The FCC Forgot Something in Piecing Together Its Complex Proposal for Broadband Privacy Regulation: Consumers

By Rosemary C. Harold

Note from the Editor:

This article discusses the FCC's proposed rules for broadband privacy, and criticizes them for departing from the FTC's tried-and-true regulation practices and for insufficiently considering consumers' expectations and needs.

The Federalist Society takes no positions on particular legal and public policy matters. Any expressions of opinion are those of the authors. Whenever we publish an article that advocates for a particular position, as here, we offer links to other perspectives on the issue, including ones opposed to the position taken in the article. We also invite responses from our readers. To join the debate, please email us at info@fedsoc.org.

• *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, NPRM, 31 FCC Rcd 2500 (2016), https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-39A1_Rcd.pdf.

• Letter from Bernie Sanders, Ed Markey, Elizabeth Warren, Richard Blumenthal, Al Franken, Patrick Leahy, and Tammy Baldwin, Senators, to Tom Wheeler, FCC Chairman, *available at* http://www.markey.senate.gov/imo/media/doc/Letter%20--%20FCC%20Privacy%20%207-7-16.pdf.

• Testimony of Prof. Paul Ohm, Subcommittee on Communications and Technology, Committee on Energy and Commerce, U.S. House of Representatives (June 14, 2016), https://ecfsapi.fcc.gov/file/106190685108718/PaulOhmTestimony06142016HouseSubCommTech.pdf.

• Reply Comments of Prof. Paul Ohm, Federal Communications Commission (June 22, 2016), https://ecfsapi.fcc.gov/file/10622254783425/OhmReplyComments.pdf.

• Natasha Lomas, *As FCC considers new broadband privacy rules, report urges wider user data safeguards*, TechCrunch (Mar. 23, 2016), https://techcrunch.com/2016/03/23/as-fcc-considers-new-broadband-privacy-rules-report-urges-wider-user-data-safeguards/.

About the Authors:

The author is a partner in the law firm of Wilkinson Barker Knauer, LLP. *She thanks her colleagues at the firm, Bryan N. Tramont, Aaron Burstein, and Melissa Turcios, for their assistance with this article.*

Introduction

Readers who wade through the Federal Communications Commission's 100+ page *Privacy Notice*—the agency's proposed rules for broadband internet access providers ("ISPs" or "broadband providers")[1]—may find it difficult to spot a strong connection between those proposals and the internet privacy protections familiar to consumers today. There is a reason for that: The FCC's proposals reflect its regulatory past, not consumers' online present.

The FCC opened its broadband privacy rulemaking proceeding in March 2016 and may be on track to adopt new rules before the November elections. This is a remarkably speedy pace, especially given the complexity of the issues and the degree to which the FCC's proposals diverge from the Federal Trade Commission's more flexible privacy regulations that have governed ISPs—and all other players in the online ecosystem—for years. The FTC's expertise in protecting consumer privacy dates back to the 1970s, well before the internet emerged; since then, the FTC has worked methodically to develop and enforce privacy requirements that center on consumers' reasonable expectations that certain information, such as health and financial data, is more sensitive and therefore warrants more protection than, say, data showing shopping habits.[2] Today, the FTC places significant emphasis on a business enterprise's disclosure of its privacy practices to consumers and the enterprise's adherence to its own promises.[3] This approach covers essentially all consumer-facing companies in the online marketplace, including "edge providers" such as browsers, search engines, online retailers, and social media. Americans who use the internet today are accustomed to the online privacy standards the FTC has fostered.[4]

The FCC, on the other hand, is a newcomer to internet privacy issues. Although the agency has enforced statute-specific

1 *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, NPRM, 31 FCC Rcd 2500 (2016) [hereinafter *Privacy Notice*], https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-39A1_Rcd.pdf.

2 *Protecting Consumer Privacy*, Fed. Trade Comm'n (FTC), https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy (last visited Aug. 31, 2016) (history of FTC privacy enforcement); Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers, Fed. Trade Comm'n 15-16 (Mar. 26, 2012) [hereinafter FTC Privacy Report], https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

3 *See generally* FTC Privacy Report, *supra* note 2, at 23-30, 60-70; *see also Enforcing Privacy Promises,* Fed. Trade Comm'n, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises (last visited Aug. 31, 2016).

4 More than 84 percent of adult Americans use the internet today, with notable variations by age. For young adults, the figure is 96 percent. Andrew Perrin & Maeve Duggan, *Americans' Internet Access: 2000-2015*, Pew Research Ctr. (June 26, 2016), http://www.pewinternet.org/2015/06/26/americans-internet-access-2000-2015.

privacy requirements on the original "common carriers" under its jurisdiction (i.e., traditional voice telephony providers)[5] until recently it lacked the legal authority to impose such rules on broadband providers. That changed in February 2015, when the FCC reversed course on its underlying legal approach to regulating ISPs by "reclassifying" broadband internet access service ("BIAS") as common carriage under Title II of the Communications Act.[6] Privacy considerations were not the driving factor behind the FCC's adoption of these "net neutrality" rules, but by virtue of an exemption for common carriers in the FTC's own governing statute,[7] the FCC's decision effectively stripped its sister agency of power to continue to police ISPs.

The FCC now is trying to fill the gap it created. Rather than build on the FTC's established foundation, however, the FCC appears determined to retrofit and expand its old rules for voice telephony[8] in a manner that likely will confuse or annoy consumers, while effectively discouraging broadband providers from offering new, competitive choices for online products and services. The FCC's proposals include a three-level consent regime, with requirements that turn on the identity of the online user of the information—i.e., whether the entity is the ISP, an affiliate, or a third party—rather than on how sensitive the information is, regardless of who may be using it. Required consent mechanisms also would vary based on whether the product or service being promoted fits into the vaguely defined (but apparently narrow) category of "communications-related services."[9] When in doubt, the proposed rules would require an ISP to seek affirmative "opt in" consent from consumers,[10] even when most consumers would not consider the data at issue—such as their online shopping interests—to be particularly sensitive.

