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

COMMENTS OF

THE FREE STATE FOUNDATION[*]

I. Introduction and Summary

These comments are submitted in response to the Commission's Notice proposing new regulations for protecting the privacy of customers of broadband services. The Commission proposes new privacy regulations without identifying any apparent problem significant enough to require such regulations and without reliable evidence that those regulations will significantly improve protections for personal information.

The proposed regulations, which clearly will reduce consumer welfare, also pose significant legal and policy shortcomings. Foremost among all the shortcomings is the fact that the FCC's proposed regulations would create disparate privacy regulatory regimes for broadband Internet service providers ("ISP") and "edge providers" like Google and Amazon. This will lead to immense consumer confusion as to the relevant applicable privacy policies because

[*] These comments express the views of Randolph J. May, President of the Free State Foundation, and Seth L. Cooper, Senior Fellow. We acknowledge the assistance of FSF Research Associate Michael J. Horney in the preparation of these comments. 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.

consumers, unsurprisingly, don't distinguish between the two different categories of providers based on regulatory classifications, especially newly-adopted ones. But, worse still, the FCC's proposal would impose more stringent regulations, including the more ubiquitous "opt-in" mandate, on ISPs than those that apply to edge providers – even though websites and services like Google indisputably collect, retain, and utilize far more personal information than do the ISPs. Indeed, Google alone (with all its various data-grabbing applications) most likely collects, stores, and utilizes far more personal information than all the ISPs combined.

The Commission's jurisdiction over privacy is narrowly circumscribed. Its 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 of the carrier-customer relationship." Section 222 does not contain any latent power for the Commission to regulate "any information that is linked or linkable to an individual" via the Internet. The Commission's proposed regulations are an improper overextension of its Section 222 authority.

The Commission mistakenly relies on a factually unsupportable "gatekeeper theory" of competition and incentives in the broadband market as a basis for its proposed privacy regulations. The Commission now apparently relies on a "gatekeeper" claim as a regulatory prop of last resort when traditional market power analysis fails to support its expansive regulatory designs. The switching costs rationale upon which the Commission bases its proposed regulations is undermined by data demonstrating pro-competitive, pro-choice marketplace trends – documented in the *Eighteenth Wireless Competition Report* – favoring easier ability and incentives to switch providers.

By proposing to subject only broadband ISPs to its new privacy regulations, the Commission's rules ignore the numerous other IP-enabled services and providers that collect

personal information from consumers using the Internet. Online video distributors (OVDs), social media platforms, along with other web-based apps and online services routinely collect personal information from consumers. The disparate regulatory treatment between commercial market participants that is not justified on any policy grounds.

The Commission proposed regulations would also reduce consumer choice. If imposed, the nearly ubiquitous "opt-in" requirements regarding PII risk would discourage ISPs from offering consumers targeted marketing deals, selling advertisements to personally design consumer experiences, or offering sponsored data as well as free data or zero-rated plans – all of which potentially could benefit them. The Commission's contemplation of a ban on certain "financial inducement practices," such as offering discounts for use of PII, would deprive consumers of their choice to enjoy free or inexpensive services. Consumers are competent to decide for themselves what form of "payment" – whether in the form of the exchange of personal information or money – that they are willing to make for services.

There is no evidentiary basis for assuming consumers want different sets of basic data privacy protections to apply depending upon whether they are doing business with an ISP or an edge provider – or certainly that they prefer more stringent requirements for ISPs than firms like Google, Amazon, and others that they know are data-grabbers. Nor is there any basis for thinking consumers want different sets of data privacy protections from a single provider depending on the particular service being used at one time or another. Instead of imposing uneven, sector-specific, choice-limiting regulations, the better policy approach to protecting consumer privacy on the Internet is to establish common standards under the jurisdiction of a common enforcer.

The digital privacy framework proposed by the White House in 2012 offers a realistic means of establishing a set of common rules with a common enforcer. Under this approach,

privacy codes of conduct are to be established through a voluntary multi-stakeholder process. The Federal Trade Commission (FTC) would have authority to enforce those codes against providers who agree to abide by them but fail to do so in practice. Significant efforts have already been expended in that process. Obviously, the proposed regulations effectively would doom the prospects of the multi-stakeholder process for establishing consumer privacy protections for ISP subscribers. The far better approach for protecting consumer privacy is to refocus resources and attention on the multi-stakeholder process in order to forge a common set of rules and a common enforcer to protect consumer privacy on the Internet.

