*Perspectives from FSF Scholars*
*January 7, 2020*
*Vol. 15, No. 2*

# There is Nothing Anemic About the FTC's Consumer Protection Capabilities

**by**

**Theodore R. Bolema ***

## I. Introduction and Summary

The D.C. Circuit's recent decision in *Mozilla v. FCC* held that the FCC acted within its legal authority in its *Restoring Internet Freedom Order* (*RIF Order*) to reclassify Internet service provider (ISP) services from Title II telecommunication services to Title I information services. The *Mozilla* decision nonetheless was not a complete win for the Federal Communications Commission. This *Perspectives* provides a critique of a specific part of the *Mozilla* decision in which the court was critical of the *RIF Order*'s justification for why Federal Trade Commission enforcement and the antitrust laws are sufficient to protect consumers from unfair and deceptive practices on the Internet. Even though the D.C. Circuit majority ultimately sided with the FCC on this issue, it criticized the FCC's explanation as "anemic" and said that it "barely survives arbitrary and capricious review on this issue." While these characterizations did not affect the outcome, they were wrong.

Federal Trade Commission officials, as well as Free State Foundation scholars, have long argued that consumers will be well protected by the FTC after the *RIF Order* – indeed, better than they were while the *Open Internet Order* precluded FTC enforcement by virtue of classifying ISPs as Title II telecommunications services. With the FTC's jurisdiction restored, allegedly harmful

blocking, degrading, and throttling practices, which were prohibited by the *Open Internet Order*, might be considered violations of the terms of service by broadband ISPs and could be investigated by the FTC as deceptive trade practices subject to enforcement actions.

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 DOJ's Antitrust Division and the FTC both have authority to investigate and pursue enforcement actions in instances where broadband ISPs engage in anticompetitive practices that could be considered potential antitrust violations.

A recent enforcement action, taken by the FTC after the *Mozilla* decision, demonstrates how FTC enforcement can address the concerns that the 2015 FCC majority claimed were the motivation for the *Open Internet Order*. AT&T recently agreed to pay $60 million to settle a complaint that the wireless provider misled millions of its smartphone customers by charging them for "unlimited" data plans while failing to adequately disclose that AT&T would slow their data speeds if they reach a certain amount of data use in a given billing cycle. As part of the settlement, AT&T is prohibited from making any representation about the speed or amount of its mobile data, including that it is "unlimited," without disclosing any material restrictions on the speed or amount of data.

While the D.C. Circuit decision regarding antitrust law enforcement and the FTC's consumer protection authority reaches the right conclusion, the court's claim that FTC enforcement is weak is incorrect and appears to ignore much of the evidence provided in the *RIF Order*. The *RIF Order*'s case for FTC enforcement is far from weak. A 12-page section of the *RIF Order* contained extensive analysis and dozens of citations supporting the FCC's analysis. The citations in these sections are to law review articles, peer-reviewed economic literature, declarations from prominent economists, and numerous regulatory filings.

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. According to this argument, the *ex post* enforcement approach of the FTC and DOJ is too weak, and only prescriptive regulation imposed *ex ante* will protect consumers. But *ex post* enforcement has a strong deterrent effect, as demonstrated by the recent enforcement action against AT&T. And the *ex ante* prescriptive approach has serious drawbacks, which are especially problematic in a dynamic market with ongoing technological change. The *ex ante* approach would require constant revision through a notice-and-comment process, which generally would 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.

It is unfortunate that the court in the *Mozilla* decision criticized the FCC's defense of its reliance on antitrust and consumer protection by the FTC and DOJ as "anemic" and "barely surviv[ing] arbitrary and capricious review on this issue." The *RIF Order* included much more meaningful support for this position than the court acknowledged. But even aside from whether the FCC's analysis was sufficient to support the *RIF Order*'s reclassification of ISPs as Title I services, the FCC's decision is correct on the merits. Broadband consumers are well served by the FTC taking

the lead in fulfilling these important consumer protection functions for all of the information and content providers in the Internet ecosystem, whether they are web giants like Google and Facebook or ISPs like Comcast and Verizon.