As a result, the FCC proposal would require ISPs and their affiliates to pepper consumers with frequent opt-in consent requests covering all sorts of data, whether sensitive or not. Edge providers, on the other hand, need only abide by the FTC's more flexible approach—which calls for opt-in consent simply when the information concerns facts that most consumers would consider sensitive and therefore in need of additional safeguards. Thus, two different online entities might seek to market the exact same product or service to consumers, but be faced with decidedly different privacy mandates. On the broadband provider side, the proposed FCC rules would impose additional costs on both consumers (in terms of time) and broadband providers (in terms of time and resources), for no obvious beneficial purpose. Consumers also may detect the differences as they comparison shop across websites and wonder why the processes are so uneven.

It should not have to be this complicated. Consumers should be able to protect their sensitive information from online disclosures without being inundated by frequent requests for sharing data that most people do not consider sacrosanct. Consumers should not be forced to guess whether an entity holding and using their data is an ISP's affiliate, or how closely related the entity's product or service is to the ISP's service, in order to understand how to make choices about the collection, use, and sharing of their private information.[11] And ISPs should be able to compete on a level regulatory playing field in offering innovative products and services against rivals (in many cases much larger and more ubiquitous entities) that still will be governed by the FTC's consumer-centric approach to privacy regulation.

The discussion below provides background on the legal and policy considerations underlying the *Privacy Notice*, followed by details on certain rule proposals—the asymmetric burdens ISPs would shoulder generally, the complex construct for obtaining consumer consent, and the FCC's skepticism about customer discount programs—and how they differ from the FTC's approach.[12] The analysis ends with a review of constitutional objections also raised against the FCC's proposal.

I. Background: Two Commissions Develop Distinctly Different Approaches to Consumer Privacy

The disconnect between the FCC and the FTC on broadband privacy is rooted partly in the two agencies' different approaches to regulation generally. The FCC has broad rulemaking authority over the relatively narrow "communications" sector of the U.S. economy, and for decades it has proposed and adopted new rules—often very detailed ones—for the entities under its jurisdiction. While this rules-based approach arguably may help regulated entities by establishing bright-line directives, it is not well suited to parts of the communications sector undergoing rapid technological change. Adopting a new set of substantial rules usually takes years; the time frame often includes court challenges and remands back to the FCC that require another round of notice-and-comment rulemaking.[13] The result too often has been prescriptive regulations tailored to the technology in place at the time of the rules' adoption, but which may become increasingly out of date (and even nonsensical) as new technological breakthroughs supplant old hardware and software.[14]

5 *See* Telecommunications Act of 1996, 47 U.S.C. § 151 *et seq.* (1996) [hereinafter 1996 Act], https://transition.fcc.gov/Reports/1934new.pdf; 47 U.S.C. § 222 (common carrier privacy requirements).

6 *Protecting and Promoting the Open Internet*, Report & Order, 30 FCC Rcd 5601 (2015) [hereinafter *Open Internet Order*], https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1_Rcd.pdf.

7 Federal Trade Commission Act, 15 U.S.C. § 45(a)(2) [hereinafter FTC Act].

8 *Privacy Notice*, *supra* note 1, ¶ 302.

9 *Id.* ¶¶ 71-73.

10 *Id.* ¶¶ 139-142.

11 At different points the *Privacy Notice* focuses on one or more of the three activities—data collection by the ISP, internal use of the data by the ISP, and sharing of the data with third parties. For simplicity's sake, this overview employs the term "use" broadly to refer to all three activities.

12 The *Privacy Notice* calls for comment on several other significant issues that are not addressed here, including the timing and wording of ISP messages seeking consumer consent; data security requirements; breach notification mandates; and the use of disaggregated, anonymous consumer data as a privacy-protection mechanism.

13 One illustration of this process is the FCC's history of attempting to update its broadcast ownership rules, which over five cycles of rulemaking and court remand over two decades has resulted in little change. *See, e.g.*, Prometheus Radio Project v. FCC, 824 F.3d 33 (2016) (referencing vacating the new FCC media ownership rules).

14 For example, the FCC's effort to implement a provision of the Telecommunications Act of 1996 calling for "competitive availability" of "navigation devices" used with cable services, 47 U.S.C. § 76.640(a)-

In contrast, the FTC has relatively little notice-and-comment rulemaking authority. Instead, it largely proceeds by pursuing enforcement actions against specific companies under Section 5 of the Federal Trade Commission Act, which broadly empowers the FTC to police "unfair or deceptive acts or practices."[15] With respect to consumer privacy cases, the FTC typically deems misleading privacy policies or practices to be "deceptive" while unreasonable data security safeguards are treated as "unfair."[16] Over time, the agency has developed three core principles—transparency, consumer choice, and data security—to guide its privacy enforcement actions.[17]

The FTC has brought more than 500 privacy and data security cases to date, covering both online and offline information.[18] Companies now operating under FTC enforcement orders include online giants such as Facebook, Google, Twitter, and Snapchat.[19] The FTC also has considered whether ISPs are so distinct from other "large platform providers" that special, more stringent regulations should apply. The general answer was determined to be "no": "[A]ny privacy framework should be technology neutral. ISPs are just one type of large platform provider that may have access to all or nearly all of a consumer's online activity."[20]