II. The Commission Lacks Jurisdictional Authority for Its Sweeping Regulation of Consumers' Privacy and Broadband ISPs

Section 222, claimed by the Commission as the authority for its proposed regulations,[1] is limited to customer proprietary network information (CPNI) – a category specific to the voice communications context. CPNI addresses telecommunications providers' collection and use of individualized subscriber information regarding the time and length of calls, phone numbers called, and consumer voice billing when such information "is made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[2]

Section 222 therefore confers FCC jurisdiction over a different and narrower category of information than the broad personally identifiable information (PII) category that the Commission now proposes and plans to regulate. The Commission proposes to define PII "as any information that is linked or linkable to an individual" – that is, information that "can be used on its own, in context, or in combination to identify an individual or to logically associate

[1] In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Notice of Proposed Rulemaking ("Notice"), WC Docket No. 16-106 (rel. Apr. 1, 2016).
[2] 47 U.S.C. § 222(h)(1)(A).

with other information about a specific individual."[3] Regulation of PII is a gross overextension of the authority conferred by Congress under Section 222. It is legally improper for the Commission to reinterpret its circumscribed privacy mandate regarding telephone services and overextend that authority to the competitive broadband services.

III. The Commission's Proposed Privacy Regulations Are Built on False Factual Premises

The Commission relies on a factually unsupportable "gatekeeper theory" of competition and incentives in the broadband market as a basis for its proposed privacy regulations.[4] This dubious broadband gatekeeper premise is undermined by well-known data, most of which the Commission reports on itself, about innovation and competition in the broadband market. Publicly available data from mid-2014 shows that consumers have multiple options for fixed broadband services. For wireline broadband, service with download speeds of 25Mbps or greater was available to 85.3% of the population, service with download speeds of 10Mbps or greater was available to 92.9%, and service with download speeds of 3 Mbps or greater was available to 95.4%.[5] At that time, 19.1% of the population had access to 4 or more wireline Internet providers 56% had access to 3 or more providers, and 88.4% had access to 2 or more providers.[6]

Furthermore, the Commission's dubious mobile broadband gatekeeper premise becomes even more dubious when wireless broadband availability is taken into account. According to data cited in the *Eighteenth Wireless Competition Report* (2015), as of the middle of last year, 91.5% of the U.S. population lived in census blocks with 4G LTE network coverage provided by three

[3] Notice, at ¶¶ 60, 61.
[4] *See* Notice at ¶¶ 128, 267.
[5] NTIA, National Broadband Map, available at: http://www.broadbandmap.gov/summarize/nationwide.
[6] NTIA, National Broadband Map.

or more wireless providers.[7] And 82.2% lived in census blocks with four or more LTE providers.[8]

The switching costs rationale that the Commission claims as a basis for its proposed regulation is similarly undermined by the *Eighteenth Report*'s observations of pro-consumer marketplace trends favoring easier ability and incentives to switch providers.[9] The *Eighteenth Report* identifies "a rapid shift from traditional postpaid contract plans to no-contract plans."[10] Bring your own device ("BYOD") and handset leasing options are now widely available to consumers. Marketing has increasingly focused on offering Early Termination Fee ("ETF") buyouts to encourage customers switching from competing providers. The rise of no-contract postpaid wireless options and ETF buyouts renders the Commission's gatekeeper premise for privacy regulations particularly untenable.

Further, the faulty "gatekeeper premise" – which apparently now is the agency's go-to last resort as a regulatory prop –reflects a false static picture of the mobile broadband market. The wireless market is dynamic, not static. In just a handful of years, the wireless market has transformed from interconnected analog voice services to a myriad of digital high-speed data communications services. This dynamism is also reflected in the *Eighteenth Report*, which observed "there is wide variety of pricing plans offered by the different mobile wireless service providers that vary along several dimensions, and that may frequently change."[11]

Protecting consumer privacy is surely a laudable and worthwhile policy goal. But doing so in the manner proposed in the Notice requires strong reasons – which are absent here.

---

[7] Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993, Annual Report and Analysis of Competitive Market Conditions With Respect to Mobile Wireless, Including Commercial Mobile Services, *Eighteenth Report*, WT Docket No. 15-125 (Dec. 23, 2015), at 28.
[8] *Eighteenth Report*, at 28.
[9] *See Notice*, at ¶¶ 128, 267.
[10] *Eighteenth Report*, at 53, ¶ 73.
[11] *Eighteenth Report*, at 65, ¶ 104.

