Santa Clara University
School of Law

Santa Clara Law Review

Volume 58 | Number 1 Article 2

6-2-2018

Broadband Privacy

Sean Howell

BROADBAND PRIVACY

Sean Howell*

TABLE OF CONTENTS

* Sean is a law clerk to the Honorable Charles R. Breyer (N.D. Cal). He is also a former Ninth Circuit clerk and a recent graduate of Berkeley Law. He is interested in the implications of technological change for telecommunications policy, data-protection law, antitrust, and speech regulation. Many thanks to Christopher Klapperich and the staff of the Santa Clara Law Review for their thoughtful suggestions and their incisive, careful editing.

INTRODUCTION

When the Obama-era Federal Communications Commission (FCC) issued the Open Internet Order, establishing net neutrality rules, its action had the side effect of handing the FCC responsibility for policing the data-protection practices of broadband internet access providers ("broadband providers").[1] The Commission took an aggressive approach to broadband privacy—pursuing the first-ever privacy enforcement action against a broadband provider, and passing what was likely the most stringent prescriptive data-privacy regulation in American history to date. But the FCC's patrol of the privacy beat was short-lived. Following the election of President Donald Trump, the Commission's new Republican majority suspended the broadband privacy rules, and Congress later scrapped them altogether. The Commission subsequently repealed the Open Internet Order, a move that had the collateral effect of restoring jurisdiction over broadband privacy to the Federal Trade Commission (FTC).

While the FCC's detailed privacy rules are no longer, they continue to inspire debate. Several state legislatures have taken up the issue of whether they should enact their own broadband privacy rules, modeled after the repealed federal regulations.[2] In addition, the FCC's rules provide a helpful jumping-off point for analyzing the existing state of broadband-privacy enforcement, and for assessing the shape that enforcement should take under the FTC. The privacy practices of broadband providers have largely flown under the radar, with the practices of "edge providers"[3] such as Google and Facebook receiving

1. The Open Internet Order reclassified broadband as a common-carrier service under Title II of the Telecommunications Act of 1996. In re Protecting and Promoting the Open Internet, 30 FCC Rcd. 5601, 5604-5607 (2015) [hereinafter Open Internet Order]. This indirectly stripped the Federal Trade Commission (FTC) of jurisdiction to police broadband providers' privacy practices under Section 5 of the FTC Act, because Section 5 does not apply to common carriers. *See* 15 U.S.C. § 45; *see also infra* Part I at 104–09.

2. *See* Ernesto Falcon, Legislative Analysis, *How Silicon Valley's Dirty Tricks Helped Stall Broadband Privacy in California*, ELECTRONIC FRONTIER FOUNDATION (Oct. 23, 2017), https://www.eff.org/deeplinks/2017/10/how-silicon-valleys-dirty-tricks-helped-stall-broadband-privacy-california [hereinafter Falcon, *Broadband Privacy in California*].

3. Edge providers are firms that use the broadband network to provide content, applications, and other services to end users. *See* Open Internet Order, *supra* note 1, at 5608.

the lion's share of attention from consumer advocates, media outlets, academics, and regulators. But large broadband providers' ability to collect data on individuals are approached by those of only a handful of firms, and their privacy practices are accordingly worthy of attention.

This Article seeks to untangle some of the knottier issues regarding broadband privacy. Part I provides a brief introduction to privacy issues that have arisen in the broadband space.[4] Part II offers the first comprehensive comparison between the FCC's repealed broadband privacy rules and the FTC's likely enforcement of broadband privacy under its authority to police unfair and deceptive trade practices.[5] Privacy advocates lamented the loss of the FCC as a broadband-privacy enforcer, apparently assuming that FTC enforcement would not be as robust. However, looking to past FTC enforcement actions and policy statements to anticipate the Commission's likely approach to broadband privacy, this Article posits that the FTC's enforcement regime is actually likely to be quite similar to the FCC's aborted regulation in most respects. While there are a couple of points on which FTC regulation will probably be less stringent, this fact will likely benefit consumers on the whole by fostering competition in nearby data-intensive markets. Moreover, the FTC's loose, standards-based procedural approach is preferable to the FCC's highly prescriptive rules because it provides needed regulatory flexibility in a rapidly evolving area.

A number of questions remain about the details of how the FTC will enforce privacy standards against broadband providers. Part III examines three particularly pressing questions.[6] First, should privacy standards be enforced differently against broadband providers than against other firms? That is, do broadband providers' market positions and access to data, as well as the relative lack of visibility of their data-collection practices, justify the application of stricter privacy rules? Second, should the FTC make an exception to its privacy standards for the practice of scrutinizing Internet traffic in order to provide different treatment to different types of content and applications? Conversely, should the Commission use its privacy rules as a backdoor means of "net neutrality" regulation? Third, how is the FTC's enforcement of broadband providers' privacy practices likely to play out on the ground?

---

4. *See infra* Part I.
5. *See infra* Part II.
6. *See infra* Part III.

I. A BRIEF INTRODUCTION TO BROADBAND PRIVACY

There has been much discussion of the ability of so-called "edge providers" such as Google and Facebook to monitor user behavior online.[7] Until fairly recently, however, comparatively little attention has been paid to the implications of data collection by broadband internet access providers—firms like AT&T, Comcast, and Time Warner that provide access to substantially all Internet endpoints at speeds faster than dial-up, through wired connections and/or cellular networks.[8]

Internet service providers (ISPs) have been testing various monitoring practices for years, but have usually backed away from collecting customers' data following detection, bad publicity, and legal action. The first public attempt by a stateside telecommunications (telecom) provider to collect, store, and process user data for advertising purposes came in 2008, when Charter partnered with a firm called NebuAd to collect and analyze information on broadband customers' browsing behavior, using the information to help content providers target advertisements to web users.[9] A consumer backlash followed, however, and Charter quickly suspended its plans.[10]

In 2011, two Berkeley computer scientists discovered that ISPs were tracking consumers' use of certain search terms for marketing purposes.[11] The providers again quickly announced that they were dropping the practice.[12]

Most recently, reports emerged in 2014 that Verizon Wireless had injected unique identifiers known as tracking headers or "supercookies"[13] into the Internet traffic of over 100 million customers

---

7. *See, e.g.*, Jeffrey Rosen, *The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google*, 80 FORDHAM L. REV. 1525 (2012).

8. 47 CFR § 8.2(a).

9. Saul Hansell, *Charter Suspends Plans to Sell Customer Data to Advertisers*, N.Y. TIMES (June 24, 2008), https://bits.blogs.nytimes.com/2008/06/24/charter-suspends-plan-to-sell-customer-data-to-advertisers/.

10. *Id.*

11. Jim Giles, *US Internet Providers Hijacking Users' Search Queries*, NEW SCIENTIST (Aug. 9, 2011), https://www.newscientist.com/article/dn20768-us-internet-providers-hijacking-users-search-queries/.

12. *Id.*

13. "Supercookies" refers to unique identifiers inserted into the headers of users' web traffic in order to track users across the web and serve targeted advertisements to them. In re Cellco P'ship d/b/a Verizon Wireless, 31 FCC Rcd. 1843, 1847 (2016) [hereinafter Verizon Order]. They are known as "supercookies" because users cannot easily delete them, as they can with the cookies that websites use to track users. *See* Robert McMillan, *Verizon's 'Perma-Cookie' Is a Privacy-Killing Machine*, WIRED (Oct. 27, 2014), https://www.wired.com/2014/10/verizons-perma-cookie/.

on its mobile network.[14] This practice allowed Verizon and its partners to gather data on the web-browsing habits of those customers, and made it impossible for customers to prevent the tracking except by encrypting their web traffic or using a virtual private network (VPN).[15] A subsequent FCC investigation found that Verizon had begun inserting tracking headers into internet traffic as early as 2012.[16] AT&T acknowledged that it had also engaged in the practice, and agreed to desist.[17] The FCC eventually filed a complaint against Verizon, and the parties reached a settlement.[18]

Shortly thereafter, the FCC began developing comprehensive rules governing broadband providers' collection, storage, and use of customer data.[19] At least in theory, broadband privacy had previously fallen within the FTC's regulatory domain, pursuant to the Commission's capacious authority to police "unfair or deceptive acts or practices in or affecting commerce" under Section 5 of the FTC Act.[20] However, the FCC's 2015 reclassification of broadband as a common-carrier service pursuant to Title II of the Communications Act[21] indirectly stripped the FTC of its privacy jurisdiction over broadband providers, because Section 5 does not apply to common carriers.[22] Accordingly, the FCC reasoned that it would have to assume responsibility for broadband privacy if it wished to avoid a "gap" in the American privacy regime.[23]

In the days leading up to the 2016 presidential election, the Obama FCC rolled out its Broadband Privacy Order, a 169-page whopper (excluding appendices) that covered the collection, storage, and use of customer data by broadband providers.[24] The order was short-lived, however. Before it went into effect, the FCC stayed it in

14. Verizon Order, *supra* note 12, at 1847–51; *see also* McMillan, *supra* note 12.

15. *Id.* at 1847–51.

16. *Id.*

17. Elizabeth Weise, *AT&T Ends Tracking of Customers by "Supercookie,"* USA TODAY (Nov. 14, 2014), https://www.usatoday.com/story/tech/2014/11/14/att-supercookies-tracking/19041911/.

18. Verizon Order, *supra* note 12, at 1843–44.

19. In re Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 31 FCC Rcd. 2500, 2508 (2016) [hereinafter Broadband Privacy NPRM].

20. 15 U.S.C. § 45(a)(1).

21. Open Internet Order, *supra* note 1, at 5604–07.

22. *See* 15 U.S.C. § 45(a)(2).

23. In re Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket. No. 16–148, 2016 WL 6538282, 14051 (2016) [hereinafter Broadband Privacy Order].

24. *See generally id.*

part.[25] Shortly thereafter, Congress passed and President Trump signed legislation repealing it.[26] The other shoe dropped when the Trump FCC repealed the Open Internet Order, terminating the classification of broadband providers as common carriers and thereby restoring the FTC's jurisdiction over those providers' privacy practices pursuant to Section 5.[27]

Consumer advocates met the repeal of the FCC's rules with dismay. "Today's vote means that Americans will never be safe online from having their most personal details stealthily scrutinized and sold to the highest bidder," Jeffrey Chester, executive director of the Center for Digital Democracy, told *The Washington Post*.[28] Obama holdovers at both the FCC and FTC issued a press release calling the move "the antithesis of putting #ConsumersFirst."[29] State legislators introduced bills to reinstate the FCC's rules at the state level.[30]

Meanwhile, the newly installed Republican chairs of the FCC and FTC urged people not to believe the "hyperventilating headlines" warning of dire privacy consequences.[31] They asserted that the FCC's rules would have distorted competition in the Internet ecosystem, and that returning privacy jurisdiction over broadband providers to the FTC

---

25. In re Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 30 FCC Rcd. (2017), https://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0301/FCC-17-19A1.pdf [hereinafter Protecting the Privacy of Customers].