Developing regulation through case precedent may not provide immediate, bright-line guidance to regulated entities, but it does allow for flexible and relatively quick adaptation of settled principles to new situations, including changes over time in technology and consumer use. As FTC Commissioner Maureen Ohlhausen has explained, her agency's case-by-case application of its principles "has major advantages over a prescriptive rule-making approach. The FTC's approach minimizes the regulator's knowledge problem, fosters incrementalism, and focuses limited resources on addressing consumer harm. These advantages are particularly beneficial in fast-changing areas such as privacy and data security."[21]

The FTC also provides guidance by developing issue-specific reports and other educational tools, which often draw on input from interested businesses, consumers, and academics. For online privacy purposes, the FTC's 2012 report *Protecting Consumer Privacy in an Era of Rapid Change* ("*FTC Privacy Report*") has been seminal. Consistent with FTC case law, the *FTC Privacy Report* distinguishes between (1) personal data collected and used "consistent with the context of the transaction or the company's relationship with the consumer," for which express consent is not needed; and (2) collecting sensitive data or using consumer data "in a materially different manner than claimed when the data was collected," for which affirmative consent is required.[22] The FTC approach encourages online entities to provide "opt out" options to consumers who may prefer to restrict the use and sharing of personal information—a construct that studies show leads to more sharing of non-sensitive information, such as buying habits, than does the more restrictive "opt in" alternative.[23]

Section 5 reins in the FTC's broad authority in a few specific business arenas, however, and common carriage is one of them.[24] Until 2015, that exemption was not much of a limitation with respect to broadband privacy because the FCC—in a series of pronouncements and decisions between 1998 and 2008—determined that BIAS was not common carriage.[25] Instead, the

(b), triggered years of regulatory and engineering efforts to develop the "CableCARD" rules, § 76.1205(b)-(c), 1602(b). Those rules supported technology that could separate content security from set-top boxes, which then could be independently developed and sold in retail stores. By the time the analog-based technology reached the marketplace, however, cable operators were upgrading their systems to digital technology, which is not compatible with CableCARDs. *See* FCC Public Notice, Comment Sought on Video Device Navigation (Dec. 3, 2009) ("The Commission's CableCARD rules have resulted in limited success in developing a retail market for navigation devices.").

15 FTC Act, *supra* note 7, § 45(a)(1).

16 *See, e.g.*, FTC, Commission Statement Marking the FTC's 50th Data Security Settlement at 1 (Jan. 31, 2014), https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.

17 *See* Comments of the Staff of the Bureau of Consumer Protection of the FTC, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106, 6 (filed Feb. 23, 2016) [hereinafter FTC Staff Comments], https://ecfsapi.fcc.gov/file/60002078443.pdf.

18 *Id.* at 4 and n.11, *citing* Letter from Edith Ramirez, Chairwoman, FTC, to Věra Jourová, Comm'r for Justice, Consumers & Gender Equality, Eur. Comm'n at 3 (Feb. 23, 2016), https://www.ftc.gov/public-statements/2016/02/letter-chairwoman-edith-ramirez-vera-jourova-commissioner-justice.

19 *See, e.g.*, *Snapchat, Inc.*, FTC File No. 132-3078, Docket No. C-4501 (2014); *see generally Privacy and Security Cases*, Fed.Trade Comm'n, https://www.ftc.gov/datasecurity (last visited Aug. 31, 2016).

20 FTC Privacy Report, *supra* note 3, at 56; *see also* J. Howard Beales & Jeffrey A. Eisenbach, Putting Consumers First: A Functionality-Based Approach to Online Privacy (Jan. 1, 2013), http://ssrn.com/abstract=2211540 (arguing that attempts to impose an asymmetric privacy regulations targeted at particular technologies, business models or types of firms would be counterproductive); *see also* Big Data: A Tool for Inclusion or Exclusion?, Fed. Trade Comm'n (Jan. 2016) [hereinafter FTC Big Data], https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf (focusing on how commercial use of big data from consumer information can impact low-income and underserved populations).

21 Comment of Comm'r Maureen K. Ohlhausen, Fed. Trade Comm'n, WC Docket No. 16-106 at note 4 (filed May 27, 2016) [hereinafter Ohlhausen Statement], https://ecfsapi.fcc.gov/file/60002079250.pdf.

22 FTC Privacy Report, *supra* note 2, at vii-viii.

23 *See* Mindi Chahal, *Consumers less likely to 'opt in' to marketing than to 'opt out'*, Marketing Week, May 7, 2014, https://www.marketingweek.com/2014/05/07/consumers-less-likely-to-opt-in-to-marketing-than-to-opt-out/ (study found that 29 percent of respondents would opt-in compared to 51 percent who would not opt-out); Eric J. Johnson, et. al., Defaults, Framing and Privacy: *Why Opting In-Opting Out*, 13 Marketing Letters 5, 7-9 (2002), https://www0.gsb.columbia.edu/mygsb/faculty/research/pubfiles/1173/defaults_framing_and_privacy.pdf. (finding that opt-out choices led to participation by up to twice as many people as opt-in choices).

24 The exemption dates back to the FTC Act's 1914 beginnings. *See* T.C. Hurst & Son v. FTC, 268 F. 874 (E.D. Va. 1920).

25 The FCC's analysis of the issue began with a 1998 report to lawmakers, *Federal-State Joint Board on Universal Service, Report to Congress*, CC Docket No. 96-45, 13 FCC Rcd 11501 (1998), and consistently reached the same conclusion in platform-by-platform classification decisions. *See, e.g.,* High-Speed Access to the Internet over Cable and Other Facilities, 17 F.C.C.R. 4798, 4802 (2002), *aff'd* Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs., 545 U.S. 967 (2005).

