Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Competition and Consumer Protection in the 21st Century – "The Intersection between Privacy, Big Data, and Competition"

Project Number P181201
August 20, 2018

To the FTC Commissioners and Staff:

Introduction and Summary

These comments express the views of Randolph J. May, President of the Free State Foundation, 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 an independent, nonpartisan, non-profit free market-oriented think tank focusing heavily on communications and Internet law and policy.

Within the realm of that communications and Internet law and policy work, the Free State Foundation has focused on and devoted scholarly resources to researching and writing about the public policy privacy-related issues raised in the context of service offerings by content providers such as Facebook and Google (so-called "edge providers") on the one hand and Internet service providers such as Verizon and Comcast on the other. It is with this expertise and experience in mind that we offer these comments on "The Intersection between Privacy, Big Data, and Competition."

The exchange of non-sensitive consumer information enables companies to sell targeted advertising, which covers the costs of offering “free” content and services to consumers. Substantial evidence shows that the overwhelming majority of consumers are willing to exchange personal information for “free” content and services. However, it is important that firms provide consumers with adequate disclosure regarding the collection and use of

their personally identifiable data. This way, as part of the bargain, consumers are empowered to make informed choices that reflect their preferences.

Because the functioning of much of the Internet ecosystem involves the exchange of non-sensitive consumer information, as a default, "opt-out" rules, as opposed to "opt-in" rules, spur the development of additional Internet content and services. This enables the monetization of a greater pool of consumer information, while still empowering consumers with a choice about whether or not they want their data collected and used. For certain clearly sensitive information, for example relating to health or financial services, the default should be opt-in rather than opt-out.

Consumers expect the application of consistent privacy rules throughout the entire 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. Internet communications do not stop or change at state borders and neither should privacy laws. To the extent state-by-state privacy regulations differ, this creates a "patchwork problem" for service providers that, at a minimum, imposes additional costs but also is likely to stifle investment and innovation. The FTC should regulate the privacy practices of both edge providers and ISPs in a consistent manner, and to the extent that a "patchwork" of state laws and regulations develop that impose more stringent requirements on service providers than those imposed at the federal level, then those state laws and regulations that conflict with federal policy should be preempted.

Targeted Advertising Spurs “Free” Online Content

Digital advertising is a business model that allows consumers to access online content and information 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 advertising agencies which are then able to send prospective consumers targeted ads. Without advertising revenue, websites and applications would be forced to charge subscription fees in order to continue operating. Obviously, many consumers would object to losing access to content they demand in the marketplace.

And, of course, assuming movement to a subscription-based business model, low-income consumers are more likely to be harmed than others. Although ISPs typically charge subscription fees, one could make the case that the price of broadband access subscriptions would be higher if ISPs did not also employ, at least to some extent, the

advertising business model.[1] In 2017, digital advertising in the United States was an $88 billion market.[2]

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% of consumers prefer to receive targeted advertising in exchange for free online content.[3] 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% of consumers are willing to share personal data in return for discounts, and 65.2% of consumers are willing to share personal data in return for loyalty points for goods and services.[4] 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.[5]

Timely and Adequate Disclosure of Privacy Practices Is Necessary to Ensure Consumer Choice

Consumers value "free" content and services in exchange for their non-sensitive information. They also have concerns about privacy protections, but these can be addressed by ensuring adequate disclosure which enables consumers to make choices. This means, as a general rule, having the opportunity to "opt-out" of data collection. FSF scholars have contended that the FTC's current general approach to online privacy regulation best comports with what consumers expect when they are online.

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. 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. But before consumers choose to opt-in or opt-out, it is

---

[1] Michael Horney, "FCC Privacy Rules Would Harm Consumers by Creating Barriers for ISP Advertising," *Perspectives from FSF Scholars* Vol. 11, No. 28, (August 3, 2016), available at: http://freestatefoundation.org/images/FCC_Privacy_Rules_Would_Harm_Consumers_by_Creating_Barriers_for_ISP_Advertising_080216.pdf.