26. Steve Lohr, *Trump Completes Repeal of Online Privacy Protections from Obama Era*, N.Y. TIMES (April 3, 2017), https://www.nytimes.com/2017/04/03/technology/trump-repeal-online-privacy-protections.html. The Trump FCC had stayed the order the day before it was scheduled to go into effect. Protecting the Privacy of Customers*, supra* note 24.

27. FCC, In re Restoring Internet Freedom, Declaratory Ruling, Report and Order, and Order, 2018 WL 305638, at *8–10, *23–26 (Jan. 4, 2018). Note that the repeal order might be subject to challenge under the Administrative Procedure Act. *See, e.g.*, Nat'l Cable and Telecom. Ass'n v. Brand X Internet Servs., 545 U.S. 967, 981–82 (2005) (agency action arbitrary and capricious where agency fails to adequately explain reasons for change of course).

28. Brian Fung, *The House Just Voted to Wipe Away the FCC's Landmark Internet Privacy Protections*, WASH. POST (March 28, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/03/28/the-house-just-voted-to-wipe-out-the-fccs-landmark-internet-privacy-protections/.

29. Press Release, *Joint Statement of FCC Commissioner Mignon Clyburn and FTC Commissioner Terrell McSweeny*, FCC (Mar. 23, 2017), https://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0323/DOC-344042A1.pdf.

30. *See* Falcon, *Broadband Privacy in California*, *supra* note 2.

31. Ajit Pai & Maureen Ohlhausen, *No, Republicans Didn't Just Strip Away your Internet Privacy Rights*, WASH. POST (April 4, 2017), https://www.washingtonpost.com/opinions/no-republicans-didnt-just-strip-away-your-internet-privacy-rights/2017/04/04/73e6d500-18ab-11e7-9887-1a5314b56a08_story.html.

would ensure a "comprehensive framework that will protect . . . privacy throughout the Internet."[32]

Part II evaluates these competing claims in comparing the FTC's likely enforcement of broadband privacy to the FCC's Broadband Privacy Order. First, however, understanding the issues in play requires a rudimentary technical understanding of broadband providers' ability to monitor the traffic that flows through their networks.

When a user types a web address into her browser, the broadband provider transmits the website's contents from the edge provider to the user in the form of "packets."[33] Each of these packets carries data about the site.[34] The packets are reassembled when they reach the user to form intelligible content.[35]

Each packet contains several different types of information. Two are relevant to our purposes. First, packets contain "headers," which convey an internet protocol (IP) address that tells the broadband provider where it must route the packet.[36] Second, packets contain an "application payload," which transmits the substance of the data being conveyed.[37]

In inserting supercookies into customers' traffic, Verizon and AT&T only interacted with the headers of packets, appending a unique identifier to the address information.[38] If the recipient website had an arrangement with the broadband provider, the website could match the identifier to a particular user and access the provider's store of information about that user.[39] It could then use that information to serve the user relevant ads.[40]

The header is the only part of the packet a broadband provider must read in order to route traffic.[41] However, carriers have also

---

32. *Id.*

33. JONATHAN E. NUECHTERLEIN & PHILIP J. WEISER, DIGITAL CROSSROADS: AMERICAN TELECOMMUNICATIONS POLICY IN THE DIGITAL AGE 42 (1st ed. 2007).

34. *Id.*

35. *Id.*

36. Duncan Geere, *How Deep Packet Inspection Works*, WIRED (Apr. 27, 2012), http://www.wired.co.uk/article/how-deep-packet-inspection-works.

37. *Id.*

38. Jacob Hoffman Andrews, *Verizon Injecting Perma-Cookies to Track Mobile Customers, Bypassing Privacy Controls*, ELECTRONIC FRONTIER FOUNDATION (Nov. 3, 2014), https://www.eff.org/deeplinks/2014/11/verizon-x-uidh; *see also* Jacob Davidson, *Verizon and AT&T Snooping on Customers' Web Activity*, TIME (Nov. 4, 2014), http://time.com/money/3556165/verizon-att-supercookies/.

39. *Id.*

40. *Id.*

41. *See* Geere, *supra* note 34.

developed the ability to examine the payload of the packet.[42] This practice is known as "deep packet inspection," or "DPI."[43] It has attracted much attention from data-privacy advocates, because it enables broadband providers to view potentially sensitive contents of messages sent by users—for example, e-mails, chats, and information entered into web forms.[44] However, the practice is not yet cost-effective or widely used, and by some accounts may never be.[45] Nick Feamster, professor of computer science at Princeton University, has called DPI a "red herring" in discussions of broadband privacy because it remains too expensive to be widely used,[46] notwithstanding dramatic declines in data-storage costs in recent years.[47] AT&T and Verizon have insisted that they do not use deep packet inspection for marketing purposes, and would not do so without first seeking affirmative express consent from customers.[48] Accordingly, broadband providers' ability to track users' movements around the web via packet headers appears to be the more pressing privacy issue at the moment.[49]

---

42. *Id.*

43. *Id.*

44. *Id.*

45. Letter from Nick Feamster, Professor, Dep't of Computer Sci., Princeton U., to Chairman & Comm'rs of the Fed. Comm. Comm'n, RE: Docket. No. 16-106, Protecting the Privacy of Customers of Broadband and other Telecommunications Services 6 (May 27, 2016), https://ecfsapi.fcc.gov/file/60002079367.pdf [hereinafter Feamster Comment Letter].

46. *Id.*

47. John Hagel et al., *From Exponential Technologies to Exponential Innovation*, DELOITTE Figure 2 (Oct. 4, 2013), http://dupress.com/articles/from-exponential-technologies-to-exponential-innovation/ (noting drop in data storage costs $569 to $0.03 per gigabyte between 1992 and 2002).

48. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 55 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [hereinafter FTC PRIVACY REPORT].

49. The Future of Privacy Forum has stated that "the types of data that are available and being used for ad targeting today are quite visible and widely available." Reply Comments from the Future of Privacy Forum to Fed. Comm. Comm'n on WC Docket. No. 16-106, FCC 5, (Jul. 6, 2016), https://ecfsapi.fcc.gov/file/10706083993286/FCC%20Reply%20Filing%20-%207.6.16.pdf. Broadband providers appear poised to exploit web-browsing and application-usage information. *See* Comments of AT&T Servs. Inc., In re Protecting the Privacy of Customers of Broadband and other Telecommunications Services, WC Docket. No. 16-106, at 60 (May 27, 2016), https://ecfsapi.fcc.gov/file/60002080023.pdf [hereinafter AT&T Comment Letter]; Rich McCormick, *Verizon Will Share your Browsing Habits with AOL's Massive Ad Network*, THE VERGE (Oct. 6, 2015), https://www.theverge.com/2015/10/6/9468025/verizon-will-share-your-browsing-habits-with-aols-massive-ad-network; Brian Fung, *Internet Providers Want to Know More about You than Google Does, Privacy Groups Say*, WASH. POST. (Jan. 20, 2016) (describing a "land-grab for ad targeting technology"), https://www.washingtonpost.com/news/the-switch/wp/2016/01/20/your-internet-provider-is-turning-into-a-data-hungry-tech-company-

Broadband providers have been experimenting with collecting user data for years. It is only recently that the practice has attracted serious regulatory attention, however. The next section delves deeper into the FCC's plans to regulate broadband privacy under Title II of the Telecommunications Act, and the FTC's likely approach under Section 5 of the FTC Act.

II. COMPARING THE FTC AND FCC APPROACHES

While defenders and opponents of the FCC's Broadband Privacy Order alike seem to agree that the FCC's rules marked a significant departure from the FTC privacy framework,[50] the analysis offered here suggests that the FTC's substantive approach is in fact likely to be quite similar to the FCC's. The only significant difference is the type of consent broadband providers are required to obtain from users before collecting web-browsing and app-usage data. While the FCC's rule may have been somewhat more privacy-protective, the FTC's substantive standards are preferable in terms of overall consumer welfare because they are more likely to encourage competition in nearby data-driven markets. In addition, the flexibility afforded by Section 5 of the FTC Act is preferable to the FCC's rulemaking approach when it comes to broadband privacy, because it will enable the FTC to adjust its privacy standards amid rapid technological change, as the costs and benefits of data collection become clearer.

A. FCC Broadband Privacy Order

The FCC's short-lived Broadband Privacy Order remains the most detailed regulatory assessment of the issues surrounding broadband privacy to date. This section describes the statutory authority on which the FCC's order was based, and details the substance of the FCC's order.

1. Statutory Authority

While the Telecommunications Act of 1996 contains provisions that apply more clearly to data privacy than does the FTC Act, the FCC's statutory authority in the privacy realm is likely more limited than the FTC's. The FCC located the authority for its Broadband Privacy Order in § 222 of the Telecommunications Act.[51] Section 222

consumer-groups-warn/.

50. *See* Broadband Privacy Order, *supra* note 22, at 210 (Pai, Comm'r, dissenting).

51. *See* 47 U.S.C. § 222.

provides that "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers."[52] The provision bars dominant telecom carriers from using other carriers' information for any purpose other than to facilitate interconnection with the network.[53] It also limits carriers' ability to use and disclose information pertaining to customers.[54]

The Broadband Privacy Order expanded the scope of the FCC's previous interpretations of § 222 in two major ways. Most obviously, the order brought broadband services within § 222's reach; previously, the section had only applied to wireline telephone providers.[55]

The order also expanded the types of customer information subject to § 222. Scholars often divide privacy statutes between those that protect communicative attributes, and those that protect communicative content.[56] Until the FCC's recent aggressive privacy enforcement, § 222 was considered an example of the former.[57] The clearest indication that § 222 was designed to protect communicative attributes rather than content is its use of the term "customer proprietary network information" (CPNI), rather than the term "personally identifiable information" (PII).[58] PII is typically invoked in statutes meant to protect content information.[59] The FCC had previously held that CPNI, in contrast, covered information kept on file by telephone companies, such as addresses, bills, and "pen register" information (e.g., the number called, the time of a call, and the duration of a call).[60] This is classic "attribute" information.[61] Indeed, in prior orders, the FCC had explicitly stated that "call content information is not considered CPNI."[62]