FCC decided, it was best "classified" as a lightly regulated, non-common carriage offering under Title I of the Communications Act, which contains few explicit regulatory mandates. Because ISPs face competition from rivals (including cable operators, wireless providers, and wireline telephony networks), the FCC concluded that market forces would deliver consumer benefits in the form of service options and fair prices without the need for heavy-handed rules.

Then the FCC changed its mind.[26] The sharpest dispute in the FCC net neutrality rulemaking concerned the reclassification decision, which determined the legal foundation on which the new rules rest. Common carriage status under Title II comes with scores of obligations and mandates.[27] In reclassifying broadband service, the FCC used its "forbearance" authority to avoid imposing many common-carriage rules on ISPs.[28] But the FCC did apply the Title II privacy provision, Section 222 of the Communications Act, to broadband providers.

Section 222 has given the FCC has some limited experience over the last two decades with privacy regulation of traditional voice telephony providers. In 1996, Congress directed the FCC to regulate a certain type of common carriage data: the "customer proprietary network information" ("CPNI") collected in connection with the provision of "telecommunications service" such as traditional voice telephony. The statute defines CPNI as "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service … and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[29] CPNI originally was understood to mean data such as customer calling patterns, payment history, and other information derived from a customer's actual use of the voice telephony service, but not more general personal information such as a customer's name and phone number, which often is publicly available from other sources.[30] Section 222 also allows common carriers to use, disclose, or share "aggregate" CPNI (i.e., collective data reflecting patterns of use among large numbers of unidentified customers) for any purpose.[31] Such generalized data has been critical for many benign purposes, such as routine traffic management and long-range network expansion planning.[32]

Until it issued the *Privacy Notice*, the FCC had never indicated that it would revamp its Section 222 rules to expand the provision's reach well beyond CPNI to include a potentially boundless set of "personally identifiable information."[33] Most observers expected the FCC to extend its Section 222 authority to broadband providers in the wake of the net neutrality decision, but many also hoped that the agency would craft regulations patterned on the FTC's approach. That hope seemed reasonable; FCC Chairman Tom Wheeler had repeatedly praised the FTC's privacy efforts through the first quarter of 2016. In January 2016, he said, "[w]hat the FTC has done in that regard is to build a terrific model and so I think one of our challenges is to make sure we're consistent with the kind of thoughtful, rational approach that the FTC has taken."[34] Just days before the FCC's March adoption of the *Privacy Notice*, Chairman Wheeler told reporters that "[w]e're following the same kind of conceptual framework that the FTC has."[35]

But that does not appear to be the way that the FCC's broadband privacy proposal turned out, and even the FTC staff experts on consumer privacy have (politely) said as much.

II. The FCC's Broadband Privacy Rule Proposals—And What the FTC Thinks of Them

Among the more than 250,000 submissions in the broadband privacy rulemaking, two filings stand out: the comments of the FTC's Bureau of Consumer Protection ("FTC Staff Comments") and a related statement from FTC Commissioner Ohlhausen.[36] These submissions are not unprecedented; the views of both the FTC and the U.S. Department of Justice's Antitrust Division occasionally have popped up in various FCC dockets. But the two FTC filings in the broadband privacy proceeding are noteworthy for how often they respectfully disagree with the FCC's rule proposals and underlying assumptions. Below is an overview of several key issues on which the agencies appear to be split.

26 Despite general agreement on light-touch regulation for the internet, a majority of FCC commissioners still wished to impose enforceable regulations on broadband internet access, which led to a series of court losses for the agency. *See* Formal Complaint of Free Press and Public Knowledge Against Comcast Corp. for Secretly Degrading Peer-to-Peer Applications, 23 FCC Rcd. 13,028 (2008), *vacated*, Comcast Corp. v. FCC, 600 F.3d 642, 644 (D.C. Cir. 2010); Preserving the Open Internet, Report & Order, 25 FCC Rcd. 17,905 (2010), *vacated in part*, Verizon v. FCC, 740 F.3d 623 (D.C. Cir. 2014) (certain rules unlawfully imposed common-carrier duties without invoking Title II).

27 There are several ongoing court challenges to the reclassification. *See, e.g.*, Joint Pet'n for Reh'g En Banc, U.S. Telecom Assoc. v. FCC, No. 15-1063 (D.C. Ct. App. July 29, 2016).

28 *Open Internet Order*, *supra* note 6, ¶¶ 493-527.

29 47 U.S.C. § 222(h)(1)(A).

30 Beginning in 2014, however, the FCC's Enforcement Bureau has been interpreting other provisions in Section 222 to broadly encompass additional "private information that customers have an interest in protecting from public exposure," including "personally identifiable information" ("PII"). *See, e.g.*, Terracom, Inc., & Yourtel Am., Inc., Order & Consent Decree, 30 FCC Rcd. 7075 (E.B. 2015).

31 47 U.S.C. § 222(c)(3).

32 As a result, a number of carriers argued both at the FCC and on Capitol Hill that data that can be helpful for network diagnostic purposes should not be deemed "CPNI" under Section 222. *See, e.g.*, Letter from Timothy P. McKone, Exec. Vice Pres., Fed. Relations, AT&T, Inc., to Sen. Al Franken (D-Minn.) at 1 (Dec. 14, 2011) (AT&T uses Carrier IQ "to collect diagnostic information about its network.").

33 *See* EPIC Customer Proprietary Network Information (CPNI), Order, 22 FCC Rcd 6927 (2007) (requiring requires each carrier to certify compliance with the regulations governing customer information).

34 Margaret Harding McGill, FCC, *FTC Chiefs Zero In On Data Security, Privacy*, Law360 (Jan. 6, 2016), http://www.law360.com/articles/743314/fcc-ftc-chiefs-zero-in-on-data-security-privacy.