IV. The Commission's Proposal Would Create Disparity by Imposing Privacy Regulations Only on One Group of Market Participants

By proposing to subject only broadband ISPs to its new privacy regulations, the Commission's rules ignore the numerous other IP-enabled services and providers that collect personal information from consumers using the Internet. This results in a lack of parity between commercial market participants that is not justified on any policy grounds.

ISPs are not the only sector within the Internet ecosystem that collects data from consumers. Online video distributors (OVDs), social media platforms, along with other web-based apps and online services routinely collect personal information from consumers. As the Internet of Things" or "Internet of Everything" develops and the number of Internet-connected devices proliferates, the types of providers, services, and applications that collect data from consumers will likewise proliferate.

Internet traffic data provides a telling indicator of how today's Internet ecosystem differs so drastically from the public switched telephone network that was contemplated by Section 222. Some operating systems, search engines, and edge providers have high concentrations of Internet traffic. For example, Apple and Google hold roughly 93% of the American mobile operating system market.[12] Google sees roughly 64% of web searches in the U.S.[13] And Netflix and YouTube account for almost 55% of all downstream traffic on fixed networks in North America.[14] A force-fit of the proposed regulations on ISPs fails to account for the diversity and complexity of Internet traffic and corresponding personal data collection that takes place in

[12] *See* NETMARKETSHARE, "Mobile/Tablet Operating System Market Share" (April 2016), available at: https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=1
[13] Parker Thomas, "Google Search Engine Market Share Fell to 64%" *Market Realist* (Dec. 29, 2015), available at: http://marketrealist.com/2015/12/googles-search-engine-market-share-fell-64/
[14] *See* Sandvine, "Global Internet Phenomena Report" (Dec. 2015), available at: https://www.sandvine.com/trends/global-internet-phenomena/

today's Internet ecosystem. Its proposed regulations would thus hamper ongoing efforts by ISPs to create new services service offerings catered to evolving consumer privacy preferences.[15]

Furthermore, as Peter Swire and his colleagues estimate in their paper, "Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others," 7 % of Internet traffic will be encrypted by the end of 2016.[16] That means ISPs will, at best, only have access to roughly 30% of consumer data. Leading operating systems, web browsers, and video applications will have primary access to consumer personal information.

If the proposed regulations are adopted, ISPs will be subject to more stringent regulatory scrutiny than edge providers like Google, Facebook, and Amazon. If the encryption estimates by Swire and his colleagues are correct, the disparity in regulatory treatment between ISPs and non-ISPs will be compounded by the disparity in access to consumer personal information.

This uneven and under-inclusive policy for privacy protection would have negative consequences for competition. It would likely create barriers to entry for ISPs in the online advertising market, since they would face consumer data collection restrictions that incumbent rivals do not. For the same reason, the Commission's unequally applied regulations would confer unfair advantage to Facebook and Google, which already hold over one-third of that market.

By proposing to subject only broadband ISPs to its new privacy regulations, the Commission runs afoul of the rule of law principle that laws should be applied equally to all. Service providers that collect consumer personal information should be subject to the same rules unless clear reasons exist for treating them differently. The Commission fails to offer any

[15] available at: http://repository.cmu.edu/cgi/viewcontent.cgi?article=1098&context=jpc
[16] 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* (Feb. 29, 2016), available at: http://peterswire.net/wp-content/uploads/Online-Privacy-and-ISPs.pdf

reasons to justify the disparate treatment of ISPs embodied in its proposed regulations. The Commission should not adopt any privacy policy reflecting that degree of regulatory favoritism.

V. The Commission's Proposed Privacy Regulations Will Reduce Consumer Choices

By requiring ISPs create an "opt out" policy regarding the collection of "any information that is linked or linkable to an individual," the Commission risks discouraging ISPs from offering consumers targeted marketing deals or selling advertisements to personally design consumer experiences. Its regulation also risks discouraging ISP offerings such as sponsored data as well as free data or zero-rated plans that potentially could benefit them.

