Before the
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, D.C. 22030

In the Matter of	)	
	)	
Developing the Administration's	)	Docket No. 180821780-8780-01
Approach to Consumer Privacy	)	

COMMENTS OF
THE FREE STATE FOUNDATION[1]

I. Introduction and Summary

These comments are submitted to NTIA regarding its proposed approach to advance consumer privacy while protecting prosperity and innovation. NTIA's principle-based approach sets out desired privacy protection outcomes for consumers as well as high-level goals for federal action to protect privacy. In these comments, we focus on how case-by-case enforcement by the Federal Trade Commission (FTC) offers the best means for achieving federal goals for a harmonized system of clear legal rules that facilitate flexibility in privacy protection approaches for consumers. Our comments identify steps for bolstering the FTC's jurisdiction over consumer privacy and for establishing the agency as the common enforcer of privacy protections across all online service platforms. At the same time, the comments emphasize that overly restrictive privacy policies, such as ubiquitous mandatory opt-in, that are inconsistent with consumers' preferences will reduce the amount of information available to satisfy consumer demands.

[1] These comments express the views of Randolph J. May, President of the Free State Foundation, Seth L. Cooper, Senior Fellow, and Michael J. Horney, Research Fellow. The views expressed do not necessarily represent the views of others associated with the Free State Foundation. The Free State Foundation is a nonpartisan, non-profit free market-oriented think tank.

We commend NTIA for pursuing consumer privacy protections by "[r]efocus[ing] on the outcomes of organizational practices, rather than on dictating what those practices should be." In other words, NTIA rightly seeks to cultivate "a set of inputs for building better privacy protections into products and services." The stunning variety of existing and emerging digital services and applications involving significantly different uses of various types of consumer information makes detailed government-prescribed codes unrealistic, unworkable, and likely detrimental to innovation, investment, and consumer welfare. Instead, NTIA's Notice rightly calls for an approach to protecting consumer privacy by "managing risk and minimizing harm to consumers from collection, storage, use, and sharing of their info." This approach is suited to today's dynamic digital services ecosystem, and ultimately necessary for "balancing flexibility with the need for legal clarity and strong consumer protections."

Online consumers expect consistent rules to protect their privacy throughout the United States. Therefore, privacy regulation in the U.S. should reflect those expectations, whether consumers are doing business with an Internet service provider (ISP) or an edge provider like Google or Facebook. Case-by-case enforcement by the FTC offers the best means for a harmonized system of clear legal rules that enables flexibility and that is conducive to desired privacy protection outcomes. The FTC's capabilities, expertise, and analytical approach toward consumer privacy make it the preferred agency to serve as a common enforcer of privacy protections. Unlike a proscriptive approach relying on *ex ante* rules, a case-by-case approach allows for individualized examination of the type and use of consumer data involved as well as the underlying digital content, service, or application. Agency enforcement precedents provide a prophylactic function and

guidance regarding what privacy practices are permitted or not. And by avoiding rigid categorical restrictions, a case-by-case approach is hospitable to experimentation and innovation in new digital services and privacy protection measures.

The FTC's present approach to collection of consumer information generally comports with consumers' online expectations. With regard to personally identifiable sensitive consumer information, like financial and health records, the FTC requires an affirmative "opt-in" choice for the collection and use of such data. And with regard to non-sensitive consumer information, like general web browsing or application usage, the FTC's policy is to allow opt-out as the default choice for the collection and use of such data.

Many online service providers allow consumers to access online services and content without the payment of fees. There is considerable evidence that Internet consumers value "free" content and services, even if it means they must share personal information. Thus, consumers "pay" for accessing online content by exchanging their personal non-sensitive information. By collecting consumer information and making that data available to advertisers, online providers are then able to deliver prospective consumers targeted ads they value.

Further, the FTC's approach requires that online service providers make the relevant privacy disclosures about information collection and use "clearly and prominently, immediately prior to the initial collection of or transmission of information, and on a separate screen from any final 'end user license agreement,' 'privacy policy,' 'terms of use' page, or similar document." When consumers are presented the relevant

information regarding their privacy protection choices, they are able to make informed decisions that reflect their preferences.