35 Kate Tummarello & Alex Byers, *Wheeler's crystal ball: Net neutrality decision soon*, Politico (Mar. 17, 2016), http://www.politico.com/tipsheets/morning-tech/2016/03/wheelers-crystal-ball-net-neutrality-decision-soon-garland-a-quick-study-on-telecom-issues-a-path-forward-for-small-biz-bill-in-the-senate-213269.

36 Ohlhausen Statement, *supra* note 21, at 2-4.

A. Are Broadband Providers So Different From Other Online Entities That Heavier Regulation Is Needed?

- FCC: ISPs have unique access to consumer data and so warrant more regulation.
- FTC: No, ISPs are like other big players in the online arena, and privacy regulation should be technology neutral.

From the outset, the FCC's *Privacy Notice* justifies its elaborate rule proposals by contending that ISPs are uniquely positioned to develop highly detailed, comprehensive profiles of their customers. The FCC contends that, absent the use of encryption, "last mile" broadband networks have the ubiquitous ability to monitor traffic transmitted between the consumer and each online destination, including the ability to review the content being accessed or exchanged.[37] According to the FCC, even when traffic is encrypted, the broadband provider can determine which websites a customer has visited, for how long, and during what hours of the day, among other information.[38] Thus, the FCC concludes, ISPs capture a breadth of data that edge providers do not. The FCC also claims that once a broadband consumer signs up for an ISP's service, the consumer simply cannot avoid that network—or easily switch—as he or she could for a search engine or some other edge provider service.[39]

As noted above, the FTC disagrees, at least with respect to the FCC's assertion that ISPs have a uniquely comprehensive view of consumers' online activity. The FTC characterizes ISPs as "just one type of large platform provider that may have access to all or nearly all of a consumer's online activity."[40] At a privacy workshop the FTC held in 2012, the Associate Director of the agency's Privacy Division stated that "there are lots of business models . . . that can permit an entity to get a pretty comprehensive window into consumers' browsing behavior."[41] The FTC has repeatedly stressed the value of a technology-neutral approach to privacy regulation in order to ensure that the government does not "pick[ ] winners and losers" in the online marketplace.[42]

The FTC Staff Comments warned that "the FCC's proposed rules, if implemented, would impose a number of specific requirements on the provision of [broadband] services that would not generally apply to other services that collect and use significant amounts of consumer data. This outcome is not optimal."[43] The FTC has called for broad-based privacy laws applicable to all companies, but until Congress passes such legislation, the FTC Staff Comments gently suggest, federal agencies should harmonize their privacy protection efforts as much as possible.[44]

The two agencies' disagreement about ISPs' technological advantages echoes a split among the private commenters—including public interest groups, associations, and broadband providers—as to whether the purported advantages are real. Several public interest groups, including some allied with edge providers that would not be subject to onerous FCC rules, agree with the FCC's interpretation.[45] Broadband providers and others, including the former head of the FTC's Bureau of Consumer Protection, strongly disagree.[46] Many in the latter group cite to an analysis developed by Georgia Tech's Institute for Information Security and Privacy, which finds that, due to a combination of factors, any given ISP's view of subscriber data is limited, not comprehensive, and is becoming narrower. These factors include a typical consumer's use of multiple devices to access the internet using different ISPs, pervasive encryption of websites, and growing use of proxy services such as virtual private networks ("VPNs")—all of which inhibit any single ISP from being able to track and collect data about subscribers' online activities.

The importance of this issue is hard to overstate: Either ISPs have an advantage in collecting and using consumers' personal data or they do not. If they do not, asymmetric regulation of them is unjustified, and could harm consumers in several ways. Beyond simply confusing or annoying them with elaborate consent mechanisms, the FCC's approach could hurt consumers by effectively blocking the delivery of some targeted advertising that they may want and find useful—although plenty of targeted advertising delivered by edge providers would remain unfettered. The FCC's proposals also may impede competition by dissuading or preventing ISPs from offering new and innovative services, such as home alarm systems, online entertainment platforms, and health-monitoring services, to rival those offered by edge providers.

B. Is a Detailed, Multi-Layered Consent Regime Based on the Identity of the Broadband Entity Necessary?

- FCC: A consent regime based on the data user's identity will help consumers.
- FTC: No, distinctions should turn on the sensitivity of the data, not the entity using it.

The FCC's concept for how broadband providers should obtain consumer consent to use personal information may be the most challenging aspect of the rulemaking—at least for those who are not steeped in FCC regulation. The FCC admits that it drew on its decades-old voice telephony rules in creating the concept, even though the old rules covered considerably less

37 *Privacy Notice*, *supra* note 1, ¶ 4.

38 *Id.* ¶ 4.

39 *Id.*

40 FTC Privacy Report, *supra* note 2, at 56.

41 *See* Transcript of Fed. Trade Comm'n Workshop, The Big Picture: Comprehensive Online Data Collection at 272 (Dec. 6, 2012), https://www.ftc.gov/sites/default/files/documents/public_events/The%20Big%20Picture%3A%20Comprehensive%20Online%20Data%20Collection/bigpicture_transcript_21206ftc.pdf.

42 *Id. See also* FTC Privacy Report, *supra* note 2, at 11.

43 FTC Staff Comments, *supra* note 17, at 8.

44 *Id.* at 8.

45 *See, e.g.*, Comments of Pub. Knowledge, Benton Found., Consumer Action, Consumer Fed'n of Am. & Nat'l Consumers League, WC Docket No. 16-106 (filed May 27, 2016) [hereinafter Public Knowledge Comments], https://ecfsapi.fcc.gov/file/60002080037.pdf.

