THE FREE STATE FOUNDATION
A Free Market Think Tank for Maryland.....Because Ideas Matter

Perspectives from FSF Scholars
April 4, 2019
Vol. 14, No. 9

Protecting Privacy on the Internet: Key Principles for Any Reform

by

Theodore R. Bolema *

I. Introduction and Summary

Interest in strengthening privacy enforcement is likely to increase following a stream of revelations of invasive violations of consumers' privacy expectations by Facebook and other edge providers, as well as the apps supplying private data to them. For example, a recent *Wall Street Journal* report details how social media giants collect intensely personal information from many popular apps just seconds after users enter it, sometimes even when the user has no connection to the social media company. Recent calls for legislation to enhance privacy protection enforcement include a report from the U.S. Government Accountability Office and a recent speech by Chairman Joseph J. Simons of the Federal Trade Commission (FTC).

If the current Congress is looking to increase federal protections for privacy on the Internet, it is important that any future proposals start from a firm foundation. Specifically, any privacy protection regime should be based on two key principles: that it will (1) be applied equally across platforms, and (2) be overseen by a single lead federal agency with the expertise and capability to protect broadband consumers. For the latter, the FTC is the only agency at the federal or state level that has the institutional structures, experience, and expertise to take this lead role in Internet privacy protection.

The 2015 *Open Internet Order* (*Title II Order*) set off an era of confusion over the rules for privacy protections on the Internet and which federal agency was in charge. After assuming authority to regulate Internet service providers (ISPs) as common carriers, and thereby divesting the Federal Trade Commission of authority over them, the Federal Communications Commission (FCC) then proceeded to adopt its 2016 *Broadband Privacy Order*, which imposed burdensome requirements on ISPs like those for cable and mobile telephone companies, including opt-in consent requirements. Thus, the *Title II Order*, coupled with the *Broadband Privacy Order*, had the effect of leaving non-ISP edge providers like Google, Facebook, and Amazon subject to the less stringent requirements enforced by the FTC, even though these edge providers collect far more personal data over the Internet than ISPs.

Clarity was restored after the FCC implemented its 2017 *Restoring Internet Freedom Order* (*RIF Order*), which repealed the *Title II Order*, reestablishing the FTC's jurisdiction to regulate the privacy protection practices of both edge providers and ISPs. The FTC has been the primary agency for privacy enforcement in the United States for several decades. Its expertise in this field exceeds that of any other federal or state agency.

There is no reason to believe that consumers want one set of data privacy protections from ISPs and a different set of protections from edge providers. Indeed, consumers in many cases are unlikely to be able to distinguish between providing data to an edge provider and providing data to an ISP. Moreover, the distinctions between the two are breaking down as ISPs increasingly are providing content and edge providers are offering services like Google Voice that compete with communications services offered by ISPs.

Strong evidence is now emerging that the most invasive violations of consumers' privacy expectations are committed not by ISPs at all, but from the same edge providers like Facebook that received more favorable regulatory treatment as a result of the coupling of the FCC's *Title II* and 2016 *Broadband Privacy Orders*. As we learn more about the aggressive collection and use of highly personal data by edge providers like Facebook, the approach resulting from the *Title II Order* era favoring edge providers with less stringent requirements now seems particularly misguided.

To the extent any additional rulemaking authority is considered, as FTC Chairman Simons stated in his address at the Free State Foundation conference, it should be carefully "targeted." If Congress seeks to strengthen current Internet privacy protections, it should so in a way that maintains the current symmetrical structure of FTC enforcement authority over both the edge providers and ISPs.

II. Privacy Threats by ISPs vs Threats From Edge Providers

The 2015 *Title II Order* set off an era of confusion over the rules for privacy protections on the Internet and which federal agency was in charge. The *Title II Order* did this by effectively stripping the Federal Trade Commission of its jurisdiction over ISP practices that are potentially harmful to consumers, including practices involving online privacy.[1] Before 2015,

[1] NPRM, at ¶66; Federal Communications Commission, "Protecting and Promoting the Open Internet Notice of Proposed Rulemaking," GN Docket No. 14-28 (February 26, 2015), at ¶462, available at: https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf.

ISPs were classified as Title I information services, which allowed broadband services to develop and thrive with relatively light touch regulation.[2] For the entire history of the Internet before the 2015 *Title II Order*, the FTC, as well as other state and federal enforcement agencies, had the same authority over broadband that they have over other market participants under their general enforcement statutes.