There are some important steps that Congress should take to bolster the FTC's jurisdiction over consumer privacy and to establish the agency as the common enforcer of privacy protections across all online service platforms. Transferring the FCC's privacy jurisdiction over traditional telephone, cable, and direct broadcast satellite (DBS) services to the FTC is one step. Due to technological convergence, continued enforcement of legacy FCC privacy regulations is increasingly arbitrary and likely to result in one set of providers being unfairly disadvantaged by being subject to overly-restrictive and unevenly applied rules that do not match current market realities. Consumers and online service providers alike would benefit from a simpler, more consistent set of privacy expectations.

Internet communications do not stop at state borders and neither should privacy laws. To the extent that any state laws and regulations impose more stringent requirements on service providers than those set at the federal level, then those state laws and regulations that conflict with federal policy should be preempted.

II. The Digital Marketplace Should Be Governed by Harmonized Clear Legal Rules That Enable Flexibility in Privacy Protection Approaches

Increasingly, consumers expect their privacy to be protected by consistent rules that apply throughout the digital marketplace. A simple set of common rules regarding the privacy and security of their financial and other sensitive personal data are the most consumer-friendly. And there is no basis for presuming consumers want different data privacy protections in connection with their purchase or use of digital content, services, or applications merely because a particular online service provider traditionally has been

subject to one set of sector-specific rules or another. Thus, privacy rules should reflect consumer expectations of consistent and broadly applied protections, regardless of whether consumers' data is being collected, used, stored, or shared by a broadband Internet service provider (ISP) or by an online edge provider.

Moreover, establishment of a common set of privacy protection rules subject to enforcement by a single federal agency makes sense for online service providers. Today's Digital Age marketplace is characterized by convergence among once distinct platforms for video, voice, data, and other services. At every layer of the Internet, reaching from the core to the edge and throughout, myriad business arrangements prevail between companies that are sometimes competitors and sometimes collaborators. In this environment, it is arbitrary to apply disparate rules applied to broadband ISPs and to edge providers who offer similar content, services, or applications because such providers traditionally belonged to different sectors. Disparate rules create the substantial likelihood that some online service providers that collect personal data would be disadvantaged without justification as a result of their being subject to different privacy regulatory regimes.

Importantly, like any other market participant, online services providers require clarity in the law. Such clarity allows digital services providers to ascertain what sort of conduct is likely permitted and what will likely be forbidden, thereby allowing them to adhere to the rules and avoid unnecessary compliance costs. Legal clarity, consistent with a prescriptive approach to consumer privacy, also ensures that online service providers have flexibility to pursue innovative business models and means for protecting consumer

privacy. Such flexibility facilitates consumers' choice among new content, services, and applications in the digital marketplace.

III. Case-by-Case Enforcement by the FTC Offers the Best Means for Desired Privacy Protection Outcomes

Like other types of regulatory enforcement, privacy enforcement unavoidably involves discretionary decisionmaking influenced by the agency's institutional preferences, historic concerns, capabilities, expertise, and analytical approach. A common enforcer of consumer data privacy protections is therefore necessary to ensure a harmonized and consistent policy approach. The FTC's capabilities, expertise, and analytical approach toward consumer privacy make it the preferred agency to enforce privacy protections across all digital platforms.

The FTC has considerable authority to enforce privacy-related protections for consumers under Section 5 of the Federal Trade Commission Act, along with other federal statutes.[2] The agency has authority to bring enforcement actions, on a case-by-case basis, to stop law violations. Pursuant to its enforcement authority, the FTC can remediate alleged unlawful behavior harming consumer privacy through implementation of comprehensive privacy and security programs, monetary compensation to consumers, deletion of illegally obtained consumer data, provision of robust consumer notice and choice mechanisms, and by seeking civil monetary penalties against violators.

