Perspectives from FSF Scholars
October 19, 2017
Vol. 12, No. 35

The FTC Has the Authority, Expertise, and Capability to Protect Broadband Consumers

by

Theodore R. Bolema *

I. Introduction and Summary

As part of its *Restoring Internet Freedom* Notice of Proposed Rulemaking (NPRM), the Federal Communications Commission is reevaluating its regulatory authority over consumer protection matters involving Internet service providers (ISPs).[1] If the FCC decides it lacks authority to regulate ISPs as telecommunications carriers under Title II of the Communications Act, the effect of this decision should be to restore the Federal Trade Commission to the role it held until 2015. In essence, this means the FTC would be the lead federal agency with responsibility for safeguarding online privacy and for protecting consumers against other ISP practices that allegedly are anticompetitive or cause consumer harm.

Consumers will be well served if the FTC takes the lead in fulfilling these important consumer protection functions. 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

[1] Federal Communications Commission, "Protecting and Promoting the Open Internet Notice of Proposed Rulemaking" ("NPRM"), WC Docket No. 17-108; FCC 17-60, at ¶66, adopted May 18, 2017, available at: https://www.fcc.gov/document/restoring-internet-freedom-notice-proposed-rulemaking.

decades of investigating and bringing cases in many industries, including cases involving online privacy and ISPs.

By reclassifying ISPs as Title II telecommunications service providers, the 2015 *Open Internet Order* ("*Title II Order*") effectively stripped the FTC of its jurisdiction over broadband ISP practices that are potentially harmful to consumers, including practices involving online privacy.[2] After assuming this newly-derived Title II regulatory authority, the FCC adopted stringent, prescriptive privacy restrictions on ISPs, including opt-in requirements, which were not applicable to non-ISPs like Google, Facebook, and Amazon that collect far more personal data over the Internet than ISPs. Under the FTC's privacy regime, these non-ISPs remained subject to less stringent privacy protecting regulation, including opt-out requirements.[3]

The resulting asymmetric and confusing privacy enforcement approach has been criticized by current and former consumer protection officials from both political parties. When the FCC's overreaching privacy order was blocked by a joint resolution from the U.S. Congress, the Internet privacy protection regime was further complicated.[4] The FCC now has an opportunity to help end the current uncertainty about Internet consumer protection policy and enforcement by restoring the primary authority to the agency best suited to the task – the Federal Trade Commission.

If its authority is restored, the FTC will be re-empowered to use Section 5 of the Federal Trade Commission Act of 1914 to investigate and bring enforcement actions to stop law violations and require ISPs to take affirmative steps to remediate any unlawful behavior. 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. Using this authority, the FTC says that to date it has brought hundreds of privacy and data security cases protecting billions of consumers.[5]

The FTC's Bureau of Consumer Protection already includes a dedicated Division of Privacy and Identity Protection, a staff of economists, and investigative staff in field offices around the country.[6] Even though the FTC has been precluded from privacy enforcement regarding ISPs' practices recently, it has continued its privacy protection activities in all of the other Internet ecosystem market segments subject to its jurisdiction. And it still has staff with experience in privacy enforcement with regard to telecommunications. In contrast, the FCC staff has limited experience that is specific to ISP privacy protection.

---

[2] 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.

[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] 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.

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

[6] U.S. Federal Trade Commission, "About the Bureau of Consumer Protection Update" (visited October 12, 2017), available at: https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/about-bureau-consumer-protection.

Federal antitrust enforcement, by the FTC and by the Antitrust Division of the Department of Justice, can also address consumer protection concerns related to Internet providers. The Antitrust Division and the FTC both have authority to investigate and pursue legal action in instances where broadband ISPs engage in anticompetitive practices that could be considered potential antitrust violations. The Antitrust Division already has an established Telecommunications and Media Enforcement Section that "is responsible for civil antitrust enforcement, competition advocacy, and competition policy in the areas of the Internet, including the services infrastructure and hardware that comprise the Internet."[7]

One of the main arguments that has been asserted for retaining Title II classification of ISPs is that only public utility-style prescriptive regulations are sufficient to address broadband privacy and consumer protection concerns. Pro-regulation groups have asserted 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.

This 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 by the FCC inevitably would fail to anticipate and keep up with rapid changes in Internet technology and market practices. For these reasons, the arguments for *ex ante* prescriptive regulation over *ex post* case-by-case regulation provide no support for retaining Title II regulation of broadband providers.