## II. The 2019 *Mozilla* Decision

The D.C. Court of Appeals recently largely rejected challenges to a number of aspects of the FCC's 2017 *Restoring Internet Freedom Order*.[1] These challenges were based on the *RIF Order* largely repealing the FCC's 2015 *Open Internet Order*,[2] which imposed a number of restrictions on Internet Service Providers (ISPs) in the name of promoting "net neutrality." In particular, the *Open Internet Order* classified ISPs as "telecommunications services," which allowed the FCC to prohibit ISPs from blocking, throttling, or charging for priority Internet traffic, among other regulatory powers claimed by the FCC. The 2017 *RIF Order* restored ISPs to the status of "information services."

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 by the FCC. Title II services may also be regulated only by the FCC, with other federal agencies mostly blocked from imposing their own regulations or consumer protection rules on Title II service.[3] Before 2015, ISPs were classified as Title I information services, which allowed broadband services to develop and thrive with relatively light touch regulation.

By reclassifying broadband providers as Title II telecommunications services, the 2015 *Open Internet Order* effectively stripped the FTC of jurisdiction over broadband ISP practices that are potentially harmful to consumers, including practices involving online privacy. By restoring ISPs as information services, the 2017 *RIF Order* returned to the Federal Trade Commission, as well as other state and federal enforcement agencies, the same authority over ISPs that they have over other market participants under their general enforcement statutes.

The D.C. Circuit's decision in *Mozilla v. FCC* held that the FCC acted within its legal authority to reclassify ISP services from Title II telecommunication services to Title I information services.[4] The *Mozilla* decision was nonetheless not a complete win for the FCC. The D.C. Circuit pushed back on several specific provisions in the *Open Internet Order* that related to

---

[1] *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.

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

[3] 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: https://freestatefoundation.org//wp-content/uploads/2019/08/FSF-Initial-Comments-Restoring-Internet-Freedom-071717-1.pdf.

[4] Mozilla Corporation v. Federal Communications Commission and United States of America, United States Court of Appeals for the District of Columbia Circuit, No 18-1051 (decided October 1, 2019), available at: https://www.cadc.uscourts.gov/internet/opinions.nsf/FA43C305E2B9A35485258486004F6D0F/$file/18-1051-1808766.pdf.

Internet access for public safety purposes, pole attachments for broadband deployment, and benefit eligibility for low-income households. The *Mozilla* majority also struck down a provision in the *RIF Order* that would, as a blanket matter, have preempted states from passing their own net neutrality laws that contravened the FCC's deregulatory policy. The court's majority did acknowledge that, even under its theory, the FCC may possess to review such state laws individually and preempt those that are inconsistent with the FCC clearly-articulated policies.[5]

This *Perspectives* provides a critique of a specific part of the *Mozilla* decision in which the D.C. Circuit Court was critical of the FCC's justification in the *RIF Order* for why the antitrust laws and FTC enforcement are sufficient to protect consumers from unfair and deceptive practices on the Internet.

In *Mozilla*, the court upheld the broad regulatory framework that the *RIF Order* intended for ISPs:

> The Commission found that "[i]n the unlikely event that ISPs engage in conduct that harms Internet openness," legal regimes like "antitrust law and the FTC's authority under Section 5 of the FTC Act to prohibit unfair and deceptive practice" will provide protection for consumers. The Commission reasoned that antitrust and consumer protection laws are particularly well-suited to addressing openness concerns because "they apply to the whole of the Internet ecosystem, including edge providers, thereby avoiding tilting the playing field against ISPs and causing economic distortions by regulating only one side of business transactions on the Internet." Petitioners argue that reliance on antitrust and consumer protection law was an improper delegation of authority. We disagree.[6]

The *Mozilla* court then explained why, as a general principle, the FCC could conclude that the antitrust and consumer protection laws provide sufficient protection against the relevant types of bad conduct on the Internet:

> But the Commission has not "mechanically accept[ed] the standards" of other laws as satisfying its own. Instead, it has conducted an independent assessment of the degree of problematic conduct that has been and will be committed by broadband providers and whether, as a policy matter, the benefits of restricting that conduct outweigh the costs. A reasonable piece of that policy-making puzzle, then, is an assessment of other regulatory regimes that might already limit the conduct in question. Therefore, it was not impermissible for the Commission to recognize that the Department of Justice and Federal Trade Commission have the ability to police blocking and throttling practices *ex post*.[7]

---

[5] For an analysis of the implication of the *Mozilla* decision striking down the provision in the RIF Order that would have preempted states from passing their own net neutrality laws, see Daniel A. Lyons, "Conflict Preemption of State Net Neutrality Efforts After *Mozilla*," *Perspectives from FSF Scholars*, Vol. 14, No. 29 (October 4, 2019), available at: https://freestatefoundation.org//wp-content/uploads/2019/10/Conflict-Preemption-of-State-Net-Neutrality-Efforts-After-Mozilla-100419.pdf.