[2] *See* Theodore R. Bolema, "The FTC Has the Authority, Expertise, and Capability to Protect Broadband Consumers," *Perspectives from FSF Scholars*, Vol. 12 No. 35 (October 19, 2017), at: http://freestatefoundation.org/images/The_FTC_Has_the_Authority,_Expertise,_and_Capability_to_Protect_Broadband_Consumers_101917.pdf.

The FTC's Bureau of Consumer Protection includes the Division of Privacy and Identity Protection, and the agency has extensive experience in investigating and bringing privacy-related cases in many industry contexts, including cases involving online privacy. At the Free State Foundation's Eighth Annual Telecom Policy Conference in 2016, Commissioner Maureen K. Ohlhausen of the Federal Trade Commission explained:

> [T]he FTC is the primary privacy and data protection agency in the U.S., and probably the most active enforcer of privacy laws in the world. We have brought more than 150 privacy and data security enforcement actions, including actions against ISPs and against some of the biggest companies in the Internet ecosystem.[3]

Further, the FTC's established analytical approach to consumer privacy is ideally suited to address financial and other personal data collection and security practices in the digital marketplace. Commissioner Ohlhausen further described the FTC's consumer-based analytical approach to privacy protection:

> [U]nfairness establishes a baseline prohibition on practices that the overwhelming majority of consumers would never knowingly approve. Above that baseline, consumers remain free to find providers that match their preferences, and our deception authority governs those arrangements.[4]

Importantly, case-by-case enforcement, based on the FTC's Section 5 authority and informed by agency enforcement precedents, addresses consumer privacy in a way that targets clear harms but allows for flexibility in digital service provider approaches to protecting privacy. The FTC's analytical approach and enforcement precedents constitute a developed body of law that providers can look to as a guide. Unlike a proscriptive regulatory approach relying on *ex ante* rules, a case-by-case approach allows for

---

[3] Maureen K. Ohlhausen, Commissioner, U.S. Federal Trade Commission, "Privacy Regulation in the Internet Ecosystem," Free State Foundation Eighth Annual Telecom Policy Conference (March 23, 2016), available at: https://www.ftc.gov/system/files/documents/public_statements/941643/160323fsf1.pdf.
[4] Ohlhausen, "Privacy Regulation in the Internet Ecosystem."

individualized examination of the type and use of consumer data involved as well as the underlying digital content, service, or application. By avoiding rigid and categorical restrictions, a case-by-case approach is hospitable to experimentation and innovation in new digital services and privacy protection measures.

IV. The FTC's Approach to Collection of Consumer Information Comports With Consumers' Online Expectations and With Desirable Privacy Outcomes

The FTC's general approach to collection of consumer information by online service providers best comports with what consumers expect when they are online. And the agency's approach is consonant with privacy outcomes identified in NTIA's notice, including transparency and user control.

With regard to personally identifiable sensitive consumer information, like financial and health records, the FTC requires an affirmative "opt-in" choice for the collection and use of such data. And with regard to non-sensitive consumer information, like web browsing or application usage, the FTC's policy is to allow opt-out as the default choice for the collection and use of such data.

It is important that Internet providers not be required to employ opt-in privacy practices for non-sensitive personal information. Both opt-in and opt-out require companies to notify consumers about what information is being collected and how it might be used. And both give consumers a choice about whether they wish to consent to use of their information. Indeed, it is important that online service providers furnish timely and adequate disclosure about what data may be collected and how it may be used before consumers choose to opt-in or opt-out.

The primary difference between opt-in and opt-out policies is how they function as a "default" rule. With opt-out, the company is free to collect and use information if the consumer does not affirmatively indicate he or she wishes to refuse consent. With opt-in, if a consumer fails to affirmatively provide consent, the company cannot collect and use information. Therefore, under an opt-in rule, the pool of information available for monetization is significantly smaller because studies show that many consumers simply fail to express a preference. With less information available, Internet companies have fewer advertising dollars with which to subsidize their "free" services. At the margin, this could lead to companies charging a fee for services, like Gmail, that currently are offered for "free."[5] Or not providing services at all.