---

52. *Id.* § 222(a).
53. *Id.* § 222(b).
54. *Id.* § 222(c).
55. Broadband Privacy Order, *supra* note 22, at ¶ 1.
56. *See* Susan Freiwald, *Uncertain Privacy: Communication Attributes after the Digital Telephony Act*, 69 S. CAL. L. REV. 949, 950–52 (1996).
57. *See* Fred H. Cate, *Privacy and Telecommunications*, 33 WAKE FOREST L. REV. 1, 40 (1998) (describing 47 U.S.C. § 222 as protecting "communication attributes" rather than content).
58. 47 U.S.C. § 222(c).
59. *See* Freiwald, *supra* note 54, at 1014–16. For instance, the Telecommunications Act protects the personally identifiable information of both satellite and cable subscribers. 47 U.S.C. §§ 338(i)(1)(A), 551.
60. In re Implementation of the Telecommunications Act of 1996, 22 F.C.C. Rcd. 6927, 6975–76 (citing app'x B subpart U.2) (2007).
61. *See* Freiwald, *supra* note 54, at 953–55.
62. In re Implementation of the Telecommunications Act of 1996, 11 FCC Rcd. 12513,

The Broadband Privacy Order, however, interpreted § 222 as protecting content, requiring the Commission to significantly expand its interpretation of the statute.[63] The FCC did so in two significant ways. First, it broadened the definition of CPNI, holding that CPNI now included "any part of the substance, purport, or meaning of a communication."[64] Second, the Commission held that the § 222 covered more categories of information than just CPNI—insisting that it protected "customer proprietary information" (PI), as well.[65] The Commission described PI as all the data to which broadband providers have access "in connection with their provision of service"[66]—that is, every piece of customer data, more or less. This included information such as names and addresses that the Commission had previously excluded from its definition of CPNI.[67] This was a dramatic re-interpretation of the statute. It marked a departure from earlier orders interpreting § 222 in the telephony context, and finds no support in the FCC's Computer Inquiries—the rulemaking proceedings in which the terms "customer proprietary information" (PI) and "customer proprietary network information" (CPNI) first appeared, where the Commission used the terms interchangeably.[68]

Assessing the validity of the FCC's interpretation of § 222 is beyond the scope of this Article. It is merely worth noting that the FCC appeared to be covering its bases in finding overlapping grants of authority so that its rules could survive even if a reviewing court rejected part of the Commission's interpretation of § 222.[69] Indeed, the Commission even established a backstop in case a court invalidated its interpretation of § 222 entirely, maintaining that Title II's general anti-discrimination and "reasonable rate" provisions, in addition to other sections of the Telecommunications Act, provided independent authority for its privacy rules.[70]

12532 (1996).

63. Broadband Privacy Order, *supra* note 22, ¶ 6.

64. *Id.* ¶ 102.

65. *Id.* ¶¶ 85–87.

66. *Id.* ¶ 266.

67. *Id.* ¶ 95.

68. *Id.* ¶ 369.

69. Broadband Privacy Order, *supra* note 22, ¶ 102 (noting that content is protected both as CPNI, and as an independent category); *see also id.* ¶ 353 ("Even assuming a contrary reading of Section 222(a), subsection (c) would still invest the Commission with substantial regulatory authority over personal information that BIAS providers and other telecommunications carriers collect from their customers . . . .").

70. *Id.* ¶ 297.

2. Privacy Provisions

The FCC built its order around the notice-and-choice framework so familiar in American privacy law. It laid the groundwork by adopting a notably broad conception of the harm occasioned by broadband providers' collection, storage, and use of customer data, finding that the threats posed by such practices included "not only identity theft or financial loss but also reputational damage, personal embarrassment, or loss of control over the exposure of intimate personal details."[71] The FCC especially relied on the last item—loss of control—to justify far-reaching privacy protections, tailoring its rules to guard against not only improper uses of customer information, but also the mere act of collecting and storing data.[72]

a. Notice

The Commission laid out nuanced requirements for both the type of information privacy notices must contain, and the manner in which notices must be presented to consumers.[73] First, it required broadband providers to inform potential customers of their privacy practices at the point of sale to give them a fair chance to decide whether or not to subscribe to the service.[74] It also mandated that privacy policies "clearly and accurately inform" customers of all material privacy practices,[75] and that the policies be readable—"written and formatted in ways that ensure the material information in them is comprehensible and easily understood."[76]

The rules further required the notices to give customers information about the types of data collected; how data would be used; with whom and for what purposes data would be shared; and how customers could exercise choices regarding data collection.[77] The Commission specifically required providers to reassure customers that refusing to authorize data collection would not result in "degraded service."[78]

The FCC also mandated that providers make their privacy policies easily accessible through their websites and applications,[79] and that

71. *Id.* ¶ 266.
72. *Id.* ¶¶ 267, 379–80.
73. *Id.* ¶¶ 122–65.
74. Broadband Privacy Order, *supra* note 22, ¶ 138.
75. *Id.* ¶ 134.
76. *Id.* ¶ 147.
77. *Id.* ¶ 122.
78. *Id.* ¶ 134.
79. *Id.* ¶ 8.

they present the choice mechanism simultaneous with the notice.[80] Finally, the Commission required carriers to notify customers in advance of material retroactive changes to their privacy policies.[81]

b. Choice

The FCC also spelled out the form of customer approval carriers were required to obtain in order to collect, use, and share certain types of information.[82] These choice provisions were what occasioned much of the controversy around the Broadband Privacy Order.

The Commission placed data-related practices into one of three categories of required approval: (1) "opt-in" choice, that is, practices for which carriers were required to obtain express affirmative consent; (2) "opt-out" choice, that is, practices carriers had to enable customers to avoid if they so chose; and (3) practices that did not require any form of choice.[83] In its Notice of Proposed Rulemaking ("NPRM"), the Commission had initially suggested more lenient treatment of providers' collection of data for certain types of first-party marketing,[84] but it scratched this proposal in the final rule.[85]

At first glance, the difference between opt-in and opt-out choice may not seem particularly significant. In practice, however, the distinction is quite important. As Commissioner Michael O'Rielly noted in dissenting from the FCC order, approval schemes basically function as property rules, given that most customers ignore privacy notices and simply stick with the default setting.[86] Opt-in choice tends to vest this property right in the customer, opt-out choice in the collector.[87]

The Commission decided to require opt-in approval for "sensitive" data, which it defined to include the content of communications, as well as web-browsing and application-usage history and their "functional equivalents"—a catch-all term that would give the Commission flexibility to regulate new types of interfaces emerging with the so-called "Internet of Things" (a term used to describe physical objects that send and receive data over the web).[88]

80. Broadband Privacy Order, *supra* note 22, ¶ 133.
81. *Id.* ¶ 195.
82. *Id.* ¶¶ 166–234.
83. *Id.* ¶ 9.
84. *See* Broadband Privacy NPRM, *supra* note 18, at 2532.
85. Broadband Privacy Order, *supra* note 22, ¶¶ 199–200.
86. *Id.* at 216 (O'Rielly, Comm'r, dissenting).
87. *See id*.
88. *Id.* ¶¶ 181, 185. The Commission also classified certain types of information as

The Commission also required opt-in consent for material retroactive changes to privacy policies.[89] It mandated opt out approval for all other forms of data gathering, save those expressly exempted in § 222.[90]

The FCC also stated that it would allow firms to pay customers to opt in to data collection.[91] However, the Commission cautioned that it was prohibiting "take-it-or-leave-it offering[ings] [of] . . . broadband service contingent on customers surrendering their privacy rights."[92] It did not specify how exactly it would evaluate when payment for data would rise to the level of a violation, saying only that it would step in if customers were "essentially compelled to choose between protecting their personal information and very high prices."[93]

3. Security Provisions

Finally, the Commission imposed requirements relating to data security and data-breach notification.[94] It required carriers to take "reasonable measures" to ensure the security of customers' data,[95] declining to impose more specific requirements because it recognized that "what constitutes 'reasonable' data security is an evolving concept."[96] And it required providers to notify the FCC, Federal Bureau of Investigation (FBI), and Secret Service within seven business days of any data breach, unless the breach posed "no reasonable risk of . . . harm."[97] It modeled this requirement on state data-breach-notification statutes.[98]

B. Likely FTC Regulation of Broadband Privacy

It is difficult to make an apples-to-apples comparison between the FCC's and FTC's regulation of broadband privacy, given the

---

sensitive, such as Social Security numbers and medical data, *id.* ¶ 9, but these categories were arguably redundant given the inclusion of content, browsing history, and app usage history.

89. *Id.* ¶ 195.

90. *Id.* ¶ 9.

91. Broadband Privacy Order, *supra* note 22, ¶ 298–303.

92. *Id.* ¶ 294–97.

93. *Id.* ¶ 303.

94. *See generally id.* ¶ 235–60.

95. *See generally id.* ¶ 238–47. The Commission did not detail practices that would meet this standard. It suggested that it was essentially incorporating the FTC's approach to data security, as it has developed in dozens of Section 5 enforcement actions. *See id.* ¶ 240.

96. *Id.* ¶ 236.

97. Broadband Privacy Order, *supra* note 22, ¶ 264, 278.

98. *Id.* ¶ 264

commissions' divergent approaches. While the FCC enshrined its planned regulation in a detailed rule, the FTC, for all intents and purposes, lacks rulemaking authority.[99] Instead, it enforces privacy requirements pursuant to the open-ended mandate of Section 5 of the FTC Act, which condemns "unfair or deceptive acts or practices in or affecting commerce."[100]

Accordingly, in order to discern the likely shape of the FTC's enforcement of broadband privacy, we must look to the Commission's past privacy-enforcement actions and policy statements. The FTC has detailed its views on privacy best practices in guidelines, press releases, workshops, and white papers—documents that Professors Woodrow Hartzog and Dan Solove describe as "soft law," similar to dicta in judicial opinions.[101] In addition, the FTC has brought so many privacy actions that its interpretation of Section 5's standards has hardened into rule-like form, as Hartzog and Solove have argued.[102] While its privacy settlements lack precedential force, the FTC "has demonstrated a commitment to remaining consistent in practice."[103]

Analyzing the FTC's enforcement actions and policy statements enables us to understand how the Commission might enforce Section 5 against broadband providers now that it has the authority to do so, and points up areas where the Commission's approach will need further development. It also reveals that the difference between the two commissions' approaches may be slighter than either privacy advocates or objectors to the FCC's rules have supposed.

1. FTC Statutory Authority over Broadband Privacy Practices

The FTC does not have specific statutory authority to regulate data privacy. Instead, it brings privacy actions pursuant to its general

99. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 620 (2014) [hereinafter Solove & Hartzog, *New Common Law*] ("[F]or Section 5 enforcement – one of the largest areas of its jurisprudence – the FTC has only Magnuson-Moss rulemaking authority, which is so procedurally burdensome that it is largely ineffective.").

100. 15 U.S.C. § 45.

101. Solove & Hartzog, *New Common Law*, *supra* note 97, at 625–26; *see also* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 616–17 (D. N.J. 2014).

102. Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2232 (2015); Solove & Hartzog, *New Common Law*, *supra* note 99, at 586, 607 ("Technically, consent orders legally function as contracts rather than as binding precedent. Yet, in practice, the orders function much more broadly than a contract between a company and the FTC. In the world of privacy law practice, everything the FTC says and does is delicately parsed, like the statements of the Chairman of the Federal Reserve.").