After declaring ISPs to be common carriers subject to Title II, the FCC adopted its 2016 *Broadband Privacy Order*.[3] This *Order* imposed stringent privacy restrictions on ISPs, including opt-in consent requirements. At the same time, the *Order* had the effect of leaving non-ISPs like Google, Facebook, and Amazon subject to the FTC's less stringent privacy requirements, including in most instances only opt-out consent requirements, even though these edge providers collect far more personal data over the Internet than ISPs do. Therefore, the effect of the *Broadband Privacy Order* was to place ISPs at a disadvantage with edge providers and confuse consumers with its uneven application.[4]

Fortunately, the ill-conceived 2016 *Broadband Privacy Order* never took effect because it was blocked by a joint resolution from the U.S. Congress pursuant to the Congressional Review Act.[5] As a result, while the *Title II Order* was in effect, neither the FCC nor the FTC was providing privacy protection enforcement regarding the ISPs. This void in protecting consumers' online privacy ended after the FCC implemented its 2017 *RIF Order*, which repealed the *Title II Order*, thereby restoring the FTC's jurisdiction to oversee the privacy practices of both edge providers and ISPs.[6] As will be discussed below, if Congress seeks to

---

[2] The Telecommunications Act of 1996 draws a distinction between Title I "information services" and Title II "telecommunications services." Title I information services are lightly regulated, if at all, while Title II telecommunications services are considered common carriers and may be subject to public utility-style regulation. For a more complete discussion of the legal and jurisdictional issues raised by the Title II Order, *see* "Comments of Free State Foundation," WC Docket No. 17-108 (July 17, 2017), available at: http://www.freestatefoundation.org/images/FSF_Initial_Comments_-_Restoring_Internet_Freedom_-_071717.pdf.

[3] Federal Communications Commission, "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," WC Docket No. 16-106 (October 27, 2016), available at: https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-148A1.pdf.

[4] For a more complete discussion of the flaws in 2016 Broadband Privacy Order, *see* Free State Foundation, "Reply Comments to Oppositions for Petitions for Reconsideration, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," WC Docket No. 16-106 (March 16, 2017), available at: https://ecfsapi.fcc.gov/file/1031625753193/FSF%20Reply%20Comments%20Re%20Protecting%20the%20Privacy%20of%20Customers%20of%20Broadband%20and%20Other%20Telecommunications%20Services%20031617.pdf.

[5] 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.

[6] Restoring Internet Freedom Order, WC Docket No. 17-108, (December 14, 2017), available at: https://apps.fcc.gov/edocs_public/attachmatch/FCC-17-166A1.pdf. For a more complete explanation of why the FTC is better able to protect consumers' privacy, *see* Theodore Bolema, "The FTC Has the Authority, Expertise, and Capability to Protect Broadband Consumers," *Perspectives from FSF Scholars*, Vol. 12, No. 35 (October 19, 2017), available at: http://www.freestatefoundation.org/images/The_FTC_Has_the_Authority,_Expertise,_and_Capability_to_Protect_Broadband_Consumers_101917.pdf.

strengthen current Internet privacy protections, it should so in a way that maintains the current symmetrical structure of FTC enforcement authority over both the edge providers and ISPs.

Strong evidence is now emerging that the most invasive violations of consumers' privacy expectations are not by ISPs at all, which were the focus of the FCC under the *Title II Order*, but rather by Facebook and other edge providers, as well as the apps supplying private data to them. A recent *Wall Street Journal* report details how social media giants collect intensely personal information from many popular apps just seconds after users enter it, sometimes even when the user has no connection to the social media company. According to the report:

> It is already known that many smartphone apps send information to Facebook about when users open them, and sometimes what they do inside. Previously unreported is how at least 11 popular apps, totaling tens of millions of downloads, have also been sharing sensitive data entered by users. The findings alarmed some privacy experts who reviewed the Journal's testing.
>
> Facebook is under scrutiny from Washington and European regulators for how it treats the information of users and nonusers alike. It has been fined for allowing now defunct political-data firm Cambridge Analytica illicit access to user's data and has drawn criticism for giving companies special access to user records well after it said it had walled off that information.
>
> In the case of apps, the Journal's testing showed that Facebook software collects data from many apps even if no Facebook account is used to log in and if the end user isn't a Facebook member.[7]