[2] Sarah Sluis, "Digital Ad market Soars to $88 Billion, Facebook and Google Contribute 90% of Growth," *Ad Exchanger*, (May 10, 2018), available at: https://adexchanger.com/online-advertising/digital-ad-market-soars-to-88-billion-facebook-and-google-contribute-90-of-growth/.

[3] "Protecting Consumer Privacy in an Era of Rapid Change: Recommendation for Businesses and Policymakers," Federal Trade Commission, (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.

[4] 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.

[5] "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.

important that Internet firms provide timely and adequate disclosure about what data may be collected and how it may be used.

The FTC's present 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."[6] Companies should provide consumer disclosure about privacy practices at the "just-in-time" point, or the moment before consumer information is about to be collected. 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.

In fact, 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.[7] A more recent 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.[8]

An Opt-Out Default Increases Access to Online Content and Services

Because the exchange of consumer information is the lifeblood of the Internet, it is important that Internet companies 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.

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

---

[6] 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.

[7] Ibid., page 13, footnote 55.

[8] 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.

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."

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]

Importantly, employing a subscription-based business model risks widening the digital divide by putting Internet-based services beyond the reach of those who cannot afford to pay for them.[10] In other words, a shift in 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.

At the 2016 Advertising and Privacy Law Summit in June 2016, FTC Commissioner Maureen Ohlhausen declared that default opt-in policies for non-sensitive information harm consumers:

> Let me be clear on this point: FTC experience demonstrates that more onerous privacy regulation does not always benefit consumers. Some, however, believe that more stringent regulation adds costs to business but only provides benefits to consumers. Yet because privacy preferences vary widely, regulation can impose significant costs on consumers. Consumers who wish to receive targeted advertising or to benefit from services funded by advertising are harmed by regulation that increases the difficulty of using information. As a result, if a regulation imposes defaults that do not match consumer preferences, it forces unnecessary costs on consumers without improving consumer outcomes. The burdens imposed by overly restrictive privacy regulation, such as broad opt-in requirements for non-sensitive data, may also slow innovation and growth, harming all consumers.[11]

We agree completely with Commissioner Ohlhausen's statement.

---

[9] "Digital Advertising, Online Content, and Privacy Survey."
[10] 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.
[11] Reactions to the FCC's Proposed Privacy Regulations, Remarks of Maureen K. Ohlhausen, Commissioner, 2016 Advertising and Privacy Law Summit, (June 8, 2016), available at: https://www.ftc.gov/system/files/documents/public_statements/955183/160608kellydrye.pdf.

Consumers Expect Consistent Privacy Regulation Throughout the Internet Ecosystem

In a February 2016 paper, "Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others," Peter Swire and his colleagues at Georgia Tech stated that 70% of ISP traffic would be encrypted by the end of 2016.[12] Under that scenario, ISPs, at best, only have access to 30% of consumer data. Encryption keeps getting ever more prevalent so, in 2018, ISPs likely have access to even less consumer data.

On the other hand, as of December 2017, Google and Facebook accounted for 73% of the U.S. digital advertising market.[13] And as of July 2018, Google had access to over 86% of all Internet searches in the United States[14] and controlled almost 50% of the web browsing market.[15] Despite its recent troubles, in July 2018, Facebook still controlled 54% of the social media market.[16] The market shares of these web giants indisputably have far greater access to consumers' personal information than ISPs.

So, when it comes to access to consumer data, and market power, arguably edge providers should be subject to more stringent privacy regulation than ISPs. Nevertheless, in our view, all service providers, whether edge providers like Google and Facebook, or ISPs, generally should be subject to the same regulatory regime. Today's convergent Internet ecosystem calls for a set of common requirements to be applicable to all providers of digital communications and information services and web sites that collect and use personal data.