103. Solove & Hartzog, *New Common Law*, *supra* note 97, at 620.

consumer-protection powers under Section 5 of the FTC Act, which declares unlawful "unfair or deceptive acts or practices in or affecting commerce."[104] A practice is deceptive if it involves (1) an act (representation, omission, or practice) that would (2) deceive a reasonable consumer in a manner that is (3) material.[105] Meanwhile, a finding of unfairness requires (1) a substantial injury (2) without offsetting benefits that (3) consumers cannot reasonably avoid themselves.[106]

A recent ruling by a three-judge panel of the U.S. Court of Appeals for the Ninth Circuit has thrown the FTC's ability to enforce Section 5 against telecommunications firms into some doubt.[107] While Section 5 applies generally to "persons, partnerships, or corporations," it exempts several classes of firms from its scope.[108] Among these are "common carriers subject to the Acts to regulate commerce."[109] The FTC has long maintained that this provision does not deprive it of Section 5 authority over the non-common-carrier services of firms that otherwise operate as common carriers.[110] For instance, under the FTC's interpretation, the common-carrier exemption would prevent the Commission from enforcing Section 5 against AT&T's wireline telephone operations—which the FCC regulates as a common-carrier service under Title II of the Communications Act—but would allow it to apply Section 5 to AT&T's wireless services, which Title II does not cover.[111]

The Ninth Circuit panel rejected this interpretation, however.[112] In the first federal appellate opinion to consider the issue, the panel held that a firm which engaged in *any* regulated common-carrier

104. 15 U.S.C. § 45(a)(1).

105. Letter from James C. Miller III, Chairman, FTC, to Hon. John D. Dingell, Chairman, House Comm. on Energy & Commerce (Oct. 14, 1983), *reprinted in* In re Cliffdale Assocs., Inc., 103 F.T.C. 110, 1984 WL 565319, at *45–50 (1984) (decision & order).

106. Letter from FTC Comm'rs to Wendell H. Ford & John C. Danforth, Senators (Dec. 17, 1980), *reprinted in* In re Int'l Harvester Co., 104 F.T.C. 949, 1984 WL 565290, at *97 (1984); *see also* 15 U.S.C. § 45(n).

107. FTC v. AT&T Mobility LLC, 835 F.3d 993 (9th Cir. 2016), *reh'g en banc granted*, No. 15-16585, 2017 WL 1856836 (9th Cir. May 9, 2017).

108. *See* 15 U.S.C. § 45(a)(2).

109. *Id.*

110. *See* Comment of the Staff of the Bureau of Consumer Protection of the Fed. Trade Comm'n to the Fed. Comm. Comm'n, WC Dkt. No. 16-106, FCC 16-39 at 3 fn. 6 (May 27, 2016), https://ecfsapi.fcc.gov/file/60002078443.pdf [hereinafter FTC Comment Letter].

111. *AT&T Mobility*, 835 F.3d at 995–98.

112. *Id.* at 1003.

activity was *entirely* exempt from regulation under Section 5.[113] Thus, under the Ninth Circuit decision, the FTC would be barred from bringing a Section 5 complaint against AT&T's (non-common-carrier) broadband services because the FCC regulates AT&T's wireline telephony services under Title II.[114] However, the circuit has since reheard the case en banc, vacating its opinion.[115] It appears likely that the court will agree with the FTC's longstanding interpretation on rehearing.

2. The FTC's Substantive Approach to Broadband Privacy

Data-privacy advocates have suggested that there are three major points on which the FTC's regulation of broadband privacy will differ from the FCC's since-aborted approach. First, they note that the FTC generally has not required consumer approval for first-party marketing,[116] whereas the Broadband Privacy Order did not allow for such an exception.[117] Second, they point out that the FTC generally only requires customers' opt-in approval for collecting information classified as "sensitive,"[118] whereas the FCC would have required opt-in approval for collection of *all* content data.[119] Finally, they observe that the FTC typically does not mandate *any* form of approval for tracking users' web-browsing and app-usage habits, whereas the FCC would have required opt-in approval for this practice.[120]

However, the FTC's statements about the privacy practices of broadband providers strongly suggest it will enforce broadband privacy in a manner that is largely consonant with the FCC's rules. Though many of the commenters in the FCC broadband privacy proceeding appeared to assume that the FTC would take the same approach in enforcing Section 5 against broadband providers as it does against other firms,[121] in fact the Commission has given strong indications that

113. *Id.* at 998.

114. *See id.* at 995–98.

115. *AT&T Mobility*, 2017 WL 1856836.

116. FTC PRIVACY REPORT, *supra* note 46, at 40–42.

117. Broadband Privacy Order, *supra* note 22, ¶ 9.

118. *See, e.g.*, Complaint for Permanent Injunction and Other Equitable Relief, Fed. Trade Comm'n v. Frostwire, LLC, No. 1:11-cv-23643, at ¶¶ 22–32, ¶¶ 41–43 (S.D. Fla. Oct. 7, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111011frostwirecmpt.pdf [hereinafter Frostwire Complaint]; FTC PRIVACY REPORT, *supra* note 48, at 58–60.

119. Broadband Privacy Order, *supra* note 22, ¶ 5.

120. Frostwire Complaint, *supra* note 117, at ¶¶ 22–32, 41–43; FTC PRIVACY REPORT, *supra* note 46, at 58–60.

121. *See, e.g.*, Doug Brake et al., *Broadband Privacy: The Folly of Sector-Specific*

it sees broadband privacy as *sui generis*, and deserving of more stringent safeguards.

The Commission has detailed its views primarily in two documents: a 2012 report, *Protecting Consumer Privacy in an Era of Rapid Change* ("FTC Privacy Report"),[122] and comments to the FCC regarding broadband privacy.[123] The views expressed in these documents are not necessarily representative of how the FTC will actually enforce Section 5 against broadband providers,[124] and the approach of the Republican-majority Trump FTC may differ from those of the Democrat-majority Obama FTC. Nevertheless, they are helpful guides to understanding how the Commission might enforce Section 5 against broadband providers.

The FTC has articulated two significant respects in which the privacy practices of broadband providers might warrant different treatment from those of firms in other industries. First, though the Commission has never brought a Section 5 action against a firm for collecting non-sensitive information, it has stated that broadband providers should offer opt-in choice for collection of sensitive and non-sensitive information alike through deep packet inspection.[125] The Commission stated in its Privacy Report that it "has strong concerns about the use of DPI for purposes inconsistent with an ISP's interaction with a consumer, without express affirmative consent or more robust protection."[126] It reinforced this view in its comments in the FCC broadband privacy rulemaking, encouraging the FCC to require opt-in consent for any collection of content data through deep packet inspection—not just the types of information the Commission had previously deemed sensitive.[127]

Second, the FTC has reasoned that broadband providers should allow customers some form of choice before tracking their movements across the internet.[128] The basis for this view can be found in the FTC Privacy Report, in which the Commission reasoned that firms should

---

Regulation, INFO. TECH. & INNOVATION FOUND. 5 (Mar. 2016), http://www2.itif.org/2016-broadband-privacy-folly.pdf?_ga=2.236078978.222908656.1517294711-1584549091.1517294711 (comparing FCC regulation to the (apparently monolithic) "FTC approach").

122. FTC PRIVACY REPORT, *supra* note 46, at iii.

123. *See* FTC Comment Letter, *supra* note 110.

124. *See* FTC PRIVACY REPORT, *supra* note 46, at iii.

125. FTC Comment Letter, *supra* note 110, at 21.

126. FTC PRIVACY REPORT, *supra* note 46, at 56.

127. *Compare* FTC Comment Letter, *supra* note 122, at 20, *with* FTC PRIVACY REPORT, *supra* note 46, at 58–60.

128. FTC PRIVACY REPORT, *supra* note 46, at 27.

provide notice and choice where data collection is inconsistent with the context of their relationship with users.[129] Applying this principle to the tracking of users across third-party websites, the FTC reasoned that such tracking is "unlikely to be consistent" with the context of the web-browsing experience.[130]

These statements lend a different perspective on the FTC's likely enforcement of Section 5 in the context of broadband providers' privacy practices. If the FTC enforces Section 5 against broadband providers according to its policy statements, there would only be two differences between the commissions' enforcement of broadband privacy. First, the FTC would not require any form of customer approval for first-party marketing that makes use of data not collected through deep packet inspection or third-party tracking,[131] whereas the FCC would have required opt-out approval for the use of such data.[132] Second, the FTC would likely require that firms provide only opt-out choice for the collection of web-browsing and app-usage data by broadband providers,[133] whereas the FCC would have required opt-in choice.[134]

C. Comparing FCC and FTC Regulation of Broadband Privacy

The FTC's approach to regulating broadband privacy will likely be quite similar to the approach embodied in the FCC's since-repealed Broadband Privacy Order. While the FCC's rules would have been more privacy-protective than the FTC's enforcement of Section 5 is likely to be, the FTC's substantive approach is preferable from the perspective of consumer welfare, because it will enable broadband providers to compete in nearby data-intensive markets. In addition, the FTC's standards-based procedural approach is preferable to the FCC's regulation through prescriptive rulemaking, because it allows for needed flexibility in quickly evolving markets.

1. Comparing the Commissions' Substantive Rules

The difference between the commissions' rules regarding first-party marketing likely appears more significant than it really is. Because the FTC has endorsed approval rules for the collection of

129. *Id.*
130. *Id.* at 41.
131. *Id.* at 40–44.
132. Broadband Privacy Order, *supra* note 22, ¶ 199.
133. FTC PRIVACY REPORT, *supra* note 46, at 40–42.
134. Broadband Privacy Order, *supra* note 22, ¶ 167.

content data and information regarding third-party web browsing and app usage,[135] the difference in the commissions' approaches boils down to the treatment of information about a particular user's current subscription(s) to service. The FCC would have required opt-out approval for use of this data,[136] whereas the FTC would not require customer approval.[137] Because consumers rarely bother to exercise privacy choices at all,[138] the difference between an opt-out rule and a rule requiring no approval at all is actually not as significant as the difference between opt-in and opt-out rules would have been. It may further be supposed that the customers who choose to opt out of marketing are less likely to read marketing appeals in the first place. Accordingly, the difference between the commissions' rules on this point is negligible.