The *Wall Street Journal* report identified how prominent non-ISPs, including Apple and Google, routinely acquire highly personal data that they routinely share with others, including Facebook:

> Apple Inc. and Alphabet Inc.'s Google, which operate the two dominant app stores, don't require apps to disclose all the partners with whom data is shared. Users can decide not to grant permission for an app to access certain types of information, such as their contacts or locations. But these permissions generally don't apply to the information users supply directly to apps, which is sometimes the most personal.
>
> In the Journal's testing, Instant Heart Rate: HR Monitor, the most popular heart-rate app on Apple's iOS, made by California-based Azumio Inc., sent a user's heart rate to Facebook immediately after it was recorded.
>
> Flo Health Inc.'s Flo Period & Ovulation Tracker, which claims 25 million active users, told Facebook when a user was having her period or informed the app of an intention to get pregnant, the tests showed.

[7] Sam Schechner and Mark Secada, "You Give Apps Sensitive Personal Information, Then They Tell Facebook," *The Wall Street Journal* (February 22, 2019), available at: https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636.

> Real-estate app Realtor.com, owned by Move Inc., a subsidiary of Wall Street Journal parent News Corp, sent the social network the location and price of listings that a user viewed, noting which ones were marked as favorites, the tests showed.
>
> None of those apps provided users any apparent way to stop that information from being sent to Facebook.[8]

The *Wall Street Journal* report went on to explain why Facebook has a strong financial incentive to collect this private data and use it to enhance Facebook's revenues:

> Data drawn from mobile apps can be valuable. Advertising buyers say that because of Facebook's insights into users' behavior, it can offer marketers a better return on their investment than most other companies when they seek users who are, say, exercise enthusiasts, or in the market for a new sports car. Such ads fetch a higher cost per click.
>
> That is partly why Facebook's revenue is soaring. Research firm eMarketer projects that Facebook this year will account for 20% of the $333 billion world-wide digital-advertising market.
>
> In a call to discuss the company's most recent earnings, however, Chief Financial Officer David Wehner noted that investors should be aware that Apple and Google could possibly tighten their privacy controls around apps. That possibility, he said, is "an ongoing risk that we're monitoring for 2019."[9]

Of course, the "ongoing risk" that Mr. Wehner is describing is not a risk to consumers that their privacy protections will be compromised, but rather, is the risk to Facebook that it will lose access to much of its users' most private data.[10] Thus, as we learn more about the aggressive collection and use of highly personal data by edge providers like Facebook, the approach from the 2016 *Broadband Privacy Order* of imposing heavy-handed restrictions on ISPs while favoring edge providers with less stringent restrictions now seems particularly misguided.

III. The Two Key Principles for Privacy Enforcement and Any Reform Proposals

Professor Daniel Lyons, a Member of the Free State Foundation Board of Academic Advisors, set forth in 2017 the two guiding principles that should be followed in any policy that is intended to protect privacy on the Internet. First, consumer privacy rules should apply equally to all companies, including ISPs and edge providers, regardless of the role they play

[8] *Id*.
[9] *Id*.
[10] Moreover, one market where ISPs and edge providers clearly compete is in online advertising, so any privacy protection approach that treats edge providers and ISPs differently will have a distortionary impact on the growing online advertising market.

in the Internet ecosystem. Second, privacy rules should be subject to oversight by a regulator with a clear view of how privacy interests affect that ecosystem as a whole.[11]

Several legislative proposals sponsored by members of both political parties, currently being considered in Congress, are intended to increase online consumer privacy protections.[12] A recent U.S. Government Accountability Office report, citing Facebook's Cambridge Analytica data disclosures and other incidents in which users' personal data may have been improperly disclosed, suggests giving the FTC more authority over Internet privacy enforcement while strengthening the FTC's enforcement abilities. The GAO report concludes that: "Comprehensive Internet privacy legislation that establishes specific standards and includes traditional notice-and-comment rulemaking and broader civil penalty authority could enhance the federal government's ability to protect consumer privacy."[13]

Since the FCC adopted the *RIF Order*, several states, including California, have proposed or passed new privacy laws with differing compliance requirements for ISPs. As the *RIF 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."[14] Such state laws, if allowed to stand, would impose costs and restrictions on ISPs and edge providers that would almost certainly reduce the supply of Internet services and prevent the development and implementation of new Internet service.[15]

---

[11] Daniel A. Lyons, "The Right Way to Protect Privacy Throughout the Internet Ecosystem," *Perspectives from FSF Scholars*, Vol. 12, No. 10 (March 24, 2017), p. 7, available at: http://www.freestatefoundation.org/images/The_Right_Way_to_Protect_Privacy_Throughout_the_Internet_Ecosystem_032417.pdf.