The Federal Trade Commission has been the primary agency for privacy protection enforcement in the United States for several decades. Its expertise in this field exceeds that of any other federal or state agency and makes the FTC the better choice over the FCC to be the primary federal regulatory agency in charge of addressing privacy and other allegedly harmful ISP practices, such as throttling or paid prioritization. The reasons the FTC is better suited for this role include the FTC's established institutional structures and expertise gained from its enforcement experience, the FTC's established protocols and precedents from its enforcement activities, and the uncertainty added to the market from having an agency without such attributes take over this important regulatory function.

II. Broadband Consumer Protection Before and Since the *Open Internet Order*

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

[7] U.S. Department of Justice, "Telecommunications and Media Enforcement Section," available at: https://www.justice.gov/atr/about-division/telecommunications-and-media-enforcement-section.

subject to public utility-style regulation.[8] Before 2015, ISPs were classified as Title I information services, which allowed broadband services to develop and thrive with relatively light touch regulation. During this time, the Federal Trade Commission, 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.

By reclassifying broadband providers as Title II telecommunications services, the 2015 *Title II Order* effectively stripped the FTC of jurisdiction over broadband ISP practices that are potentially harmful to consumers, including practices involving online privacy. [9] After assuming this regulatory authority, the FCC adopted its 2016 *Broadband Privacy Order.*[10] This *Order* imposed stringent privacy restrictions on ISPs, including opt-in consent requirements. The *Order* also, in effect, left non-ISPs like Google, Facebook, and Amazon that collect far more personal data over the Internet than ISPs do, with less stringent requirements, including in most instances only opt-out consent requirements. Therefore, the effect of the *Broadband Privacy Order* was to unfairly disadvantage broadband ISPs and confuse consumers with its uneven application.[11]

Thomas Pahl, Acting Director of the FTC's Bureau of Consumer Protection, speaking this year at the Free State Foundation's Ninth Annual Telecom Policy Conference, critiqued the FCC's approach and contrasted it with the long-standing privacy policy of the FTC:

> The FCC's *Open Internet Order* therefore effectively prevented the FTC from engaging in enforcement, rulemaking, and other consumer protection activities concerning ISPs' online data security and privacy. In 2016, as many of you know, the FCC followed its *Open Internet Order* with the issuance of rules restricting and limiting ISPs' data security and practices. In doing so, the FCC chose a more rigid and prescriptive approach to broadband data security and privacy issues than the FTC's traditional case-by-case approach to these topics. The FCC's rules also set standards for broadband providers separate and apart from standards applicable to others in the online space, eschewing the FTC's more comprehensive approach.[12]

---

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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), available at: http://www.freestatefoundation.org/images/May_31_2017_FTC_Panel_Transcript_072017.pdf.

The FCC's *Broadband Privacy Order* attracted strong bipartisan criticism, as former FTC Chairman Jon Leibowitz explained:

> 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.[13]

The implementation of the *Broadband Privacy Order* was later blocked by a joint resolution from the U.S. Congress pursuant to the Congressional Review Act.[14] Thus, as the FCC considers its current NPRM and whether to return ISPs to their former Title I classification, consumer protection regarding Internet ecosystem players has been in flux. The FCC now has an opportunity to end the current uncertainty about consumer protection policy and enforcement by restoring authority over this field to the agency best suited to the task – the Federal Trade Commission.

III. The FTC Possesses the Authority, Expertise, and Capability to Protect Broadband Consumers

The FCC should recognize that the FTC's capabilities, expertise, and analytical approach toward privacy issues make it the preferred agency for addressing online privacy practices across all digital platforms. The FTC has gained extensive experience in protecting privacy from investigating and bringing cases in many industries, including cases involving online privacy and ISPs.

Institutional Capabilities of the FTC

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. The FTC describes the source of its consumer protection authority as follows:

---

[13] 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/.

[14] 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.