The only remaining significant difference between the commissions' approaches is the treatment of web-browsing and app-usage data. Thus, the determination of which commission's privacy regulation is more consumer-friendly will hinge on a comparison of their approaches on this score. The FCC's opt-in rule is plainly more privacy-protective than the FTC's likely opt-out rule. However, a comparison of the effects of the rules on consumer welfare must take into account the effect on consumers as a whole—not just the effect on consumer privacy. More stringent privacy rules are not necessarily better for consumers. Where data is an important input, rules that restrict data collection, storage, and use run the risk of degrading the quality of services, making data-intensive markets more concentrated and harming consumer welfare to an extent that may not be offset by the regulations' privacy benefits.[139] This is particularly true where regulation has the effect of increasing barriers to entry.[140]

---

135. FTC PRIVACY REPORT, *supra* note 46, at 40–41.

136. Broadband Privacy Order, *supra* note 22, ¶¶ 198–99.

137. FTC PRIVACY REPORT, *supra* note 46, at 40–44.

138. *See* J. Howard Beales, III & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHI. L. REV. 109, 114–115 (2008). One oft-cited example of the "stickiness" of default settings comes in the context of organ donations. Though Americans widely approve of organ donation, only about a quarter actually opt-in to the organ donation system. By contrast, organ donation is nearly universal in countries that set the default at "donate" and require would-be non-participants to opt out. *See* Steve Lohr, *The Default Choice, So Hard to Resist*, N.Y. TIMES (Oct. 15, 2011), http://www.nytimes.com/2011/10/16/technology/default-choices-are-hard-to-resist-online-or-not.html.

139. *See* DAVID S. EVANS, ED., PLATFORM ECONOMICS: ESSAYS ON MULTI-SIDED BUSINESSES 222–24 (2011).

140. J. Thomas Rosch, *Do Not Track: Privacy in an Internet Age*, FED. TRADE COMM'N 20–21 (Oct. 14, 2011), https://www.ftc.gov/sites/default/files/documents/public_statements/

Accordingly, one must evaluate the effects of the commissions' rules on markets. The FCC did not engage in an economic analysis in its Broadband Privacy Order. While it compared broadband providers' access to user data to that of edge providers,[141] the degree of access a firm has to a particular *input* does not necessarily correlate to its ability to compete in a given *market*.

The most obvious market in which collecting user data would better enable broadband providers to compete is the market for advertising intermediation. Ad intermediaries are firms that connect content publishers with advertisers.[142] Publishers sell space on their websites indirectly to advertisers through intermediaries, who then decide which ad to serve a given user based on information about that user's characteristics.[143] This may be relatively crude data, such as demographic information, or more detailed data, such as information about a given user's predilections and browsing habits.[144]

Increased competition is generally thought to redound to the benefit of consumers, and there is no reason to think ad intermediation is an exception. A lack of competition would likely lead to higher prices for ad intermediation services, in turn lessening the take of advertising revenue that content publishers see. This would likely cause publishers to produce less content, which could be thought of as a form of output reduction—the central harm antitrust law seeks to address.[145]

On the one hand, allowing broadband providers to collect web-browsing and app-usage data subject only to opt-out choice may make the ad intermediation market more competitive by enabling new entry.[146] On the other hand, broadband providers may be able to collect so much data, or may be able to collect data so cheaply, that they could out-compete all other firms and achieve dominance in the ad intermediation market. This would force other firms that wish to compete in ad intermediation to first enter the broadband market in

---

do-not-track-privacy-internet-age/111014-dnt-loyola.pdf.

141. Broadband Privacy Order, *supra* note 22, ¶¶ 28, 37, 35.

142. EVANS, *supra* note 137, at 215.

143. *Id.* at 217, 241.

144. *Id.* at 241.

145. *See id.* at 246.

146. *See* Letter from J. Howard Beales III, Professor of Strategic Mgmt. & Pub. Pol'y at the Geo. Wash. Sch. of Bus., to Tom Wheeler, Chairman, Fed. Comm. Comm'n, RE: Docket No. 16-106, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services 8–10 (May 27, 2016), https://scholarspace.library.gwu.edu/downloads/6969z0820 (describing higher regulatory burdens on broadband providers as entry barrier).

order to gain comparable access to data.[147] New America's Open Technology Institute peddled a version of this argument in its comments to the FCC, maintaining that allowing broadband providers to collect customer data would enable them to "thrust themselves into any other market where competitors normally must pay for intelligence about and access to target audiences."[148]

It must be noted at the outset that this is not an issue for antitrust law: no one is claiming that permissive collection rules would grant broadband providers a monopoly on ad-intermediation data, and even if this were the case, antitrust does not recognize stand-alone "monopoly leveraging" claims.[149] Regulators, however, have more flexibility than antitrust authorities. They may proscribe a practice where it threatens harm to the competitive environment, regardless of whether it rises to the level of an antitrust violation. Engaging in such "competitive handicapping" raises concerns of its own,[150] but first let's explore the case for handicapping here.

In order to evaluate the effect broadband providers' entry might have on the ad intermediation market, one must first understand the dynamics of that market. Ad intermediation is a two-sided market: intermediaries provide value by reducing search costs among advertisers and publishers, connecting content publishers who have ad space to sell with advertisers seeking to reach users.[151] Ad intermediation appears to accord with the general rule that two-sided markets skew toward a dynamic of "winner take all" or "a few winners take all," given the presence of network effects and large fixed costs that produce economies of scale.[152] The market has become more concentrated since the FTC determined in 2007 that it was "highly

147. *See* Daniel L. Rubinfeld & Michal S. Gal, *Access Barriers to Big Data*, 59 ARIZ. L. REV. 339, 375 (2017).

148. *See* Reply Comments of New Am.'s Open Tech. Inst., In re Protecting the Privacy of Customers of Broadband and other Telecommunications Services, WC Dkt. No. 16-106, at 7 (Jul. 6, 2016), https://ecfsapi.fcc.gov/file/10707717014775/2016-07-06%20-%20OTI%20Broadband%20Privacy%20Reply%20Comments%20FINAL.pdf. Note that the premise of this comment is questionable. For instance, just as broadband providers gain income from charging for broadband services, Google and Facebook gain revenue from charging advertisers to display ads on their own sites, in addition to monetizing user data by selling ads on third-party sites.

149. *See* Spectrum Sports, Inc. v. McQuillan, 506 U.S. 447, 458–59 (1993); *see also* Joseph Kattan, *The Decline of the Monopoly Leveraging Doctrine*, ANTITRUST 41, 41–42 (1994).

150. *See* STEPHEN BREYER, REGULATION AND ITS REFORM 314 (1984).

151. EVANS, *supra* note 137, at 215–18.

152. *Id.* at 14–15, 213, 276.

fragmented and correspondingly competitive."[153] One indication of this is that Google and Facebook together account for about half of display advertising revenue.[154]

Given the strong positions of Google and Facebook in the market for ad intermediation, it seems unlikely that broadband providers' collection of web-browsing and app-usage data would enable them to achieve dominance. This is particularly true given that Google and Facebook's access to web-browsing and app-usage data rivals that of broadband providers, if not outpacing it.[155] Google and Facebook track users' browsing habits across much of the internet by loading cookies onto websites for which they provide ad-intermediation or data-analytics services.[156] Their strong market positions are thus self-reinforcing: the more ad intermediation services they provide, the more data they are able to collect. Google is present in some form on over eighty percent of all third-party sites, with Facebook hovering around thirty-five percent.[157] Four other firms are present on between ten and twenty percent of sites.[158]

Moreover, while a firm's supra-competitive profits in one market may in theory enable it to price below marginal cost in another market,[159] Google and Facebook would appear to have both the resources and incentives to withstand a price war in the ad intermediation market indefinitely.[160] And it does not appear that broadband providers' costs of obtaining and analyzing data are less than those of Google and Facebook, so long-term predatory pricing would likely be unsustainable and therefore irrational.[161]

---

153. STATEMENT OF FED. TRADE COMM'N CONCERNING GOOGLE/DOUBLECLICK 8, n.8 (2007), https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf.

154. *See* David Kirkpatrick, *EMarketer: Google, Facebook Together Command 51.6% of Digital Display Advertising*, MARKETING DIVE (Mar. 15, 2017), https://www.marketingdive.com/news/emarketer-google-facebook-together-command-516-of-digital-display-adver/438129/.

155. *See* Peter Swire et al., *Online Privacy and ISPs* (May 2016 working paper), http://www.iisp.gatech.edu/working-paper-online-privacy-and-isps; *but see* Aaron Rieke et al., *What ISPs Can See: Clarifying the Technical Landscape of the Broadband Privacy Debate*, UPTURN (Mar. 2016), https://ecfsapi.fcc.gov/file/60002077347.pdf.

156. *See* Steven Englehardt & Arvind Narayanan, *Online Tracking: A 1-Million-Site Measurement and Analysis* 11 (last visited Feb. 17, 2018) https://webtransparency.cs.princeton.edu/webcensus/.

157. *Id.* at 8–9.

158. *Id.*

159. *See* Brooke Grp. Ltd. v. Brown & Williamson Tobacco Corp., 509 U.S. 209, 217 (1993).

160. *See id.* at 225.

161. *See id.*

The situation of large upstarts challenging entrenched firms in an adjacent market is strikingly similar to one the FCC faced over thirty years ago in its Computer Inquiries.[162] For years, the Commission barred firms that maintained a dominant position in the wireline telephony market from entering the separate market for "enhanced" wireline telephony services unless they did so through a separate subsidiary.[163] Eventually, however, the FCC considered doing away with that requirement and allowing telephony providers, such as AT&T and the Bell Operating Companies ("BOCs"), to enter the market for enhanced services subject to less onerous safeguards.[164] Enhanced-service vendors argued that the economies of scale enjoyed by AT&T and the BOCs would allow those firms to eliminate competition in the enhanced-services market, just as privacy advocates today warn of the threat posed by broadband providers in the ad intermediation market.[165] The Commission rejected this contention, however, instead accepting AT&T's argument that its entry would make the market for enhanced services more competitive because it was a late, non-dominant entrant, and because the enhanced-services market already featured large providers such as IBM and GTE that would be able to compete on an equal footing with AT&T and the BOCs.[166]

The situation in ad intermediation is more or less a repeat of the debate over enhanced services, with dominant broadband providers playing the role of AT&T and the BOCs, and Google and Facebook playing the role of IBM and GTE. There is again reason to think that the large upstarts' entry will make the market more competitive. Because their access to user data is independent of their presence serving ads on other firms' websites, broadband providers are uniquely positioned to compete with Google and Facebook in ad intermediation, at least in theory. Indeed, the mere threat of broadband providers' entry into the ad intermediation market may be enough to constrain the ability of Google and Facebook to raise prices for content publishing and advertising services.[167]

And even in the unlikely event that broadband providers do drive

---

162. *See* Amendment of Section 64.702 of the Commission's Rules and Regulations (Third Computer Inquiry), 104 F.C.C.2d 958, 962–69 (1986) [hereinafter Computer III].

163. Amendment of Section 64.702 of the Commission's Rules and Regulations (Second Computer Inquiry), 77 F.C.C.2d 384 (1980).

164. Computer III, *supra* note 163, at 964.

165. *Id.* at 997.