Digital advertising is a business model used by online service providers that allows consumers to access online content without the payment of fees. Instead of purchasing a subscription to an application or website, consumers often "pay" for accessing online content by exchanging their personal non-sensitive information. ISPs and edge providers, like Facebook and Google, collect consumer information and make that data available to advertisers which are then able to send prospective consumers targeted ads.

Stopped here***There is considerable evidence that Internet consumers value "free" content and services, even if it means they must share personal information. A survey cited in the FTC's May 2012 consumer privacy recommendations found that 84%

[5] *See* Daniel Lyons, "The Right Way to Protect Privacy Throughout the Internet Ecosystem," *Perspectives from FSF Scholars* Vol. 12, No. 10, (March 24, 2017), available at: http://freestatefoundation.org/images/The_Right_Way_to_Protect_Privacy_Throughout_the_Internet_Ecosystem_032417.pdf.

of consumers prefer to receive targeted advertising in exchange for free online content.[6] A 2015 Microsoft survey discovered that U.S. consumers are willing to share personal data when there are clearly defined benefits in return. The survey results show that 99.6% of consumers are willing to share personal data in return for cash rewards, 89.3% are willing to share personal data in return for discounts, and 65.2% are willing to share personal data in return for loyalty points for goods and services.[7] And an April 2018 survey conducted by the Network Advertising Initiative found that 67.1% of consumers prefer online content and services to be financed through advertising.[8]

Moreover, because consumers value targeted advertising, they want to make their own choices about privacy settings. The Network Advertising Institute survey finds that 78.6% of consumers believe that the individual (as opposed to the company or the government) should make the decision as to whether to opt out of targeted advertising.[9] A shift in federal privacy policy from an opt-out regime to an opt-in regime (regarding non-sensitive consumer information) would decrease consumer access to online content and services. For personally sensitive information such as medical or financial information, opt-in is appropriate.

---

[6] Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendation for Businesses and Policymakers" (March 2012), available at: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[7] Greg Sterling, "Survey: 99 Percent Of Consumers Will Share Personal Info For Rewards, But Want Brands To Ask Permission," *Marketing Land,* (June 2, 2015), available at: https://marketingland.com/survey-99-percent-of-consumers-will-share-personal-info-for-rewards-also-want-brands-to-ask-permission-130786.

[8] "Digital Advertising, Online Content, and Privacy," *Network Advertising Initiative*, (April 9, 2018), available at: https://surveys.google.com/reporting/survey?hl=en&org=personal&survey=blw6vtyeszrlq5auc5uvhsxbku.

[9] "Digital Advertising, Online Content, and Privacy Survey."

The FTC's approach requires that companies must make the relevant privacy disclosures about information collection and use "clearly and prominently, immediately prior to the initial collection of or transmission of information, and on a separate screen from any final 'end user license agreement,' 'privacy policy,' 'terms of use' page, or similar document." [10] By informing consumers in this way, disclosure will be of greater relevance to them. When consumers are presented the relevant information regarding their privacy protection choices, they then are able to make informed decisions that reflect their preferences.

Evidence shows that timely and adequate disclosure of privacy practices can alter consumer choices. The FTC Staff's Mobile Disclosures Report cited a nationwide survey from 2013 indicating that 57% of all app users have either uninstalled an app because of concerns relating to the sharing of their personal information, or they declined to install an app in the first place for similar reasons.[11] A Deloitte survey from September 2017 found that 64% of U.S. respondents deleted or did not download a specific application in the past 12 months due to concerns over data privacy.[12]

V. FTC Jurisdiction to Protect Consumer Privacy Should Replace FCC's Piecemeal Legacy Privacy Jurisdiction

FTC jurisdiction over consumer privacy in the digital marketplace should replace the FCC's privacy regulation of traditional telephone, cable, and direct broadcast satellite

---

[10] Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission, In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106, (May 27, 2016), available at: https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-federal-trade-commission-federal-communications-commission/160527fcccomment.pdf.

