their entirety and thereby pave the way for the restoration of the FTC's jurisdiction over privacy for all online services and providers. It is common sense not to have two different federal agencies – the FCC and the FTC – enforcing privacy rules relating to the Internet ecosystem. And there is no reason to think that

consumers want different sets of basic data privacy protections depending simply upon whether they are doing business with an ISP or an edge provider.

Alternatively, the Commission should partially withdraw and amend significantly its privacy rules. To the extent that the Commission may be concerned that rescission of its privacy rules – combined with its Title II classification of broadband services – would create a so-called "gap" in privacy regulation regarding ISPs, the Commission can conform them to the FTC's less burdensome and less costly regulatory regime.[14] The FTC's policy toward privacy better balances consumers' demand for targeted information they desire with their desire to protect personal information they determine is sensitive. The FCC could address ISPs' collection and use of personal information according to standards identical to the ones used by the FTC until Congress steps in to give the FTC authority to enforce a common privacy regime.

VI. The Commission's Rules Regarding Enterprise Broadband Should Be Withdrawn

Under the Commission's misguided approach, enterprise broadband providers are, by default, subject to the new privacy restrictions. The Commission's rules exempt enterprise broadband providers to the extent they service a contract that "specifically addresses the issues of transparency, choice, data security, and data breach; and provides a mechanism for the customer to communicate with the carrier about privacy and data security concerns."[15] Nonetheless, this creates significant regulatory uncertainty as to whether a specific contract complies with its exemption terms – or with the Commission's as-applied interpretation of its exemption terms. As pointed out by Petitioners,[16] this default privacy regulatory regime threatens existing business arrangements and will likely cause future contracts to be re-written to accord with the Commission's preferences. Such restrictions are unnecessary and wrongfully interfere with

[14] USTelecom Petition, 4-6.
[15] *Broadband Privacy Order*, at ¶ 15, 306.
[16] Level 3 Communications Petition, at 5-6.

private contracting. Customers of enterprise broadband are typically sophisticated businesses that negotiate at arms-length over terms of service. They can look after their own interests and negotiate terms. The Commission identified no specific harm warranting its restrictions on enterprise broadband providers, and none of the Opponents identified any compelling reason for retaining such restrictions. The Commission's privacy rules regarding enterprise broadband should be withdrawn.

VII. Conclusion

For the foregoing reasons, the Commission should grant the Petitions for Reconsideration and withdraw its privacy rules – or at least partially withdraw and amend its rules to conform them to the FTC's privacy framework – in accordance with the views expressed herein.

Respectfully submitted,

Randolph J. May
President

Seth L. Cooper
Senior Fellow

Free State Foundation
P.O. Box 60680
Potomac, MD 20859
301-984-8253

March 16, 2017

CERTIFICATE OF SERVICE

I, Randolph J. May, HEREBY CERTIFY that on March 16, 2017, I served the foregoing Reply Comments to Oppositions on the parties below by first-class mail, postage prepaid:

Katie McInnis
Staff Attorney
Consumers Union
1101 17th Street, NW
Washington DC 20036

Susan Grant
Director of Consumer Protection and Privacy
Consumer Federation of America
1620 I Street NW, Suite 200
Washington, DC 20006

Eric Null
New America's Open Technology Institute
740 15th St NW, Suite 900
Washington, DC 20005

Angela J. Campbell
Institute for Public Representation
Georgetown University Law Center
600 New Jersey Avenue,
NW Washington, DC 20001

Natasha Duarte
Center for Democracy & Technology
1401 K St. NW, Suite 200
Washington, DC 20005

Gaurav Laroia
Policy Counsel
Free Press
1025 Connecticut Avenue, N.W. Suite 1110
Washington, DC 20036