[6] Mozilla Corporation v. FCC at 91.

[7] Mozilla Corporation v. FCC at 92.

Even though the D.C. Circuit sided with the FCC on this issue, it nonetheless sharply criticized the FCC's explanation for its decision, characterizing it as "anemic" and asserting that it "barely survives arbitrary and capricious review on this issue." According to the Court:

> To be sure, the Commission's discussion of antitrust and consumer protection law is no model of agency decisionmaking. The Commission theorized why antitrust and consumer protection law is preferred to ex ante regulations but failed to provide any meaningful analysis of whether these laws would, in practice, prevent blocking and throttling. For example, the Commission opines that "[m]ost of the examples of net neutrality violations discussed in the Title II Order could have been investigated as antitrust violations," but fails to explain what, if any, concrete remedies might address these antitrust violations. It is concerning that the Commission provides such an anemic analysis of the safety valve that it insists will limit anticompetitive behavior among broadband providers. Nonetheless, we cannot go so far as to say that this failure is so profound that the agency "entirely failed to consider an important aspect of the problem," or otherwise engaged in unreasoned decisionmaking. That is especially true because the Commission viewed those laws as only one part of a larger regulatory and economic framework that it believes will limit broadband providers' engagement in undesirable practices. The Commission barely survives arbitrary and capricious review on this issue.[8]

As discussed below, FTC officials, as well as Free State Foundation scholars, have long argued that consumers will be well protected by the FTC after the *RIF Order*, and better than they would be if the FCC precluded FTC enforcement by classifying ISPs as Title II telecommunications services. Moreover, the *RIF Order* and documents provided on appeal make that case, but evidently were given too little weight by the D.C. Circuit.

## III. The *Mozilla* Decision Was Too Harsh on the FCC's *RIF Order* Analysis

The D.C. Circuit decision regarding antitrust law enforcement and the FTC's consumer protection authority reaches the right conclusion, but is too harsh and appears to ignore much of the evidence provided by the FCC majority in the *RIF Order*. Contrary to the criticism by the court, the *RIF Order*'s case for FTC enforcement is far from weak. A 12-page section of the *RIF Order* contained extensive analysis and dozens of citations supporting the FCC's analysis.[9] The citations in these sections are to law review articles, peer-reviewed economic literature, declarations from prominent economists, and numerous regulatory filings. Moreover, there are plenty of other good reasons why the FTC can protect consumers from harmful anticompetitive conduct by ISPs, as will be discussed in the remaining sections.

Indeed, a recent enforcement action, taken by the FTC after the *Mozilla* decision, demonstrates that FTC enforcement has teeth and can protect consumers from the harms the 2015 *Open Internet Order* was intended to address. AT&T agreed to pay $60 million to settle a complaint that the wireless provider misled millions of its smartphone customers by charging them for "unlimited" data plans while failing to adequately disclose that AT&T would slow their data speeds if they reached a certain amount of data use in a given billing cycle. According to the

[8] Mozilla Corporation v. FCC at 92-93.
[9] RIF Order, ¶¶141-54.

FTC's press release, "'AT&T promised unlimited data—without qualification—and failed to deliver on that promise,' said Andrew Smith, Director of the FTC's Bureau of Consumer Protection. 'While it seems obvious, it bears repeating that Internet providers must tell people about any restrictions on the speed or amount of data promised.'" As part of the settlement, AT&T is prohibited from making any representation about the speed or amount of its mobile data, including that it is "unlimited," without disclosing any material restrictions on the speed or amount of data.[10]

Dr. Jerry Ellig, who was the Chief Economist for the FCC at the time of the *RIF Order*, explained why he strongly disagrees with how the *Mozilla* decision characterized the FCC's analysis:

> I take exception to the court's conclusion that the FCC's analysis of antitrust and consumer protection was "anemic," because I know what is in the FCC order and in the record on this topic. The FCC order discusses the FTC's prosecution of TracFone for throttling (¶ 141). The order also notes that ISPs' public commitments not to block or throttle are enforceable under Section 5 of the FTC Act (¶ 142), points to an FTC report which suggested that an ISP could be prosecuted for treating traffic from different edge providers differently if it did not inform customers and obtain their consent (¶ 141), and cites empirical economics literature that demonstrates the deterrent effect of antitrust laws (¶ 152). The antitrust and consumer protection analysis also draws heavily on comments submitted by the FTC's acting chairman, Maureen Ohlhausen, as well as a separate comment from the FTC staff. I can only conclude that no one brought these passages in the order to the court's attention.[11]

If any appeal is to be made, or if policymakers in Congress or the states look to make legislative changes based on claims that the FTC consumer protection is inadequate to address any anticompetitive concerns over ISP conduct, the defenders of the *RIF Order* should be prepared to push back against the argument by the D.C. Circuit that the FCC made a weak case for FTC enforcement.

## IV. The Authority and Capability of the FTC to Protect Broadband Consumers

The recent settlement with AT&T regarding how it promoted its plans as offering unlimited data is hardly an anomaly. Before the 2015 *Open Internet Order*, and again since the *2017 RIF Order*,

---

[10] Federal Trade Commission, Office of Public Affairs, "AT&T to Pay $60 Million to Resolve FTC Allegations It Misled Consumers with 'Unlimited Data' Promises," November 5, 2019, available at: https://www.ftc.gov/news-events/press-releases/2019/11/att-pay-60-million-resolve-ftc-allegations-it-misled-consumers.

[11] Jerry Ellig, "Implications of Mozilla for Agency Economic Analysis," Notice and Comment: A Blog from the Yale Journal on Regulation and the ABA Section of Administrative Law & Regulatory Practice, October 10, 2019, available at: https://yalejreg.com/nc/implications-of-mozilla-for-agency-economic-analysis-by-jerry-ellig/, citing Comment of Maureen K. Ohlhausen, Acting Chairman, Federal Trade Commission, WC Docket No. 17-108 (July 17, 2017), available at: https://www.ftc.gov/system/files/documents/public_statements/1231563/mko_rif_comment_7-17-2017_final.pdf, and Comment of the Staff of the Federal Trade Commission, WC Docket No. 17-108 (July 17, 2017), available at: https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-bureau-competition-bureau-economics-federal-trade/ftc_staff_comment_to_fcc_wc_docket_no17-108_7-17-17.pdf.

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

> 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.[12]

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.[13]

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

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

country, which also have developed their own expertise in consumer protection matters.[14] 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 has brought hundreds of privacy and data security cases protecting billions of consumers.

Pro-regulation groups seeking to have the Federal Trade Commission retain its Title II regulation of ISP have claimed that the FTC does not have sufficient expertise to protect consumer privacy on the Internet.[15] Such claims significantly mischaracterize the experience and expertise of the FTC. Maureen K. Ohlhausen, Acting Chairman of the Federal Trade Commission at the time of the *RIF Order*, explained the FTC's expertise over privacy issues:

> 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.[16]

In contrast, the FCC has not claimed regulatory authority over privacy matters relating to Internet service provider offerings until recently. How the FCC was unprepared for the authority it asserted under the *Open Internet Order* was exposed almost immediately when the FCC adopted its 2016 *Broadband Privacy Order*.[17] 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* necessarily was to unfairly disadvantage broadband ISPs and confuse consumers with its uneven application.[18]

---

[14] U.S. Federal Trade Commission, "About the Bureau of Consumer Protection Update" (visited December 2, 2019), available at: https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/about-bureau-consumer-protection.

[15] For example, comments submitted by Public Knowledge and Common Cause while the FCC was considering the *RIF Order* 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.

[16] 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.

[17] 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.

[18] 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:

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.[19]

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.[20] By reclassifying broadband providers as Title I information services, the *RIF Order* has once again returned jurisdiction over broadband ISP practices that are potentially harmful to consumers, including practices involving online privacy, to the agency best suited to the task – the Federal Trade Commission.[21]

## V. Federal Antitrust Enforcement Can Address Many Consumer Protection Concerns

With the FTC's jurisdiction restored by Title I reclassification, allegedly harmful blocking, degrading, and throttling practices, which are the subject of the prohibitions that were contained

---

https://ecfsapi.fcc.gov/file/1031625753193/FSF%20Reply%20Comments%20Re%20Protecting%20the%20Privacy%20of%20Customers%20of%20Broadband%20and%20Other%20Telecommunications%20Services%20031617.pdf.