46 *See* Comments of J. Howard Beales, Prof. of Strategic Mgmt. & Pub. Pol'y, George Washington Sch. of Business, WC Docket No. 16-106 (filed May 27, 2016), https://ecfsapi.fcc.gov/file/60002077356.pdf.

data and were designed to serve narrower purposes.[47] Instead of starting anew by thinking about the consumer's perspective, the FCC proposes different types of consent mechanisms that turn on the identity of the information gatherer/user, not on the sensitivity of the consumer's data. For consent mechanism purposes, it also matters whether the ISP's (or its affiliate's) use of the data is closely "related" to the ISP's "communications services" or not.[48] How a consumer is supposed to grasp any of this is unclear; even broadband providers could struggle with the distinctions.

Specifically, the FCC would divide an ISP's uses of consumer data into three categories, with different consent mechanisms applicable to each:

(1) *Consumer consent will be implied* when the ISP simply uses consumer information, such as an email address or device identifier, in the course of providing the broadband service that the consumer has requested.[49] This would cover a very narrow category of uses, and the implied consent approach is not controversial.

(2) *Consumers must be allowed to opt out* of use their data if the ISP or its affiliate employs the information to market "communications-related services."[50] This is a slightly broader category, but perhaps not by much; the *Privacy Notice* does not define the key term other than to disfavor the broader meaning of "communications-related services" still used in the old voice telephony rules. That broader definition encompassed "information services," the forerunner of today's broadband service.

(3) *Consumers must affirmatively opt in* to consent to a broadband provider's use of personal data for any other purpose—including the sharing of consumer data with any third parties, such as advertisers or partners in marketing goods or services, whether they are communications-related or not. In the real world, this will be the broadest category of all. It will impose extra steps on consumers even when it is not warranted, as would be the case for benign uses such as targeted advertising, which is based on data many consumers do not consider sensitive (and which they will continue to receive from other online entities not subject to FCC rules). And it is likely to impede broadband providers' ability to compete with edge providers in offering such goods and services: Studies show that consumers tend to share less information under an opt-in regime than under on opt-out one, even when the personal data at issue is the same.[51]

The FTC Staff Comments suggest that consumers will not find the FCC's proposed consent regime helpful.[52] To the FTC, the focus should be on the consumer's expectations in light of the consumer's interaction with the company, whatever it may be, and on the reasonableness of those expectations, which likely will turn on the sensitivity of the particular data at issue.[53] Under this light, the FTC staff said, some elements of the FCC's consent scheme—such as implied consent to the use of personal data in the context of the actual provision of broadband service—make sense."[54]

But the FTC staff questioned other elements of the FCC's proposal. With respect to distinguishing between an ISP's affiliate and a third party, the FTC staff pointed out that consumers may find it difficult to differentiate between the two, especially if the affiliate's name offers no hint of a corporate connection to the consumer's ISP.[55] Absent an understanding of the regulations, consumers could be left wondering why some websites or online services pepper them with privacy consent requests while other comparable sites and services do not—a difference that might steer a consumer away from the ones that pester them.

More generally, the FTC staff observed, the FCC's proposed approach:

> does not reflect the different expectations and concerns that consumers have for sensitive and non-sensitive data. As a result, it could hamper beneficial uses of data that consumers may prefer, while failing to protect against practices that are more likely to be unwanted and potentially harmful. For example, consumers may prefer to hear about new innovative products offered by their BIAS providers, but may expect protection against having their sensitive information used for this or any other purpose.[56]

FTC Commissioner Ohlhausen reiterated that point in her assessment: "The FCC's three-tiered "implied consent/opt-out/opt-in" framework . . . does not account for the sensitivity of the consumer data involved. Thus, the FCC would require opt-in consent for many uses of non-sensitive consumer data by BIAS providers, yet would require no consent at all for certain uses of sensitive data by those providers"[57]

In other words, context counts, and rigid rules that repeat old regulatory distinctions, rather than provide scope to assess a consumer's reasonable expectations in the circumstances, will not serve consumers well.

C. Should Consumers Be Required to Consent in Advance to Almost Any Use of Their Data, Even When the Information Is Not Sensitive?

- FCC: Requiring affirmative opt-in consent as the general rule helps consumers.
- FTC: No, repetitive and unnecessary consent requests may be counterproductive.

The FCC's preference for opt-in consent in almost all circumstances is at odds with the FTC's approach, both the FTC

47 *See Privacy Notice*, *supra* note 1, ¶¶ 6-7, 11-13.

48 *Id.* ¶ 107; Peter Swire et al., *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others* (Inst. for Info. Sec'y & Privacy at Georgia Tech., Working Paper, Feb. 29, 2016), http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf.

49 *Privacy Notice*, *supra* note 1, ¶¶ 112-21.

50 *Id.* ¶ 122.

51 *See supra* note 23; *see also* Thomas M. Lenard & Paul H. Rubin, *In Defense of Data: Information and the Costs of Privacy*, Technology Policy Institute, 46 (May 2009) ("[C]onsumers have a tendency not to change the default, whatever it might be.").

52 FTC Staff Comments, *supra* note 17, at 22.

53 *Id.* at 19.

54 *Id.* at 16.

55 *Id.* at 23-24.

56 *Id.* at 22-23.