166. *Id.* at 991, 1010.

167. *See* Bernard Caillaud & Bruno Jullien, *Chicken & Egg: Competition among Intermediation Service Providers*, 34 RAND J. ECON. 309, 321–22 (2003).

Google, Facebook, and other competitors from the ad intermediation market, they would presumably still be faced with competition in that market from other broadband carriers. It is unlikely that any one provider enjoys sufficiently broad access to user data that it could dominate the ad intermediation market, were Google and Facebook to somehow abdicate their positions. Thus, allowing broadband providers to track users across apps and websites is likely to drive down prices in the ad intermediation market in both the short and long term, which would presumably redound to consumers' benefit in the form of more and/or better content from publishers (which will have more funds to invest in content development), as well as more relevant ads (because advertisers, enjoying lower costs per ad, will place more ads). This could be viewed as an increase in output, which is the central goal of American competition law.

Meanwhile, the privacy harms occasioned by allowing broadband providers to collect web-browsing and app-usage data appear relatively insignificant, at least when compared with the potential harms occasioned by deep-packet inspection. Whereas broadband providers would theoretically have unparalleled access to content data if they engaged in deep packet inspection to the full extent of their technical abilities, their access to web-browsing data would be matched by at least Google, given its presence on the great majority of websites and its ability to collect data through both the Chrome browser and the Android ecosystem.[168] Indeed, Commissioner O'Rielly has argued that broadband providers' collection of web-browsing and app-usage data would cause *no* harm to consumers, given that such data is already widely collected and traded.[169] O'Rielly is probably overstating the case. Nevertheless, the point that regulators must focus on the *marginal* harm of data collection is well-taken.

Accordingly, once one accounts for competitive effects on the ad intermediation market, it is not so clear that the substantive rules embodied in the FCC's Broadband Privacy Order would have been better for consumers on the whole. Indeed, from a general consumer welfare perspective, FTC jurisdiction over broadband privacy appears preferable to FCC jurisdiction.

---

168. *See* Swire, *supra* note 156, at 23, 75–77. 90–93; Petition for Reconsideration, In re Protecting the Privacy of Customers of Broadband and other Telecommunications Services, WC Dkt. No. 16-106, at 2–7 (Dec. 21, 2016), https://ecfsapi.fcc.gov/file/1221003408004/Oracle_Broadband_Privacy_Petition_for_Reconsideration.pdf [hereinafter Oracle Pet'n for Reconsideration].

169. *See* Broadband Privacy Order, *supra* note 22, ¶¶ 216–17 (O'Rielly, Comm'r, dissenting) ("[A]ll that the FCC has really done is raise the transaction costs").

2. Comparing the Commissions' Procedural Approaches

Moreover, the procedural flexibility afforded by Section 5 of the FTC Act is better-suited to broadband-privacy enforcement than is the FCC's prescriptive rulemaking approach. The costs and benefits of privacy regulation are difficult to measure in general,[170] but they are particularly so in cases like this, where the extent to which the regulated firms plan to collect data and the uses to which they plan to put that data are unclear.[171] As David Evans has observed, broadband "and the Web are very new technologies by historical standards," and thus call for modesty on the part of regulators.[172] Regulatory modesty is particularly warranted in light of the staggering gains in dynamic efficiency often brought by advances in technology[173]—gains that can be blunted by overly aggressive regulation. The FTC's standards-based enforcement is more sensitive to potential dynamic efficiencies because it enables the Commission to easily adapt its approach amidst rapid change.

The comments in the FCC's broadband privacy proceeding[174] underscore just how speculative the costs and benefits of data collection by broadband providers really are at the moment. The discussion was characterized by vagueness on both sides. The FCC was widely panned for failing to conduct a cost-benefit analysis at all,[175] and for failing to provide any evidence of perhaps its primary justification for the Broadband Privacy Order: that the adoption of privacy rules would speed broadband adoption.[176] However, opponents

170. *See* Julie E. Cohen, *The Regulatory State in the Information Age*, 17 THEORETICAL INQUIRIES L. 369, 392 (2016) ("Skeptics charge that cost-benefit analysis persistently undervalues threatened harms that are diffuse, cumulative, and difficult to describe in monetized, present-value terms, and that it therefore predictably works to the advantage of vested economic interests.").

171. *See* FTC PRIVACY REPORT, *supra* note 46, at C-7–8 (Rosch, Comm'r, dissenting) (contending that the FTC should wait to see whether broadband providers will actually engage in deep packet inspection before requiring such providers to obtain opt-in consent from their customers).

172. EVANS, *supra* note 137, at 265.

173. *See* Thomas O. Barnett, *Maximizing Welfare Through Technological Innovation*, 15 GEO. MASON L. REV. 1191, 1194–96 (2008) ("[D]ynamic efficiency accounts for the lion's share of efficiency/welfare gains.")

174. *See* Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Dkt. 16-106.

175. *See, e.g.*, Broadband Privacy Order, *supra* note 22, ¶ 219 (O'Reilly, Comm'r, dissenting).

176. One survey found that less than 0.5% of broadband *non-adopters* "report privacy concerns as the primary reason for not subscribing." Thomas Lenard and Scott Wallsten, *An Economic Analysis of the FCC's Privacy Notice of Proposed Rulemaking*, TECH. POL'Y

of the FCC's rule didn't do much better in assessing costs and benefits—an indication, perhaps, that those costs and benefits have not yet become sufficiently clear to analyze cogently. For instance, rather than offer specific examples of areas in which restrictive rules might hamper innovation, AT&T pointed to past Internet innovations that the FCC's rules would have blocked, had those rules been in place at the time.[177] AT&T did mention that data collection and end use might enable broadband providers to enter the markets for apps or "over-the-top 'edge services'" such as video streaming or Voice Over Internet Protocol (VOIP).[178] But opponents of the FCC's rules failed to explain how access to data would enable broadband providers to compete in these markets in a manner that would actually enhance economic welfare, rather than simply shift profits from one group of firms to another.

The technology of data collection, storage, and analysis is itself still evolving, as well. For instance, whether deep packet inspection will prove economically feasible will largely hinge on future advances in data-storage technology.[179] Likewise, whether privacy-protective technologies such as encryption and VPNs might provide an effective substitute for regulation remains to be seen.[180] Waiting until costs and benefits become somewhat more definite before deciding which practices to condemn increases the likelihood that regulators will arrive at the right result. This is the lesson of the Pennsylvania stop-look-and-listen rule in negligence law: novel circumstances may cast a practice that has heretofore appeared unquestionably unreasonable in a new light.[181]

Accordingly, the FTC's measured, case-by-case approach better lends itself to regulatory realism in this area. It allows the Commission to focus on actual harms rather than speculative ones, and avoids forcing it to predict changes in technology and business practices. Meanwhile, the slow pace of informal rulemaking under the Administrative Procedure Act exacerbates the inflexibility of prescriptive rules like the FCC's. As Jeffrey Eisenach has observed,

---

INST. 20 (May 2016), https://ecfsapi.fcc.gov/file/60002055729.pdf (drawn from data in Bureau of Census for U.S. Dep't of Commerce, *Current Population Survey*, July 2015 (2016)).

177. AT&T Comment Letter, *supra* note 47, at 51–53.

178. *Id.* at 55, 59.

179. *See* Feamster Comment Letter, *supra* note 43, at 6.

180. *See id.*

181. *See* James Fleming Jr. & David K. Sigerson, *Particularizing Standards of Conduct in Negligence Trials*, 5 VAND. L. REV. 697, 704–05 (1952).

"once a rule is in place, it can take at least as long to modify or repeal it as it took to pass it in the first place, creating the possibility that rules designed to address an ephemeral problem persist long after the problem is resolved—and so are transformed from cure to disease."[182]

The FTC's willingness to rely on a broader range of regulatory measures than the FCC represents another source of flexibility.[183] For instance, the FTC has embraced self-regulatory models, urging firms to collaborate on a standard "do not track mechanism" that would give consumers greater control over cross-website tracking.[184] In addition, the FTC's historically nuanced assessment of the manner in which firms provide choice helpfully plays down the distinction between opt-in and opt-out choice.[185] For instance, in its enforcement proceedings, the Commission often emphasizes the prominence of a firm's notice-and-choice mechanism over the issue of what type of choice the firm provides (opt-out or opt-in).[186] This flexible and nuanced approach to regulation enables the FTC to achieve privacy goals in a minimally intrusive manner. While the FCC may well have developed a similar approach in time, the FTC's long experience bodes well for its regulation of broadband privacy. And while the FTC may lack industry-specific expertise, its privacy expertise is likely more relevant in the context of broadband privacy. Moreover, though the FCC's historical focus on competition as well as consumer-protection concerns would appear to give it an advantage in regulating in an area that incorporates both, this apparent edge was muted by the Commission's complete failure to address the effect its rules would have on adjacent markets in the Broadband Privacy Order.

All told, then, there is little reason to think that consumers would have been better off under the FCC's broadband privacy regime than they will be under the FTC's Section 5 enforcement. As it considers bringing privacy-enforcement actions against broadband providers, the

182. Jeffrey Eisenach, *Broadband Competition in the Internet Ecosystem*, AM. ENTERPRISE INST. 28 (Oct. 2012), https://www.aei.org/publication/broadband-competition-in-the-internet-ecosystem/.

183. *See* Philip J. Weiser, *The Future of Internet Regulation*, 43 U.C. DAVIS L. REV. 529, 557-58 (2009) ("The FTC is much more comfortable with and inclined to consider the potential use of self-regulation than the FCC").

184. FTC PRIVACY REPORT, *supra* note 46, at 52–55.

185. *Id.* at 50–52.

186. *See, e.g.*, Complaint for Permanent Injunction and Other Equitable and Monetary Relief, Fed. Trade Comm'n v. Vizio, No. 2:17-cv-00758, at ¶ 23 (D.N.J. Feb. 6, 2017), https://www.ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.pd; Complaint, In re Sears Holding Mgmt. Corp., No. C-4264, at ¶ 13 (Aug. 31, 2009), https://www.ftc.gov/sites/default/files/documents/cases/2009/09/090604searscmpt.pdf.

FTC should resist calls from privacy advocates to raise its threshold for consumer choice regarding web-browsing and app-usage data.

III. THREE QUESTIONS FOR THE FTC REGARDING BROADBAND PRIVACY

Several significant questions linger regarding the FTC's Section 5 enforcement in the context of broadband privacy. Some were thrashed out before the FCC, but warrant reexamination, while others concern circumstances unique to the FTC's approach.