[11] *Id*., at 13, fn 55.

[12] Gina Pingitore, Vikram Rao, Kristen Cavallaro, Kruttika Dwivedi, "To Share or Not To Share: What Consumers Really Think About Sharing Their Personal Information," Deloitte Insights, (September 5, 2017), available at: https://www2.deloitte.com/insights/us/en/industry/retail-distribution/sharing-personal-information-consumer-privacy-concerns.html.

(DBS) services. Currently, the FCC has jurisdiction over telephone subscriber privacy under Section 222 of the Communications Act and over cable subscriber privacy under Section 551. The FCC also has jurisdiction over DBS subscriber privacy under Section 338 of the Satellite Home Viewing Improvement Act. Transferring consumer privacy jurisdiction over those specific services from the FCC to the FTC is a necessary step to establishing a common enforcer of privacy across digital service platforms. Consumers and online service providers alike would benefit from a simpler, more consistent set of privacy expectations.

Whatever rationale may have once existed for regulating telephone, cable, and DBS subscribers' privacy in a disparate fashion no longer holds. In today's digital broadband environment, voice, video, and data services are offered by traditional telephone and cable providers. DBS providers typically offer stand-alone video services or bundled packages that include voice and Internet services, including through agency resale agreements. Wireless providers also offer voice and data services, with 4G and forthcoming 5G upgrades enabling increasingly popular downloading and streaming of HD video content. Due to technological convergence, enforcement of legacy FCC privacy regulations is increasingly arbitrary and likely to result in one set of market providers being unfairly disadvantaged by being subject to overly-restrictive and unevenly applied rules that do not match current market realities.

To further a common enforcer approach to consumer privacy in the digital marketplace, Congress should act to transfer privacy jurisdiction over telephone, cable, and DBS subscribers to the FTC, and NTIA should recommend such legislation to Congress.

VI. FTC Jurisdiction to Protect Consumer Privacy Should Include Broadband Internet Access Services

In early 2017, Congress passed the Congressional Review Act to repeal the FCC's 2016 *Broadband Privacy Order*.[13] By that 2016 order, the Obama Administration FCC imposed an onerous privacy regime on broadband Internet access service providers – but not on online edge providers that typically collect far more financial and personal information from online consumers. The Obama Administration FCC stripped away the FTC's consumer protection authority over broadband ISPs. However, the FCC's adoption of the *Restoring Internet Freedom Order* in December 2017 revived the FTC's authority over ISPs. And in February of 2018, a unanimous *en banc* decision of the Ninth Circuit confirmed the FTC's Section 5 jurisdiction extends to non-common carrier services – including broadband Internet access services – offered by providers offering some services on a common carrier basis.[14]

Acting FTC Director of Consumer Protection Thomas Pahl described what the public could expect if jurisdiction over broadband ISP privacy practices is returned to the FTC:

> The FTC is ready, willing, and able to protect the data security and privacy of broadband subscribers . . . .We have a wealth of consumer protection and competition experience and expertise, which we will bring to bear on online data security and privacy laws. We will apply data security and privacy standards to all companies that compete in the online space regardless of whether the companies provide broadband services, data analysis, social media, or other services. Our approach would ensure

[13] U.S. Congress. Senate. *A joint resolution providing for congressional disapproval under chapter 8 of title 5, United States Code, of the rule submitted by the Federal Communications Commission relating to "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services,"* 115th Cong. 1st sess. S.J.R. 34, available at: https://www.congress.gov/bill/115th-congress/senate-joint-resolution/34.

[14] *FTC v. AT&T Mobility LLC*, 883 F.3d 848 (9th Cir. 2018) (*en banc*).

the standards the government applies are comprehensive, consistent, and pro-competitive.[15]

To maintain a consistent federal policy toward consumer privacy and prevent future incursion into the FTC's privacy jurisdiction, Congress should codify FTC's jurisdiction over consumer privacy practices by broadband ISPs, including non-common carrier services offered by ISPs. Removal of FCC authority to regulate privacy would prevent future possible fragmenting of federal privacy policy.