[12] Editorial Board, "There's hope for federal online privacy legislation," *Washington Post*, (January 21, 2019), available at: https://www.washingtonpost.com/opinions/theres-hope-for-federal-online-privacy-legislation/2019/01/21/f6113a2c-1a9b-11e9-88fe-f9f77a3bcb6c_story.html?utm_term=.2280e9000cd3.

[13] United States Government Accountability Office, "Report to the Chairman, Committee on Energy and Commerce, House of Representatives: Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility," GAO Report 19-52 (January 2019), available at: https://www.gao.gov/assets/700/696437.pdf. According to the GAO Highlights at the beginning of the report: "In April 2018, Facebook disclosed that a Cambridge University researcher may have improperly shared the data of up to 87 million of its users with a political consulting firm. This disclosure followed other recent incidents involving the misuse of consumers' personal information from the Internet, which is used by about three-quarters of Americans. GAO was asked to review federal oversight of Internet privacy. This report addresses, among other objectives: (1) how FTC and FCC have overseen consumers' Internet privacy and (2) selected stakeholders' views on the strengths and limitations of how Internet privacy currently is overseen and how, if it all, this approach could be enhanced."

[14] *RIF Order*, at ¶ 200.

[15] For a more complete discussion of these new or proposed state-level laws and their implications, *see* 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. Cooper also discusses how these state-level regulations are likely unenforceable if they conflict with provisions in the FCC's *RIF Order*.

Joseph Simons, the current Chairman of the FTC, speaking at the Free State Foundation's Eleventh Annual Telecom Policy Conference in 2019, called for Congress to enact legislation that would give the FTC three new tools to protect privacy and data security on the Internet:

> Despite the fact that we are using all the tools Congress has given us, I note that we could use additional authority in the privacy and data security area. I have urged Congress to enact legislation that would give the FTC three tools: (1) the authority to seek civil penalties for initial privacy and data security violations, which would create an important deterrent effect; (2) targeted APA [Administrative Procedures Act] rulemaking authority that would allow the FTC to keep up with technological developments; and (3) jurisdiction over nonprofits and common carriers. The process of enacting federal privacy legislation will involve difficult policy tradeoffs that I believe are appropriately left to Congress. Regardless of what Congress chooses to enact, I commit to using our extensive expertise and experience to enforce any new legislation vigorously and enthusiastically.[16]

The current Congress may well decide that legislation is needed to enhance existing privacy enforcement. If so, it is important that any future proposals to improve the privacy protection for Internet users start from a firm foundation so that the resulting policy will be applied equally across platforms and be overseen by a single lead federal agency with the expertise and capability to protect broadband consumers.

IV. Principle 1: Privacy Protections Should Be Applied Equally Across Platforms

The approach of applying privacy protections equally across platforms was endorsed by Acting FTC Chairman Maureen K. Ohlhausen and FCC Chairman Ajit Pai in early 2017, when they issued a joint statement criticizing the approach of the 2016 *Broadband Privacy Order*. According to the heads of these two agencies at the time:

> The Federal Communications Commission and the Federal Trade Commission are committed to protecting the online privacy of American consumers. We believe that the best way to do that is through a comprehensive and consistent framework. After all, Americans care about the overall privacy of their information when they use the Internet, and they shouldn't have to be lawyers or engineers to figure out if their information is protected differently depending on which part of the Internet holds it.[17]

This position is hardly partisan. When former FTC Chairman Jon Leibowitz, a Democrat, made similar criticisms of the *Broadband Privacy Order*, he pointed out that this view is shared by leading policymakers from both parties and by many consumer advocacy groups:

---

[16] Joseph J. Simons, Chairman, U.S. Federal Trade Commission, "Prepared Remarks of Chairman Joseph J. Simons," Free State Foundation Eighth Annual Telecom Policy Conference (March 26, 2019), available at: https://www.ftc.gov/system/files/documents/public_statements/1508991/free_state_foundation_speech_march_26.pdf.