The Commission's contemplation of a ban on certain "financial inducement practices" such as offering discounts for use of PII would deprive consumers of their choice to enjoy free or free or inexpensive services and applications.[17] For targeted advertising and other business models, personal information, not money, is the source of value that consumers provide in exchange for services. In essence, consumers can sell or license their personal information in exchange for obtaining services. Such personal information may then be used to customize the services rendered and thereby maximize return values to the consumer. Banning arrangements in which consumers opt to pay for equivalent services rather than provide personal information amounts to an onerous form of price control that reduces consumer welfare. A ban would enshrine in regulation the mistaken assumption that consumers are not competent to decide what form of payment – whether in personal information or money – that they are willing to make for services. Consumers who choose not to "opt in" – a requirement not generally imposed by the FTC – may lose out on beneficial offerings. The critical point is that the choice should be left up

[17] *See* Notice, at ¶¶ 259-263.

to consumers. A ban, however, would eliminate consumer choice and result in regulation-imposed opportunity costs on consumers through loss of service offerings.

VI. Common Rules and a Common Enforcer Would Better Protect Consumer Privacy

Today's convergent Internet ecosystem calls for a set of common principles to be applicable for all providers of digital communications and information services that collect and use personal data. From an end-user perspective, simple and consistent rules concerning the privacy of their personal data are the most consumer-friendly.

Consistency is what consumers increasingly are to expect from IP-based service. There is no reason to think consumers want different sets of basic data privacy protections depending upon whether they are doing business with an ISP or an edge provider. And in many instances those distinctions break down, since an ISP may also be a content provider, and an edge provider may be offering voice services or apps that were traditionally provided by telephone companies. Nor is there any basis in thinking consumers want different data privacy protections from a single provider depending on the particular service being used at one time or another.

The digital privacy framework proposed by the White House in 2012 offers a realistic means of establishing a set of common rules with a common enforcer. Under this approach, privacy codes of conduct are to be established through a voluntary multi-stakeholder process.[18] Service providers who agree to abide by the codes – and who actually abide by them in practice – would gain safe harbor from direct FTC enforcement of the principles. Under Section 5 of the FTC Act, the FTC would adjudicate all disputes on a case-by-case basis.

[18] The White House, "Consumer Data Privacy in a Networked World: A Framework for Promoting Privacy and Promoting Innovation in the Global Digital Economy" (Feb. 23, 2012), available at: https://www.whitehouse.gov/sites/default/files/privacy-final.pdf

This approach would give consumers a simpler and more consistent set of privacy expectations. And consolidating such jurisdiction in the FTC would also reduce the likelihood that particular types of information collectors and purveyors would be disadvantaged without justification as a result of their being subject to different privacy regulatory regimes.

A common enforcer is also important because regulatory policy is often – if not invariably – impacted by the particular regulatory agency charged with its enforcement. Discretionary decision-making upon which enforcement necessarily depends is influenced by an agency's institutional preferences, historic concerns, capabilities, and expertise. Consistency in data privacy policy could be undermined if different agencies – in this instance, the FCC and the FTC – with different priorities and different personnel are given overlapping oversight authority.

Contrary to the Notice, the White House's digital privacy framework appropriately recognizes that the current FCC privacy jurisdiction over telecommunications, cable, and satellite firms should be transferred to the FTC.[19] But even in the absence of a transferal, ISPs should be given the ability to voluntarily opt-out from Section 222 upon choosing to comply with any new privacy regime subject to FTC's enforcement jurisdiction.

Indeed, an unwise and likely harmful effect of the Commission's assumption of authority over broadband ISPs under Section 222 is that Federal Trade Commission (FTC) authority will be removed from broadband ISP practices. From an institutional standpoint, the FTC is better positioned to address privacy matters broadly across the Internet ecosystem. It also has broad institutional enforcement experience in privacy matters. The FTC relies upon an *ex post* enforcement and adjudication process that is more fact-specific, more attuned to marketplace

[19] "Consumer Data Privacy in a Networked World," at 39.

economics, and, thereby, more conducive to fostering innovation than regulation based on *ex ante* rules.

The White House digital privacy framework and the multi-stakeholder process offer a sensible route for addressing privacy on the Internet. That approach is far preferable to the disparate and heavy-handed approach proposed by the Commission. Significant time and efforts have already been expended in that process. Unfortunately, the proposed regulations would effectively doom the prospects of the multi-stakeholder process for establishing consumer privacy protections. The far better approach for protecting consumer privacy is to refocus resources and attention to the multi-stakeholder process and make a common set of rules and a common enforcer the hallmark of consumer privacy protection on the Internet.

VII. Conclusion

For the foregoing reasons, the Commission should act 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

May 27, 2016