57 Ohlhausen Statement, *supra* note 21, at 2.

Staff Comments and Commissioner Ohlhausen explained. The FTC staff suggested that the FCC reserve opt-in requirements for a narrow universe of sensitive information that could be collected by broadband providers, including: (1) the actual content of communications, and (2) Social Security numbers or health, financial, children's, or precise geolocation data.[58]

Commissioner Ohlhausen discussed the issue, including the FTC's preference for opt-out consent, at more length. The FTC approach also hews closely to context, Ohlhausen stated, "reflecting the fact that consumer privacy preferences differ greatly depending on the type of data and its use."[59] While consumer preferences are "fairly uniform" with regard to strong protections for sensitive data such as personal financial or medical information, the FTC "know[s] from experience as well as academic research—including a recent Pew study—that for uses of non-sensitive data, people have widely varying privacy preferences."[60]

In addition, the FCC should consider the burdens of exercising and obtaining consent for both consumers and businesses, Ohlhausen said:

> Reading a notice and making a decision takes time that, in the aggregate, can be quite substantial. Regulations should impose such costs in a way that maximizes the benefits while minimizing the costs. Therefore, opt-in or opt-out defaults should match typical consumer preferences, which mean they impose the time and effort of making an active decision on those who value the choice most highly. For advertising based on non-sensitive information, this generally means an opt-out approach. For uses of sensitive information, this generally means an opt-in choice.[61]

Imposing unnecessary burdens on consumers by requiring opt-in consent in almost every instance, even for data considered non-sensitive by many people, carries consequences beyond annoying individuals, Ohlhausen stated. She noted that the cumulative effect of the "burdens imposed by a broad opt-in requirement may also have negative effects on innovation and growth," citing a recent Report of the President's Council of Advisors on Science and Technology as support.[62]

In short, a consent requirement that overburdens consumers has real costs. Besides wasting what can add up to a lot of time in the aggregate, bombarding consent requests may even tend to make consumers numb to requests that they should consider carefully, such as those involving truly sensitive data. The FCC proposal's failure to account for consumer preferences and the way that consumers today generally expect the internet to operate could be counter-productive, producing exactly the opposite result of the FCC's privacy-protection goal.

D. Should Broadband Providers Be Barred From Offering Discounts to Subscribers Who Agree to the Use and Sharing of Some of Their Personal Data?

- FCC: Prohibiting ISPs from offering "financial inducements" in exchange for consent to use of personal data may protect consumers.
- FTC: No, consumers informed about their choices should be free to opt for discount programs because they can cut costs.

The *Privacy Notice* raises questions about controversial discount programs in which an ISP offers lower priced broadband subscriptions in exchange for consumer consent to its use of some personal data, such as shopping and purchasing habits. The disagreement over these programs centers on whether such discounts could take advantage of low-income consumers who might not "generally understand that they are exchanging their information as part of those bargains."[63] Although the FCC dubbed such programs "financial inducement practices," the agency also acknowledged that "it is not unusual for consumers to receive perks in exchange for use of their personal information" in both "the bricks-and-mortar world" of consumer loyalty programs and in the broadband arena where "'free' services in exchange for information are common."[64] The FCC asked in the rulemaking whether it should prohibit financial inducement practices and, if not, what steps it should take to ensure that consumers understand the trade-offs and can change their minds later.

FTC Commissioner Ohlhausen criticized the *Privacy Notice*'s framing of the issue, beginning with the FCC's "mischaracterize[ation]" of the FTC's own 2016 Big Data Report discussion of the topic.[65] She urged the FCC not to flatly ban "dis-

58 FTC Staff Comments, *supra* note 17, at 20.

59 Ohlhausen Statement, *supra* note 21, at 2.

60 *Id.*, *citing* Lee Rainie & Maeve Duggan, *Privacy And Information Sharing*, Pew Research Ctr. (Dec. 2015), http://www.pewinternet.org/2016/01/14/privacy-andinformation-sharing.

61 Ohlhausen Statement, *supra* note 21, at 2. She cited former FTC officials who made the same point eight years ago:

> Customers rationally avoid investing in information necessary to make certain decisions . . . when their decision is very unlikely to have a significant impact on them. . . . Default rules should be designed to impose those costs on consumers who think they are worth paying. An opt-out default rule means that consumers who do not think that decision making costs are worthwhile do not need to bear those costs. Consumers who care intensely, however, will face the costs of making a decision.

J. Howard Beales, III & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. Chi. L. Rev. 109, 115 n. 20 (2008).

62 Ohlhausen Statement, *supra* note 21, at 3, *citing* President's Council of Advisors on Science and Technology, Report to the President: Big Data And Privacy: A Technological Perspective x-xi (May 2014) ("[A] policy focus on limiting data collection will not be a broadly applicable or scalable strategy – nor one likely to achieve the right balance between beneficial results and unintended negative consequences (such as inhibiting economic growth.")).

63 *Privacy Notice*, *supra* note 1, ¶ 260.

64 *Id.*

65 The FTC has not found broadband discount programs to be problematic, Ohlhausen said; the Big Data Report referred to qualms raised by some participants in FTC workshops, but noted that such programs "can create opportunities for low-income and underserved communities." Ohlhausen Statement, *supra* note 21, at 3, *citing* FTC Big Data, *supra* note 20.

counts for ad-supported BIAS" because that action would bar:

> a consumer from trading some of her data for a price discount, even if the consumer is fully informed. Would-be broadband subscribers cite high cost as more important than privacy concerns for the reason why they have not adopted broadband. Given that fact, such a ban may prohibit ad-supported broadband services and thereby eliminate a way to increase broadband adoption.[66]

If it does regulate broadband discount programs in some fashion, Ohlhausen stated, the FCC should at least take into account the FTC's views on the subject: In markets where consumers have choices among broadband providers and the terms of the discount program "are transparent and fairly disclosed . . . such choice options may result in lower prices or other consumer benefits, as companies develop new and competing ways of monetizing their business models."[67]