[17] "Joint Statement of FCC Chairman Ajit Pai and Acting FTC Chairman Maureen K. Ohlhausen on Protecting Americans' Online Privacy," March 1, 2017, available at https://www.ftc.gov/news-events/press-releases/2017/03/joint-statement-acting-ftc-chairman-maureen-k-ohlhausen-fcc.

> As the former Democratic chairman of the Federal Trade Commission, the nation's leading privacy enforcement agency, which has brought more than 500 privacy cases, including more than 50 cases against companies for misusing or failing to reasonably protect customer data, let me assure you: the FCC's rules are deeply flawed.
>
> By creating a separate set of regulations that bind only internet service providers — but not other companies that collect as much or more consumer data — with heightened restrictions on the use and sharing of data that are out of sync with consumer expectations, the FCC rejected the bedrock principle of technology-neutral privacy rules recognized by the FTC, the Obama administration, and consumer advocates alike. Protecting privacy is about putting limits on what data is collected and how it is being used, not who is doing the collecting, and for that reason, a unanimous FTC — that is, both Democratic and Republican commissioners — actually criticized the FCC's proposed rule in a bipartisan and unanimous comment letter as "not optimal," among 27 other specific criticisms of the rule.[18]

It should not be surprising that the recent disclosures about privacy violations on the Internet have mostly involved edge providers. Edge providers simply have greater access to more private data than ISPs have. As Professor Lyons explained in 2017:

> Some including the FCC have suggested that a higher privacy standard for ISPs is appropriate because ISPs "sit at a privileged place in the network" and can collect "an unprecedented breadth of electronic personal information." But this argument rings hollow. First, it is not clear that ISPs are in a position to learn more about a consumer than leading edge providers. Google not only processes roughly two-thirds of all U.S. Internet searches, it also runs the operating system on over half of all U.S. smartphones. Both Google and Facebook permit other content providers to use their logins for identity verification, allowing these titans to build a consumer profile across platforms and locations. My broadband provider may know my online behavior while at home, but Google and Facebook can build a more complete profile of my activity while at home, at work, and on mobile networks as well. Moreover, as Professor Christopher Yoo (who is also a member of the Free State Foundation Board of Academic Advisors) has observed, there is very little an ISP can determine from its allegedly "privileged position" on the network. Whereas edge providers can see all content the consumer accesses, ISPs can only see metadata and traffic flow (unless they engage in deep packet inspection, which is legally suspect under the Electronic Communications Privacy Act).[19]

---

[18] Jon Leibowitz, Letter to the Editor, *Kennebec Journal* (April 13, 2017), available at: http://www.centralmaine.com/2017/04/13/former-ftc-chairman-collins-right-on-privacy/.

[19] Daniel A. Lyons, "The Right Way to Protect Privacy Throughout the Internet Ecosystem," *Perspectives from FSF Scholars*, Vol. 12, No. 10 (March 24, 2017), p. 3, available at : http://www.freestatefoundation.org/images/The_Right_Way_to_Protect_Privacy_Throughout_the_Internet_Ecosystem_032417.pdf, citing Christopher Yoo, "The Fate of the FCC's Privacy Rule: A Chat with Professor Christopher Yoo," Forbes Washington Bytes Blog, February 9, 2017 (other citations omitted), available at https://www.forbes.com/sites/washingtonbytes/2017/02/09/the-fate-of-the-fccs-privacyrule-a-chat-with-law-professor-christopher-yoo/#634fb5433180.

There is no reason to believe that consumers want one set of data privacy protections from ISPs and a different set of protections from edge providers. Indeed, consumers in many cases are unlikely to be able to distinguish between providing data to an edge provider rather than to an ISP. In any event, the distinctions between the two are breaking down as ISPs increasingly are providing content and edge providers are offering services like Google Voice that compete with communications services offered by ISPs. Thus, the importance of consistency in privacy protection across Internet platforms will likely become even more important as service offerings by ISPs and edge providers continue to converge.

V. Principle 2: Privacy Protections Should Be Overseen by a Federal Agency With the Expertise and Capability to Protect Internet Consumers

The FCC's 2017 *RIF Order* restored the Federal Trade Commission to the role it held until 2015 as the lead federal agency with responsibility for safeguarding online privacy, as well as other protections for consumers against other ISP practices that may be anticompetitive or cause consumer harm. The FTC's expertise in this field exceeds that of any other federal or state agency. The reasons the FTC is the agency best suited to be the lead agency in protecting Internet privacy include its established institutional structures and expertise gained from its enforcement experience and its established protocols and precedents from its enforcement activities.