Consistency across the Internet ecosystem regarding privacy protection is what consumers increasingly expect. 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 service distinctions break down, because an ISP may also be a content provider, and an edge provider may be offering voice services, messaging services, or other apps that were traditionally provided by telephone companies, or at least from the consumers' perspective are comparable to traditional communications services.

---

[12] 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-andISPs.pdf.

[13] Jillian D-Onfro, "Google and Facebook Extend Their Lead in Online Ads, and That's Reason for Investors to Be Cautious," *CNBC*, (December 20, 2017), available at: https://www.cnbc.com/2017/12/20/google-facebook-digital-ad-marketshare-growth-pivotal.html.

[14] "Search Engine Market Share United States of America," *StatCounter Global Stats*, (July 2018), available at: http://gs.statcounter.com/search-engine-market-share/all/united-states-of-america.

[15] "Browser Market Share United States of America," *StatCounter Global Stats*, (July 2018), available at: http://gs.statcounter.com/browser-market-share/all/united-states-of-america.

[16] "Social Media Stats United States of America," *StatCounter Global Stats*, (July 2018), available at: http://gs.statcounter.com/social-media-stats/all/united-states-of-america.

By reclassifying ISPs as information service providers rather than telecommunications carriers, the FCC's *Restoring Internet Freedom Order*, adopted in December 2017, had the salutary effect of restoring the FTC's jurisdiction to regulate the privacy practices of both edge providers and ISPs, thus allowing the Commission, with its experience and expertise in protecting consumer privacy, to impose sanctions where warranted against both on a case-by-case basis.[17] In other words, at present, there is a symmetrical privacy regulatory regime in place, with FTC enforcement authority, that protects consumers of both the edge providers and ISPs against privacy abuses. This symmetrical regime should be maintained.

The FTC Should Preempt State Privacy Laws That Are Inconsistent with Federal Policy

Just as consumers expect consistent privacy protections to be applied to providers across the entire Internet ecosystem, they also expect consistent privacy protections throughout the entire United States.

Since the FCC adopted the *Restoring Internet Freedom Order*, 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.[18] In and of themselves, more stringent regulations adopted by states create burdens and impose additional costs that may well have the effect of suppressing consumer demand for Internet services and the effect of 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 additional costs for edge providers and for websites as they seek to comply, to the extent possible, with the varying requirements of the patchwork regime.[19]

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

---

[17] In the Matter of Restoring Internet Freedom, Declaratory Ruling, Report and Order, and Order, ("*Restoring Internet Freedom Order*"), WC Docket No. 17-108, (Adopted December 14, 2017), available at: https://www.fcc.gov/document/fcc-releases-restoring-internet-freedom-order.

[18] 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.

[19] Seth Cooper, "State Executive Orders Reimposing Net Neutrality Regulations Are Preempted by the *Restoring Internet Freedom Order*," *Perspectives from FSF Scholars* Vol. 13, No. 5, (February 2, 2018), available at: http://freestatefoundation.org/images/State_Executive_Orders_Reimposing_Net_Neutrality_Regulations_Are_Preempted_by_RIF_Order_020218.pdf.

> rules for intrastate communications without applying the same rules to interstate communications.[20]

The same applies for edge providers. Assuming it is even possible for ISPs and edge providers to distinguish between intrastate and interstate communications, as a practical matter these Internet companies likely would need to install considerable additional data processing capabilities to monitor data flows across the country. Any online activity can result in Internet traffic transmitted all across the country. 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.

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." 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 burdens interstate commerce and frustrates pro-consumer, pro-competitive, pro-investment, and pro-innovation national policy goals.

Conclusion

Thank you for the opportunity to comment on these issues. For the foregoing reasons, the Commission should act in accordance with the views expressed herein.

Sincerely,

Randolph J. May

Michael J. Horney

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

August 20, 2018

[20] *Restoring Internet Freedom Order*, at ¶ 200.