A. Are Broadband Providers Special?

The most commonly heard criticism of the FCC's Broadband Privacy Order was that it failed to harmonize with the FTC's approach.[187] This assertion is a bit puzzling, however, given that the FTC has indicated that certain types of large platform providers, including broadband providers, should be subjected to more stringent data-privacy obligations than other firms.[188] To be sure, split regulatory authority over broadband would "not [have been] optimal," as the FTC acknowledged in its comments on the Broadband Privacy Order.[189] Hard regulatory boundaries can be especially problematic when it comes to industries like broadband, where technology threatens to swamp "the jurisdictional boundaries of the existing administrative framework."[190] Nevertheless, no one disagrees with the premise that some factors, such as access to data, do indeed justify different data-privacy rules for different firms. Taking as a given the principle that similarly situated firms should be regulated similarly, a key question for the FTC regarding broadband privacy is what *differences* among firms might justify differential privacy regulation.

The FTC has openly grappled with the issue of whether broadband providers and other large platform providers should be subjected to different privacy rules since as early as 2012. The Commission evaluated the issue in its Privacy Report,[191] and held a workshop on the

187. *See* Broadband Privacy Order, *supra* note 22, ¶ 209 (Pai, Comm'r, dissenting) ("[S]ince the beginning of this proceeding, I have pushed for the Federal Communications Commission to parallel the FTC's framework as closely as possible").

188. FTC PRIVACY REPORT, *supra* note 46, at 55–57.

189. FTC Comment Letter, *supra* note 122, at 8.

190. Cohen, *supra* note 171, at 397; *see also* Kevin Werbach, *A Layered Model for Internet Policy*, 1 J. TELECOM. & HIGH TECH. L. 37, 46 (2002) ("[T]he Internet sows confusion when it comes into contact with the dominant horizontal categorization approach" embodied in the Communications Act").

191. FTC PRIVACY REPORT, *supra* note 46, at 55–57.

subject later that year.[192] In the Privacy Report, the FTC started from the principle that the privacy practices of large platform providers such as broadband providers and the makers of operating systems and browsers raise particular concerns because these entities have "very broad access to a user's online activities," and are thus able to track users "for purposes inconsistent with the context of [users'] interaction" with the firm.[193] Specifically addressing broadband providers, the FTC reasoned as follows:

> ISPs serve as a major gateway to the Internet with access to vast amounts of unencrypted data that their customers send or receive over the ISP's network. ISPs are thus in a position to develop highly detailed and comprehensive profiles of their customers—and to do so in a manner that may be completely invisible. In addition, it may be difficult for some consumers to obtain alternative sources of broadband Internet access, and they may be inhibited from switching broadband providers for reasons such as inconvenience or expense. Accordingly, the Commission has strong concerns about the use of DPI for purposes inconsistent with an ISP's interaction with a consumer, without express affirmative consent or more robust protection.[194]

In a single paragraph, the FTC identifies three variables that may justify imposing different degrees of regulation on different firms: the visibility of the firm's data collection; whether the firm has market power; and the firm's degree of access to user data.[195] Let's take these issues one at a time.

1. Market Power

Both the FCC and the FTC appear to assume that a firm's power in the broadband market should be an important consideration for regulators of broadband privacy. In its Privacy Report, the FTC asserted that so-called "take-it-or-leave-it" choice is problematic where competition offers customers few alternatives.[196] It suggested that a firm with market power should not be allowed to condition provision

192. *The Big Picture: Comprehensive Online Data Collection*, FTC (Dec. 6, 2012), https://www.ftc.gov/news-events/events-calendar/2012/12/big-picture-comprehensive-online-data-collection.

193. FTC PRIVACY REPORT, *supra* note 46, at 55.

194. *Id.* at 56.

195. The Commission also noted that technological differences in and of themselves do not merit differential treatment, cautioning that "any framework should be technology neutral." *Id.*

196. *Id.* at 50–51.

of a service on whether users permit the firm to collect their data.[197] The FCC echoed this view in the Broadband Privacy Order, prohibiting "'take-it-or-leave-it' offers in which [broadband] providers offer broadband service contingent on customers surrendering their privacy rights."[198] Even the late FTC Commissioner J. Thomas Rosch, a longtime antitrust practitioner who dissented from the Privacy Report, agreed that more onerous regulations should apply to broadband providers with market power than to those without.[199]

However, it is actually not so clear that a broadband provider with market power in broadband has any advantage over broadband providers without market power when it comes to collecting user data. Whether in a competitive or a monopoly market, the rational firm will choose the combination of price and privacy protection that maximizes profit. Assuming that users are able to understand and value privacy protections—that is, assuming that privacy is not an externality—a firm that is already charging the monopoly price for its service would have no incentive to degrade privacy. Doing so would be tantamount to increasing price—but again, the combination of price and privacy is already set at the profit-maximizing level. Degrading privacy without changing price could only reduce profits. In this respect, monopoly providers are no different from providers in a competitive broadband market. Whether in a competitive or a monopoly market, *every* offer is take-it-or-leave-it: buy my product, or buy someone else's (or don't buy at all).

If the assumption that users are able to properly value privacy protections is incorrect, then there would indeed be no check on broadband providers that wished to degrade privacy. However, this would be equally true of providers with market power as those without. Accordingly, market power in broadband cannot be said to provide broadband providers the opportunity exploit consumers, *apart from the extent to which they are already exploiting them by charging high prices*. In the absence of price regulation, then, market power in broadband services should not have any bearing on privacy regulation.

2. Visibility

The visibility of broadband providers' data collection practices, on the other hand, *would* appear to present a valid reason for asymmetric regulation. In its Privacy Report, the FTC justified its conclusion that

197. *Id.* at 50–52.
198. Broadband Privacy Order, *supra* note 22, ¶ 294.
199. FTC PRIVACY REPORT, *supra* note 46, at C-7–8 (Rosch, Comm'r, dissenting).

broadband providers should be subjected to more stringent privacy rules in part on the ground that they are able to collect data "in a manner that may be completely invisible."[200] The FCC similarly concluded that broadband providers' data collection is less visible than that of edge providers, because the latter "only have direct access to the information that customers choose to share with them by virtue of engaging their services."[201]

The FCC's phrasing overstates the case—a consumer can hardly be said to have "consented" to data collection by invisible third parties such as Google and Facebook simply by browsing third-party websites—but the general assumption that broadband providers' data collection is less visible to users than that of other firms seems sound, given that few customers are aware that such providers collect user data at all. If this is indeed the case, it would provide a valid reason to require more onerous notice requirements of broadband providers. This is generally in line with the FTC's insistence that firms give "prominent notice" where their data collection is "[in]consistent with the context of a particular transaction or the consumer's relationship with the business."[202]

However, whether *choice* rules should differ based on the visibility of data collection, as the FTC appeared to insist,[203] is a more complicated issue. While notice is the usual regulatory solution to information externalities, choice is typically thought to solve for a different externality: facilitating bargaining where transaction costs would otherwise prevent it. If choice only helps users overcome hurdles to bargaining for greater privacy protection, then the visibility of a given privacy practice should not bear on whether choice is required. Visibility presents solely an informational problem.

But the provision of opt-in choice also plays an important if little-acknowledged role in informing consumers. It incentivizes firms to make their privacy notices clear and prominent, because firms will want to encourage consumers to exercise the choice and opt in. This may provide a rationale for subjecting less-visible practices to opt-in choice requirements in situations where there is reason to believe that notice alone may not suffice.

It may also explain the FTC's seemingly anomalous stance in urging the FCC to classify content data obtained through deep packet

200. *Id.* at 56.
201. Broadband Privacy NPRM, *supra* note 18, at 2547.
202. FTC PRIVACY REPORT, *supra* note 46, at 27.
203. *Id.*

inspection as sensitive, and thus subject to opt-in choice.[204] The FTC had never before suggested that *all* content information should be classified as sensitive.[205] If it really held that view, it would presumably have brought an enforcement action against Google for its longstanding practice of collecting content data through Gmail without requiring opt-in approval. The relative *invisibility* of data-collection via deep packet inspection, however, may explain the FTC's position.

3. Access to Data

Access to data is the remaining consideration the FTC offered as a rationale for differential regulation of broadband providers in its Privacy Report. According to the FTC, greater access to data calls for more restrictive privacy rules, because it enables a firm to develop a more granular picture of users.[206] The FCC adopted this premise in the Broadband Privacy Order, reasoning that broadband providers' supposed access to more data than other large platform providers justified stricter privacy rules.[207]

Whether broadband providers actually *do* enjoy more access to user data than do edge providers, particularly Google, was hotly debated before the FCC. The FCC concluded that they did,[208] following the same finding by the FTC.[209] A number of commenters strenuously argued this conclusion was incorrect,[210] particularly in light of Google's prevalence on other firms' websites and in the markets for browsers and mobile devices.[211] Evaluating the issue in depth is beyond the scope of this article, but it should at least be noted that whether broadband providers have a data advantage over edge providers is debatable. It is unclear whether broadband providers actually do have access to more data; unclear how much value content data adds to app-usage and web-browsing data; unclear whether broadband providers will be able to monetize that data any time soon;

204. *See* FTC Comment Letter, *supra* note 122, at 20–21.

205. FTC PRIVACY REPORT, *supra* note 46, at 58–60.

206. *Id.* at 55–56.

207. Broadband Privacy Order, *supra* note 22, ¶¶ 28–37.

208. *Id.*

209. FTC PRIVACY REPORT, *supra* note 46, at 56.

210. *See* Swire, *supra* note 156; Reply Comments of the Int'l Ctr. for Law & Econ., In re Protecting the Privacy of Customers of Broadband and other Telecommunications Services, WC Dkt. No. 16-106, ICLE 14–15, (July 6, 2016), https://ecfsapi.fcc.gov/file/10707812924625/ICLE%20-%20Privacy%20NPRM%20Reply%20Comments.pdf (arguing that the quality of data broadband providers may collect is probably inferior to that of edge providers, and that such data is thus more difficult to monetize).

211. Oracle Pet'n for Reconsideration, *supra* note 169, at 4–7.

and possible that encryption will wipe out any advantage broadband providers might enjoy. In addition, the issue of which factors a regulator should take into account in determining which firm has greater access to data is up for debate (e.g., whether regulators should consider a firm's superior data-analytics abilities, or economic barriers to harvesting data in additional to technical ones).

More fundamentally, however, it is not so clear that a firm's greater ability to collect data (however defined) should necessarily entail more stringent regulatory treatment. First, as described above in the analysis of the effect that enforcement of broadband privacy might have on the ad intermediation market, firms' different positions in secondary markets may warrant different treatment.[212]

Second—perhaps counterintuitively—greater access to data might actually call for more *lenient* regulatory treatment. True, firms that collect more data may be able to cause more privacy harm on a per-byte basis, because more insights can be gleaned from analyzing data points collectively than from doing so separately. But the other side of the coin is that the *benefits* of data collection by large firms may be disproportionately large, as well, for exactly the same reason. This is not to say that this is necessarily a zero-sum game: whether large platform providers deserve stricter or looser rules will depend on a regulator's assessment of the benefits and drawbacks of data collection in a particular context. How a regulator should make this assessment is beyond the scope of this Article, which merely seeks to frame the issue appropriately.