> The Federal Trade Commission . . . is an independent U.S. law enforcement agency charged with protecting consumers and enhancing competition across broad sectors of the economy. The FTC's primary legal authority comes from Section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive practices in the marketplace. The FTC also has authority to enforce a variety of sector specific laws, including the Truth in Lending Act, the CAN-SPAM Act, the Children's Online Privacy Protection Act, the Equal Credit Opportunity Act, the Fair Credit Reporting Act, the Fair Debt Collection Practices Act, and the Telemarketing and Consumer Fraud and Abuse Prevention Act. This broad authority allows the Commission to address a wide array of practices affecting consumers, including those that emerge with the development of new technologies and business models.[15]

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 affect consumer privacy, and working with international partners on global privacy and accountability issues.[16]

The FTC's Bureau of Consumer Protection already includes a dedicated Division of Privacy and Identity Protection. This Division works closely with the FTC's other divisions, including the economists in its Bureau of Economics and the investigative staff in field offices across the country, which also have developed their own expertise in consumer protection matters. The FTC currently has field offices in Atlanta, Chicago, Cleveland, Dallas, Los Angeles, New York, San Francisco, and Seattle which "help to amplify our national impact and local presence, and allow us to respond better to the diversity of the U.S. marketplace."[17]

---

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

[16] *Id.*

[17] U.S. Federal Trade Commission, "About the Bureau of Consumer Protection Update" (visited June 25, 2017), available at: https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/about-bureau-consumer-protection.

Expertise of the FTC

Pro-regulation groups seeking to have the FTC retain its Title II regulation of ISP have claimed that the FTC does not have sufficient expertise to protect consumer privacy on the Internet. 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).[18]

This claim significantly mischaracterizes the experience and expertise of the FTC. Maureen K. Ohlhausen, Acting Chairman 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.[19]

In contrast, the FCC has not claimed regulatory authority over privacy matters relating to ISP offerings until recently, so it is behind the curve vis-à-vis the FTC. While the FCC has a strong staff of economists and other experts, as well as its own offices throughout the country, the FCC's personnel have limited experience that is specific to Internet service provider privacy protection.

Even though the FTC has been precluded from privacy enforcement relating to Internet service providers recently as a result of the FCC's Title II classification, it has continued its privacy protection activities in all of the other industries subject to its jurisdiction. And it still has staff with experience in privacy enforcement in telecommunications. Acting Director Pahl of the FTC 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

[18] 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.

[19] 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.

> 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 the standards the government applies are comprehensive, consistent, and pro-competitive.[20]

The FTC Has Established Protocols and Precedents

The FTC website describes the balance the agency must strike in its privacy protection enforcement:

> In all of its privacy work, the FTC's goals have remained constant: to protect consumers' personal information and ensure that consumers have the confidence to take advantage of the many benefits offered in the marketplace.[21]

Acting Chairman Maureen Ohlhausen further explained the FTC's approach to privacy protection:

> Specifically, our unfairness authority prohibits practices that cause substantial harm that is unavoidable by consumers and which is not outweighed by benefits to consumers or competition. Practices that the FTC has found unfair consistently match practices that consumers generally reject. For example, we brought an unfairness case against a data broker that sold highly sensitive financial information to individuals whom the data broker knew or should have known were identity thieves.
>
> Thus, unfairness 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.
>
> Establishing the baseline at the proper level is important. Too low, and we would not stop harmful practices that most consumers oppose. Too high, and we would prohibit services many consumers would prefer. If we set the privacy baseline too high, the privacy preferences of the few are imposed on the many. Our unfairness test's emphasis on real consumer harm and cost-benefit analysis helps ensure that the baseline is in the right place. And the FTC's procedural protections, such as review by our Bureau of Economics and mandatory Commission votes on settlements, create consensus and force changes to

---

[20] 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), available at: http://www.freestatefoundation.org/images/May_31_2017_FTC_Panel_Transcript_072017.pdf.

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

> be incremental. Thus, privacy practices found by the FTC to be unfair are those that reflect consumer consensus (footnotes omitted).[22]

The FTC's record on privacy regulation is hardly immune from criticism, but it has the advantage of being performed by an agency with a long history of applying economic analysis to its enforcement actions. Professor Joshua Wright, a member of the Free State Foundation's Board of Academic Advisors and former FTC Commissioner, in a speech in which he criticized some FTC analysis in privacy cases for a lack of rigor and transparency, nonetheless argues that the FTC still can and should be the intellectual leader in creating economically coherent privacy regulation:

> The FTC is at its best when it combines its unique combination of institutional features. Perhaps the most unique is that the FTC's statutory mandate includes a research and reporting function that distinguishes it from many agencies. The Commission has a long and well-regarded history of conducting its own research and using its authority to produce public reports that examine novel, emerging or otherwise important issues. Privacy should be no exception. The case for strengthening the incentives within the agency for FTC economists to produce their own research, and to be active and engaged scholars in the field of privacy economics, is quite clear.[23]

IV. Federal Antitrust Enforcement Can Also Address Many Consumer Protection Concerns

If the FCC rescinds its Title II public utility regulation of broadband Internet access services and declines to impose new regulations, there are other avenues available to protect consumers and market competition. With the FTC's jurisdiction restored by Title I reclassification, allegedly harmful blocking, degrading, and throttling practices, which are the subject of current prohibitions contained in the *Title II Order*, might be considered violations of the terms of service by broadband ISPs and could be investigated by the FTC as deceptive trade practices that are subject to enforcement actions.[24]

The Department of Justice and the FTC both have authority to investigate and pursue legal action in instances where broadband ISPs engage in anticompetitive practices that could be considered potential antitrust violations. The DOJ Antitrust Division already has an established Telecommunications and Media Enforcement Section that "is responsible for civil antitrust enforcement, competition advocacy, and competition policy in the areas of the Internet, including the services infrastructure and hardware that comprise the Internet."[25]

---

[22] 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.

[23] Joshua D. Wright, "The FTC and Privacy Regulation: The Missing Role of Economics" (speech, George Mason University Law and Economics Center, November 12, 2015), available at: http://masonlec.org/site/rte_uploads/files/Wright_PRIVACYSPEECH_FINALv2_PRINT.pdf.

[24] This is not to suggest that these practices necessarily should be prohibited as per se unlawful or under the antitrust rule of reason, but rather that if ISPs do include them in their terms of service as a matter of business judgment that the FTC would enforce them like any other terms of service.

[25] U.S. Department of Justice, "Telecommunications and Media Enforcement Section," available at: https://www.justice.gov/atr/about-division/telecommunications-and-media-enforcement-section.

Professor Wright explains why antitrust is superior to the *Open Internet Order* approach that banned paid prioritization and other vertical arrangements involving ISPs without proof of harm to competition:

> Despite the 2015 Order ban on vertical agreements by Internet service providers, rule of reason analysis would not similarly result in a total ban on vertical agreements because economics literature clearly indicates that while vertical agreements are capable of harming competition in the manner contemplated by net neutrality proponents, more often than not they are beneficial to consumers. Furthermore, with few exceptions, the [economics] literature does not support the view that these practices are used for anticompetitive reasons. . . . Reclassifying Internet service providers under Title I would restore incentives to invest in broadband markets. A less obvious benefit is that it replaces the 2015 Order's categorical ban on contract arrangements that benefit consumers – including paid prioritization and other vertical arrangements – with antitrust jurisprudence's rule of reason. A close look at the antitrust approach shows not only that it can reach the harms envisioned by net neutrality proponents, but also that it is superior to alternatives that would condemn vertical arrangements in broadband markets without proof of harm to competition.[26]

V. *Ex Post* Regulation Is Generally Superior to *Ex Ante* Regulation in Dynamic Markets

One of the main arguments that had been asserted for retaining Title II classification of ISPs is that only public utility-style prescriptive regulations are sufficient to address broadband privacy and consumer protection concerns. Pro-regulation groups have asserted that the *ex post* enforcement approach of the FTC is too weak, and only prescriptive regulation imposed *ex ante* will protect consumers.

For example, 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).[27]

---

[26] Joshua D. Wright, "Antitrust Provides a More Reasonable Framework for Net Neutrality," Free State Foundation (August 16, 2017), at 3, available at: http://www.freestatefoundation.org/images/Antitrust_Provides_a_More_Reasonable_Framework_for_Net_Neutrality_Regulation_081617.pdf.

[27] 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.