The FTC has considerable authority to implement, investigate, and enforce privacy and consumer protection under Section 5 of the Federal Trade Commission Act of 1914, as well as from other federal statutes that further enhance its regulatory authority.[20] In carrying out this regulatory mission, the FTC can draw on an extensive toolbox that it uses to protect privacy and enforce other consumer protections:

> The FTC uses a variety of tools to protect consumers' privacy and personal information. The FTC's principal tool is to bring enforcement actions to stop law violations and require companies to take affirmative steps to remediate the unlawful behavior. This includes, when appropriate, implementation of comprehensive privacy and security programs, biennial assessments by independent experts, monetary redress to consumers, disgorgement of ill-gotten gains, deletion of illegally obtained consumer information, and provision of robust notice and choice mechanisms to consumers. If a company violates an FTC order, the FTC can seek civil monetary penalties for the violations. The FTC can also obtain civil monetary penalties for violations of certain privacy statutes and rules, including the Children's Online Privacy Protection Act, the Fair Credit Reporting Act, and the Telemarketing Sales Rule. To date, the Commission has brought hundreds of privacy and data security cases protecting billions of consumers.
>
> The FTC's other tools include conducting studies and issuing reports, hosting public workshops, developing educational materials for consumers and businesses, testifying before the U.S. Congress and commenting on legislative and regulatory proposals that

[20] U.S. Federal Trade Commission, " Privacy & Data Security Update" (January 2016), available at: https://www.ftc.gov/reports/privacy-data-security-update-2015#privacy.

> affect consumer privacy, and working with international partners on global privacy and accountability issues.[21]

The FTC's Bureau of Consumer Protection includes a dedicated Division of Privacy and Identity Protection and a staff of economists, and investigative staff in field offices around the country.[22] State regulatory agencies cannot come close to matching the capabilities of the FTC's Bureau of Consumer Protection. And while the FCC staff includes many excellent lawyers and economists, it has limited experience that is specific to privacy protection.

Nonetheless, some pro-regulation groups have claimed that the FTC does not have sufficient expertise to protect consumer privacy on the Internet. This argument is usually advanced to support claims that Title II regulation from the *Open Internet Order* should be retained.[23] But this claim significantly mischaracterizes the experience and expertise of the FTC. Maureen K. Ohlhausen, then-Commissioner of the Federal Trade Commission, speaking at the Free State Foundation's Eighth Annual Telecom Policy Conference in 2016, explained the FTC's expertise over privacy issues as follows:

> Despite rumors to the contrary, the 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. (For our purposes here I consider data security to be a subset of privacy. So when I say "privacy" today I also mean data security.) The FTC has gained this expertise because of - not in spite of - our prudent privacy approach, which maximizes consumer self-determination.[24]

The other main argument from some pro-regulation groups against the FTC serving as the lead Internet privacy enforcer is that the *ex post* enforcement approach of the FTC is not up to the task, and only prescriptive regulation imposed *ex ante* can protect consumers.[25] This

---

[21] *Id.*

[22] U.S. Federal Trade Commission, "About the Bureau of Consumer Protection Update" (visited March 27, 2019), available at: https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/about-bureau-consumer-protection.

[23] For example, Public Knowledge and Common Cause have claimed: "[A]though the FTC does have experience and expertise protecting consumer privacy, it is not the expert agency on communications networks. . . . By giving the FTC exclusive jurisdiction to protect consumer broadband privacy, the FCC would not only turn a blind eye to its own expertise on communications networks but would also rob consumers of the sole privacy cop on the beat with that expertise (citations omitted)," Comments of Public Knowledge and Common Cause, WC Docket No. 17-108 (July 17, 2017), at 91-92, available at: https://ecfsapi.fcc.gov/file/1071932385942/PK%20CC%20Updated%20Comments%20with%20Appendices%20FINAL.pdf.

[24] 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.