[19] 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/.

[20] 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.

[21] Thomas Pahl, then-Acting Director of the FTC's Bureau of Consumer Protection, speaking at the Free State Foundation's Ninth Annual Telecom Policy Conference, described what the public could expect after jurisdiction over broadband ISP privacy practices is returned to the FTC: "The FTC is ready, willing, and able to protect the data security and privacy of broadband subscribers . . . .We have a wealth of consumer protection and competition experience and expertise, which we will bring to bear on online data security and privacy laws. We will apply data security and privacy standards to all companies that compete in the online space regardless of whether the companies provide broadband services, data analysis, social media, or other services. Our approach would ensure the standards the government applies are comprehensive, consistent, and pro-competitive." 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: https://freestatefoundation.org//wp-content/uploads/2019/09/May-31-2017-FTC-Panel-Transcript-072017.pdf.

in the *Open Internet Order*, might be considered violations of the broadband ISPs' terms of service and could be investigated by the FTC as deceptive trade practices that are subject to enforcement actions.[22]

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."[23]

Professor Joshua Wright, a member of the Free State Foundation's Board of Academic Advisors and former FTC Commissioner, explains why antitrust is superior to the *Open Internet Order* approach that banned paid prioritization and other vertical arrangements involving ISPs without requiring 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.[24]

## VI. *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*

---

[22] 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.

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

[24] Joshua D. Wright, "Antitrust Provides a More Reasonable Framework for Net Neutrality," Free State Foundation (August 16, 2017), at 3, available at: https://freestatefoundation.org/wp-content/uploads/2019/12/Antitrust-Provides-a-More-Reasonable-Framework-for-Net-Neutrality-Regulation-081617.pdf.

enforcement approach of the FTC and DOJ is too weak, and only prescriptive regulation imposed *ex ante* will protect consumers.[25]

Thomas Pahl, then-Acting Director of the FTC's Bureau of Consumer Protection, speaking at the Free State Foundation's Ninth Annual Telecom Policy Conference, explained the flaws in claims that *ex ante* privacy regulation is the better approach:

> 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.[26]

The *ex ante* prescriptive approach has other serious drawbacks, which are especially problematic in a dynamic market with ongoing technological change. The *ex ante* approach would require constant revision through a notice-and-comment process, which generally would be even more time-consuming than the *ex post* investigative approach long used by the FTC. [27] As such, *ex ante* privacy regulation by the FCC inevitably would fail to anticipate and keep up with rapid changes in Internet technology and practices.[28]

---

[25] 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)." 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] As Mr. Pahl further explained: "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 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." 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: https://freestatefoundation.org//wp-content/uploads/2019/09/May-31-2017-FTC-Panel-Transcript-072017.pdf.

[27] *Id.*

[28] Professor Daniel Lyons, a member of FSF's Board of Academic Advisers, speaking on the same panel as Mr. Pahl, added: "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

Pro-regulation groups' arguments fail to appreciate the deterrence benefits that are achieved from *ex post* privacy regulation. They also 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 do not justify having the FCC take over authority from the FTC as the lead enforcement agency on the Internet.

**Conclusion**

It is unfortunate that the Court of Appeals for the D. C. Circuit in the *Mozilla* decision criticized the FCC's defense of its reliance on antitrust and consumer protection by the FTC and DOJ as "anemic" and "barely surviv[ing] arbitrary and capricious review on this issue." The *RIF Order* contained much more support for this position than the court acknowledged. But even aside from whether the FCC's analysis was sufficient to support the *RIF Order*'s reclassification of ISPs as Title I services, the FCC's decision is correct on the merits.

The Federal Trade Commission has been the primary agency for privacy and consumer protection enforcement in the United States for several decades, as well as sharing antitrust enforcement with the Department of Justice. Their expertise in this field exceeds that of any other federal or state agency and makes antitrust enforcement by these agencies and consumer protection enforcement by the FTC the better choice over the FCC's heavy-handed regulatory approach that would respond much too slowly in a technologically dynamic market. Broadband consumers are well served by the FTC taking the lead in fulfilling these important consumer protection functions.

* 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. The Free State Foundation is an independent, nonpartisan free market-oriented think tank located in Rockville, Maryland.

---

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." 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 https://freestatefoundation.org//wp-content/uploads/2019/09/May-31-2017-FTC-Panel-Transcript-072017.pdf.