VII. FTC Privacy Should Preempt State Privacy Laws That Conflict with Federal Policy

Just as consumers expect consistent privacy protections to be applied to providers across the digital marketplace, they also expect consistent privacy protections throughout the United States. Federal policy recognizing the FTC as the common enforcer of consumer privacy in the digital services marketplace requires federal preemption of state and local laws that conflict FTC privacy policies.

Despite events from 2017 and early 2018 re-establishing traditional FTC authority regarding consumer privacy, multiple states have proposed or passed privacy laws that are inconsistent with the FTC's privacy policies. For example, the California Consumer Privacy Act deviates from federal policy by imposing more stringent regulations regarding the collection and use of consumer information.[16] In and of themselves, more stringent regulations adopted by states create burdens and impose additional costs that

---

[15] Thomas B. Pahl, "The View from the FTC: Overseeing Internet Practices in the Digital Age," panel discussion at the Free State Foundation's Ninth Annual Telecom Policy Conference (May 31, 2017), at: http://www.freestatefoundation.org/images/May_31_2017_FTC_Panel_Transcript_072017.pdf.

[16] *See* Michael Horney, "California Privacy Law Will Increase the Cost of Accessing Online Content," *Perspectives from FSF Scholars* Vol. 13, No. 30, (July 23, 2018), available at: http://freestatefoundation.org/images/California_Privacy_Law_Will_Increase_the_Cost_of_Accessing_Online_Content_072318.pdf.

may well have the effect of suppressing consumer demand for Internet services and chilling innovative new service offerings that satisfy consumer preferences.

Moreover, if states adopt differing laws this creates a so-called "patchwork" of regulatory regimes. This necessarily imposes even further burdens and even more costs for edge providers and for websites as they seek to comply, to the extent possible, with the varying requirements of the patchwork regime.

As the FCC's *Restoring Internet Freedom Order* explains:

> It is impossible or impracticable for ISPs to distinguish between intrastate and interstate communications over the Internet or to apply different rules in each circumstance. Accordingly, an ISP generally could not comply with state or local rules for intrastate communications without applying the same rules to interstate communications.[17]

The same applies for edge providers. It is impractical, if not actually impossible, for these Internet companies to monitor data flows across the country. Any online activity can result in Internet traffic transmitted all across the country through multiple states (or foreign countries). This means Internet companies would need to implement different practices in efforts to accommodate California's and other states' privacy laws. These additional costs imposed on Internet companies offering services in these states likely would crowd out resources that otherwise would be used for additional investment and innovation, which all consumers enjoy. Of course, such state laws are prone to conflict with one another and with federal policy, rendering compliance not only unduly burdensome but also unachievable for online service providers.

[17] FCC, *Restoring Internet Freedom*, Declaratory Ruling, Report and Order, and Order ("*Restoring Internet Freedom Order*"), WC Docket No. 17-108 (adopted December 14, 2017; released January 4, 2018), at ¶ 200.

As the FCC said in its December 2017 *Restoring Internet Freedom Order*: "[O]nly the FTC operates on a national level across industries, which is especially important when regulating providers that operate across state lines."[18] The burdens and costs imposed on ISPs and edge providers having to comply with a patchwork of differing state privacy regulatory regimes may well deter investment in broadband facilities in states which adopt privacy laws that differ from federal policy as well as deter the provision of innovative services to consumers in those states.

Thus, the FTC should preempt state privacy laws and regulations that conflict with federal policy because the imposition of such laws is impractical, burdens interstate commerce, and frustrates national policy goals of harmonization and consistency backed by FTC enforcement of consumer protection.

VIII. 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

Michael J. Horney
Research Fellow

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

November 9, 2018

[18] FCC, *Restoring Internet Freedom Order*, at ¶ 183.