Similarly, the Open Technology Institute has claimed:

> For broadband customers to retain genuine choice over how companies use their data, there should be *ex ante* rules in place, and a regulatory agency tasked with enforcing those rules. It is crucial for Americans to retain an expert agency in charge of protecting their privacy from broadband companies in such a consolidated marketplace. That privacy protection, however, is contingent on the Commission retaining its Title II classification of broadband (citations omitted).[28]

The Open Technology Institute adds:

> 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).[29]

Acting Director of the FTC's Consumer Protection Division Pahl recently explained the flaws in claims that *ex ante* privacy regulation would be superior:

> Some have argued it would be better for the government to address online data security and privacy through regulation rather than proceeding case by case. Rulemaking imposes standards based on a prediction that they will be necessary and appropriate to address future conduct. Case-by-case enforcement, by contrast, involves no such prediction because it challenges and remedies conduct that has already occurred. Of course, such enforcement also has a prophylactic effect as companies look at past enforcement to guide their conduct. The Internet has evolved in ways that we could not have predicted, and is likely to continue to do so. Given the challenges of making predictions about the Internet's future, we need case-by-case enforcement which is strong, yet flexible, like steel guardrails. We do not need prescriptive regulation, which would be an iron cage.[30]

The *ex ante* prescriptive approach has other serious drawbacks, which are especially problematic in a dynamic market with ongoing technological change. Contrary to the claim by the Open Technology Institute, the *ex ante* approach would require constant revision through a notice-and-comment process, which generally will be even more time-consuming than the *ex post* investigative approach long used by the FTC. As such, *ex ante* privacy regulation by the FCC would inevitably fail to anticipate and keep up with rapid changes in Internet technology and practices. As Mr. Pahl explains:

> The call for rules to provide guidance on online data security and privacy also overestimates the guidance provided by prescriptive regulation. Prescriptive regulation, of course, can provide some certainty in the short term. But in fast-changing areas like online data security and privacy, regulations would need to be amended very often to remain current. Amending regulations is cumbersome and time consuming, even where agencies can use APA notice and comment rulemaking procedures. And so such

---

[28] Comments of the Open Technology Institute at New America, WC Docket No. 17-108 (July 17, 2017), at 39-40, available at: https://na-production.s3.amazonaws.com/documents/OTI_NN_COMMENTS_JULY17_FINAL.pdf.
[29] *Id.*, at 38.
[30] 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), available at: http://www.freestatefoundation.org/images/May_31_2017_FTC_Panel_Transcript_072017.pdf.

> amendments by agencies are very unlikely to keep up with the pace of change. Out-of-date rules can be very unclear in their application to new technologies and cause confusion and unintended consequences in the marketplace. [31]

Professor Daniel Lyons, a member of FSF's Board of Academic Advisers, speaking on the same panel as Mr. Pahl, stated:

> The FTC is well equipped to evaluate on a case-by-case basis whether a particular agreement is one that might harm consumers. Using robust law that's been developed from a number of different cases elsewhere in the economy… they have a broader scope informed by a lot more history than the Federal Communications Commission. I agree that the *ex post* review and flexibility the FTC brings is a lot better in a dynamic marketplace than the more rigid FCC *ex ante* rulemaking.[32]

These arguments by pro-regulation groups for *ex ante* privacy regulation by the FCC describe a false choice between an idealized version of *ex post* regulation and a version of *ex post* regulation that ignores some of its more important benefits. Besides failing to appreciate the tremendous institutional advantage of the established FTC Consumer Protection Division over a Federal Communications Commission that has only recently asserted its authority in this area, pro-regulation groups' arguments fail to appreciate the deterrence benefits that are achieved from *ex post* privacy regulation. They also completely fail to consider the impossibility of effectively tailoring *ex ante* regulation to future conduct that has not occurred, as well as to changing market realities. For these reasons, the arguments for *ex ante* regulation over *ex post* regulation provide no support for retaining Title II regulation of broadband providers.

Conclusion

The Federal Trade Commission has been the primary agency for privacy and consumer protection enforcement in the United States for several decades. Its expertise in this field exceeds that of any other federal or state agency and makes the FTC the better choice over the FCC to be the primary federal regulatory agency in charge of addressing privacy and other ISP practices. The reasons the FTC is better suited for this role include the FTC's established institutional structures and expertise gained from its enforcement experience, the FTC's established protocols and precedents from its enforcement activities, and the uncertainty added to the market from having an agency without such attributes assume primary responsibility for this important regulatory function. Broadband consumers will be well served if the FTC takes the lead in fulfilling these important consumer protection functions.

* Theodore R. Bolema is a Senior Fellow of the Free State Foundation, an independent, nonpartisan free market-oriented think tank located in Rockville, Maryland.

---

[31] *Id*.

[32] Daniel Lyons, "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), available at http://www.freestatefoundation.org/images/May_31_2017_FTC_Panel_Transcript_072017.pdf.