B. How Should the FTC Reconcile Broadband Privacy and Net Neutrality?

Advocates of net neutrality argue that government intervention is necessary to prevent broadband providers from discriminating against certain types of edge providers. Now that the FCC has reversed its decision to reclassify broadband as a Title II common carrier service—rescinding its Open Internet Order, which imposed net neutrality rules—the FTC and the Department of Justice will presumably be tasked with policing anticompetitive discrimination by broadband providers under antitrust law.

As Professor Paul Ohm has pointed out, however, enforcement of

212. *See* Computer III, *supra* note 163, at 985 (noting that regulatory burdens may differ based on the "economic characteristics of both the service provider and the market for that service"); *see infra* Part II.C.2.

broadband privacy rules could be used as a backdoor means of net neutrality regulation.[213] Any privacy rules that prevent broadband providers from scrutinizing the data that flow through their networks could prevent providers from engaging in differential treatment of edge providers, because broadband providers "cannot discriminate between packets without scrutinizing them first."[214] The broadband privacy debate is thus inextricably intertwined with the issue of net neutrality. In enforcing its privacy standards against broadband providers, the FTC will have to determine whether providers should be granted an exception to monitor traffic for purposes of differential treatment.

Professor Ohm views privacy considerations as a kind of plus-factor that provides additional support for net neutrality regulation:

> An architecture of discrimination is an architecture of surveillance, one that can be lent out to intelligence agencies, copyrighted content owners, and subpoena-wielding civil litigants to reveal everybody's deepest secrets. A neutral network is a more private network.[215]

In Professor Ohm's conception, a procompetitive instance of discrimination—say, requiring a video provider like Netflix to pay for its disproportionate use of bandwidth, enabling broadband providers to reduce prices for users—might be overcome by privacy concerns, and rendered unlawful.[216] In other words, privacy concerns may push otherwise unobjectionable discriminatory treatment over the line into unreasonableness.

The idea of taking privacy into account in considering differential pricing of broadband service is effectively a dead letter, however, now that net neutrality has become an issue for antitrust enforcement. Consumer concerns such as privacy have no role in American antitrust analysis, unless they can be folded into an argument that a particular practice will decrease output.[217] For instance, as Richard Posner has pointed out, the fact that fewer cars on the road would lead to less pollution would not be a valid defense in an antitrust suit against colluding automakers.[218]

We might reverse Professor Ohm's hypothetical, however, and

---

213. Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1490–96 (2009).

214. *Id.* at 1490.

215. *Id.* at 1494.

216. *Id.*

217. *See* Richard A. Posner, *Antitrust Policy and the Consumer Movement*, 15 ANTITRUST BULL. 361, 362–63 (1970).

218. *Id.* at 363–65.

ask whether procompetitive or otherwise welfare-enhancing differential treatment should save a practice that would otherwise be condemned under the FTC's privacy standards. There is no barrier to the FTC considering non-privacy issues in enforcing Section 5 against a broadband provider for its privacy practices, given Section 5's broad condemnation of unfair and deceptive acts and trade practices. While allowing differential treatment to save a practice under Section 5 would run counter to the populist version of net neutrality, it is logically consistent with Professor Ohm's proposal to treat net neutrality as a concern of general welfare, rather than a narrow economic proposition. And it must be pointed out that differential treatment of edge providers is in fact often procompetitive. [219] As Jonathan Nuechterlein has observed, not even the most fervent net neutrality advocate thinks that broadband providers should *never* be allowed to treat packets differently.[220] Instead, the argument advanced by net neutrality advocates is that broadband providers have too much power in the market for Internet access, and could abuse that power by trying to promote their own affiliates to the detriment of competitors in the adjacent markets for applications and content.[221] Where a broadband provider discriminates against certain types of traffic not to favor its own products, but instead to better allocate costs among the users of its pipes, its action will generally by procompetitive.

The FTC should thus carve out an exception to its broadband privacy standards to allow for differential treatment of edge providers where such treatment is procompetitive and welfare-enhancing. This would be akin to the exception in the FCC's Broadband Privacy Order for "reasonable network management" practices.[222] The FCC found that management practices are reasonable and therefore lawful where they are "primarily used for and tailored to achiev[e] a legitimate network management purpose, taking into account the particular network architecture and technology of the broadband service."[223]

---

219. Dennis L. Weisman & Robert B. Kulick, *Price Discrimination, Two-Sided Markets, and Net Neutrality Regulation*, 13 TUL. J. TECH. & INTELL. PROP. 81, 97 (2010) ("By creating incentives for an ISP to charge lower prices on the subscriber side of the market, price discrimination on the content side of the market increases the total number of transactions between content providers and subscribers—precisely the conditions under which price discrimination is likely to increase social welfare.").

220. Jonathan Nuechterlein, *Antitrust Oversight of an Antitrust Dispute: An Institutional Perspective on the Net Neutrality Debate*, 7 J. TELECOM. & HIGH TECH. L. 19, 37 (2009).

221. *Id.* at 39.

222. Broadband Privacy Order, *supra* note 22, ¶ 208.

223. *Id.*

Here, scrutinizing network traffic to the extent necessary to make decisions regarding procompetitive differential treatment should qualify as something akin to reasonable network management.

Failing to carve out such an exception could give edge providers an incentive to use encryption tools for no other purpose than to frustrate broadband providers' attempts to treat their traffic differently. Encryption in this circumstance would either make it more costly or impossible for broadband providers to impose differential treatment on different types of traffic, thereby reducing welfare. The relevant question under Section 5 should instead be whether a firm has exceeded the scope of its procompetitive purpose for collecting and processing user data.

C. Will the FTC Prioritize Broadband Privacy?

As detailed above, the FTC's approach to the substantive privacy issues involving broadband providers will in all likelihood be largely similar to the FCC's.[224] However, the effect that FTC privacy regulation has on broadband providers will depend in large part on how it monitors providers, how deeply it investigates them, and how often it actually brings enforcement actions against them. This section seeks guidance in the Commission's past statements and its pattern of Section 5 enforcement to determine how its enforcement of broadband privacy will actually play out. The FTC's close scrutiny of Google, another large platform provider, and the Commission's responsiveness to privacy concerns when they are raised in the media indicate that it is likely to watch broadband providers fairly closely.

The FCC would likely have devoted considerable resources to enforcing its broadband privacy rules had Congress not repealed the Broadband Privacy Order, given that broadband would have been essentially the only industry over which the Commission had exclusive privacy enforcement authority.[225] In contrast, broadband is only one of many industries under the auspices of the FTC's Section 5 jurisdiction. The FTC brings only twenty-five or so privacy and data-security cases per year, and does not have the resources to scrutinize every firm closely.

Does this mean that broadband providers might fly under the

224. *See supra* Part II.C.1.

225. The Telecommunications Act also provides for the privacy of satellite and cable subscribers. 47 U.S.C. § 338(i)(1)(A); *id.* § 551. However, the FTC also has jurisdiction over these firms' privacy practices, because the FCC does not regulate them as common carriers. 15 U.S.C. § 45(a)(2).

radar, now that they fall within the scope of the FTC's jurisdiction? Answers are not easily found in FTC enforcement actions against broadband providers prior to the FCC's 2015 reclassification, because the FTC has never brought such an action, save for a 2009 complaint against DIRECTV and Comcast for violating do-not-call laws.[226] However, this lack of enforcement actions is not particularly revealing, because broadband privacy has only emerged on regulators' radars fairly recently.

Instead, given the FTC's view that large platform providers raise unique privacy concerns, the Commission's treatment of Google may provide the clearest hint of how it will scrutinize broadband providers' privacy practices. The FTC has brought only one privacy complaint against Google in its history, in a garden-variety failure-to-disclose case.[227] On the whole, however, it has monitored Google's business practices quite closely. For instance, the FTC in 2012 conducted a major investigation into whether Google's data-collection and other practices warranted an antitrust enforcement action, though it eventually decided not to file a complaint.[228] There is thus reason to think the FTC will examine broadband providers' practices fairly closely, as well.

The attention afforded broadband providers' privacy practices in the press may also increase the likelihood of FTC enforcement. The Commission frequently files complaints on the heels of news reports of invasive privacy practices—perhaps because it is responding to what it perceives to be the will of the public, perhaps because sniffing out privacy violations is easier when advocacy and media groups lead the way. For instance, both the FCC and FTC privacy-enforcement actions concerning the use of supercookies by Verizon and its partners followed widespread media attention on the practice.[229] And the FTC's

---

226. Press Release, *DIRECTV, Comcast to Pay Total of $3.21 Million for Entity-Specific Do Not Call Violations*, FTC (April 16, 2009), https://www.ftc.gov/news-events/press-releases/2009/04/directv-comcast-pay-total-321-million-entity-specific-do-not-call.

227. Complaint, In re Google Inc., No. C-4336 (Oct. 13, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzcmpt.pdf.

228. *See* Brody Mullins et al., *Inside the U.S. Antitrust Probe of Google*, WALL ST. J. (Mar. 19, 2015), https://www.wsj.com/articles/inside-the-u-s-antitrust-probe-of-google-1426793274; *see also* Press Release, *Google Agrees to Change Its Business Practices to Resolve FTC Competition Concerns*, FTC (Jan. 3, 2013), https://www.ftc.gov/news-events/press-releases/2013/01/google-agrees-change-its-business-practices-resolve-ftc.

229. *See* Natasha Singer & Brian X. Chen, *Lawmakers Call for Investigation into Verizon's Use of Mobile 'Supercookies,'* N.Y. TIMES (Feb. 6, 2016), https://bits.blogs.nytimes.com/2015/02/06/lawmakers-call-for-investigation-into-verizons-use-of-mobile-supercookies//.

2015 complaint against Nomi Technologies, a firm that tracked customers around retail stores, came on the heels of a feature about the company in *The New York Times*.[230] Continued scrutiny of broadband providers by consumer advocates and the media may thus make privacy enforcement actions in this arena more likely.

CONCLUSION

Regulators are only beginning to grapple with the issues raised by the privacy practices of broadband internet providers. Despite the widespread assumption that the FCC's governance of broadband privacy would have been more robust than the FTC's, the analysis presented here suggests that the commissions' practices are actually likely to be quite similar. Nonetheless, a number of unanswered questions remain about how the FTC will enforce Section 5 against broadband providers. How the Commission answers these questions will do much to determine how effective its regulation will be.

230. Joshua D. Wright, *The FTC and Privacy Regulation: The Missing Role of Economics*, GEO. MASON U. L. & ECON. CTR. 14 (Nov. 12, 2015), http://masonlec.org/site/rte_uploads/files/Wright_PRIVACYSPEECH_FINALv2_PRINT.pdf.