[25] For example, the Open Technology Institute has claimed: "Shifting jurisdiction to the FTC would shift consumer privacy to an agency with less authority and more roadblocks to clear, bright-line protections. The FTC's effectiveness is undermined by a lengthy review process and limited enforcement of consent orders (citations omitted)." Comments of the Open Technology Institute at New America, WC Docket No. 17-108 (July 17, 2017), at 39-40, available at: https://na-

argument fails to appreciate how the case-by-case enforcement of the FTC has a strong deterrent effect as companies look at past enforcement instances to guide their conduct. It also ignores the considerable problems with *ex ante* prescriptive regulation in a technologically dynamic, rapidly-changing market. Rulemaking imposes standards based on regulators' predictions about the future conduct and incentives impacting regulated firms. Prescriptive regulations often do more harm than good as markets evolve in ways regulators cannot predict. Case-by-case enforcement, by contrast, involves no such predictions because it challenges and remedies conduct that has already occurred. The *ex ante* approach also requires frequent revision through a notice-and-comment process, which generally will be even more time-consuming than the *ex post* investigative and enforcement approach long used by the FTC.

As such, *ex ante* privacy regulation likely would fail to anticipate and keep up with rapid changes in Internet technology and market practices.[26] To the extent any additional rulemaking authority is considered, as FTC Chairman Simons stated in his address at the Free State Foundation conference, it should be carefully "targeted."[27]

Thus, the FTC's capabilities, expertise, and analytical approach toward privacy enforcement make it the preferred agency for addressing online privacy practices across all digital platforms. The FTC has gained extensive experience protecting privacy from several decades of investigating and bringing cases in many industries, including cases involving online privacy and ISPs. Internet consumers will be well served if the FTC retains the lead role in protecting online privacy, and this role for the FTC should be retained in any proposals before Congress to strengthen Internet consumers' privacy protections.

---

production.s3.amazonaws.com/documents/OTI_NN_COMMENTS_JULY17_FINAL.pdf. Similarly, Public Knowledge and Common Cause have argued: "The FTC protects consumer privacy pursuant to its general consumer protection authority under section 5 of the Federal Trade Commission Act to bar unfair and deceptive acts or practices. Because the FTC lacks both effective rulemaking authority and specific power from Congress to develop standards to protect consumer privacy specifically, the agency is constrained by the limits of section 5 to apply the same, general "unfair and deceptive" standard to online privacy issues. Consequently, the FTC's enforcement actions usually involve broken privacy promises or determining whether companies are adhering to general industry practices rather than what practices would best protect consumers. Consumers expect adequate privacy protections when accessing broadband networks. Unfortunately, enforcement actions without the ability to adopt bright line rules are not enough to protect consumer broadband privacy (citations omitted)." Comments of Public Knowledge and Common Cause, WC Docket No. 17-108 (July 17, 2017), at 92-93, available at: https://ecfsapi.fcc.gov/file/1071932385942/PK%20CC%20Updated%20Comments%20with%20Appendices%20FINAL.pdf.

[26] For a more complete analysis of the advantages of the FTC's ex post approach over a hypothetical FCC ex ante approach advocated by proponents of the *Title II Order*, *see* Theodore Bolema, "The FTC Has the Authority, Expertise, and Capability to Protect Broadband Consumers," *Perspectives from FSF Scholars*, Vol. 12, No. 35 (October 19, 2017), available at: http://www.freestatefoundation.org/images/The_FTC_Has_the_Authority,_Expertise,_and_Capability_to_Protect_Broadband_Consumers_101917.pdf.

[27] Joseph J. Simons, Chairman, U.S. Federal Trade Commission, "Prepared Remarks of Chairman Joseph J. Simons," Free State Foundation Eighth Annual Telecom Policy Conference (March 26, 2019), available at: https://www.ftc.gov/system/files/documents/public_statements/1508991/free_state_foundation_speech_march_26.pdf.

Conclusion

As we learn more about invasive violations of consumers' privacy expectations by Facebook and other edge providers, Congressional interest in legislation to enhance existing privacy protection enforcement is likely to increase. If so, it is important that any future proposals to improve consumer protections in the Internet ecosystem start from a firm foundation so that the resulting policy will be applied equally across platforms and be overseen by the Federal Trade Commission, the only federal or state agency with the expertise and capability to protect broadband consumers. These two guiding principles generally apply to current federal policies aimed at protecting consumer privacy, and should be preserved regardless of whether policymakers keep privacy regulatory authority unchanged or seek to strengthen the enforcement powers of the FTC.

* Theodore R. Bolema is a member of the Free State Foundation's Board of Academic Advisors and Executive Director of the Institute for the Study of Economic Growth at Wichita State University.