The discount program debate has been among the liveliest arguments in the FCC's rulemaking docket, with even public interest commenters split as to whether the offerings are beneficial or not.[68] The issue also has become a vehicle for re-arguing larger broadband policy disputes, including the competitiveness, or not, of the BIAS marketplace and incentives needed to drive greater broadband adoption and deployment.[69]

III. Constitutional Dimension: Asymmetric Restraints on Speech Raise Red Flags

Although the FTC staff and Commissioner Ohlhausen confined their input to policy issues, scores of other commenters raised serious legal arguments as well. Statutory authority contentions are front and center for most of them,[70] but another legal issue also is in play: the constitutional right of broadband providers to engage in commercial speech—a right that encompasses the effort to craft such messages for delivery. Somewhat surprisingly, the *Privacy Notice* pays little attention to the First Amendment implications of disproportionately burdening ISPs with broad opt-in consent mandates that would not apply to other entities that use non-sensitive consumer data to market comparable goods and services online. The FCC devotes just one oblique paragraph to the issue.[71]

This attempt to sidestep the First Amendment may reflect the FCC's understanding of the constitutional pitfalls. The FCC routinely confronts free speech challenges to its regulations, primarily in the media space but occasionally also in contexts such as common carriage.[72] The *Privacy Notice* does cite the *Central Hudson* test for evaluating commercial speech restrictions and ticks quickly through the three prongs of the test: (1) the speech restriction must serve a "substantial" government goal; (2) the restraint must "directly advance" that interest; and (3) the restriction must be "no[ ] more extensive than necessary to serve those interests."[73] Yet the FCC never actually applies the test to the facts at hand. The *Privacy Notice* simply asserts, with no evidentiary support, that its proposals—which would effectively restrict, and perhaps stymie, ISPs' use of non-sensitive consumer data to shape targeted advertisements—satisfy the First Amendment. In response, numerous commenters, including constitutional expert Laurence Tribe, point to constitutional infirmities in the proposed rules, including elements that may warrant a more exacting analysis than the "intermediate scrutiny" review accorded to commercial speech regulations.[74]

Even if the FCC's proposed rules were reviewed under intermediate scrutiny, they would be vulnerable. The preeminence of the FTC in the privacy field complicates the FCC's First Amendment position enormously. Government officials considering new speech restrictions rarely need to explain why their favored proposals are better than those of another agency. Even if the FCC's proposed rules could survive the first two prongs of *Central Hudson*, the FTC's privacy regulation will be a major obstacle at the end, because it provides a more tailored alternative for protecting consumer privacy that has been field-tested for years.

In fact, there are no sure wins for the FCC at any point in the *Central Hudson* analysis—and it would need to win on all of them. Regulators typically prevail on the first prong of the test,[75]

66 Ohlhausen Statement, *supra* note 21, at 3.

67 *Id.*

68 *Compare, e.g.*, Comments of Ctr. for Democracy & Tech., WC Docket No. 16-106 at 20-21 (filed May 27, 2016) [hereinafter Ctr. for Democracy & Tech. Comments] *with* Comments of MMTC, WC Docket No. 16-106 at 8 (filed May 27, 2016).

69 *See, e.g.*, Comments of the National Cable & Telecommunications Ass'n, WC Docket No. 16-106 at 13 (filed May 27, 2016) (ISP marketplace is competitive); Reply Comments of the Electronic Privacy Information Center, WC Docket No. 16-106 at 8 (filed July 6, 2016) (most sectors of online marketplace a monopoly or duopoly); Letter of American Association of People with Disabilities, WC Docket No. 16-106 at 1 (filed July 6, 2016) (expressing concern about effect of rule change on broadband adoption and deployment).

70 Critics of the FCC's proposals, including broadband providers large and small, contend that Section 222's telephony-oriented text does not support the sweeping new regulations that the FCC is considering, while supporters insist that the old language can stretch to encompass today's broadband services. *See, e.g.*, Comments of Free Press, WC Docket No. 16-106 at 8-13 (filed May 31, 2016) (supporting an expansive interpretation of Section 222); Ctr. for Democracy & Tech. Comments, *supra* note 68, at 11-12. Wireless broadband providers point to additional provisions of the Communications Act specific to them to bolster contentions that the proposed rules are legally unsound. *See, e.g.*, Comments of Verizon, WC Docket No. 16-106 at 16-28 (filed May 27, 2016); Comments of CTIA, WC Docket No. 16-106 at 44, 55-58 (filed May 26, 2016).

71 *Privacy Notice*, *supra* note 1, ¶ 302.

72 *See, e.g.,* Red Lion Broadcasting v. FCC, 395 U.S. 367 (1969) (spectrum scarcity justifies lower standard of First Amendment protection for broadcasters); Turner Broadcasting System, Inc. v. FCC, 520 U.S. 180 (1997) (upholding mandatory carriage of broadcast stations on cable systems); U.S. West Communications, Inc. v. FCC, 182 F.3d 1224 (10th Cir. 1999) (striking down restraints on analysis and sharing of CPNI among affiliates for use in crafting marketing messages).

73 *Privacy Notice*, *supra* note 1, ¶ 302, *citing* Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557 (1980).

74 Letter of CTIA, *et al.*, WC Docket No. 16-106 (filed May 27, 2016) (submitting Laurence H. Tribe & Jonathan S. Massey, *The Federal Communications Commission's Proposed Broadband Privacy Rules Would Violate the First Amendment* at 23-24, 30-31 (dated May 27, 2016) (FCC proposals incorporate improper speaker- and content-based distinctions)).

75 *See, e.g.*, City of Cincinnati v. Discovery Network, Inc., 507 U.S. 410, 416 (1993).

and the FCC's generalized goal of protecting consumer privacy looks at first blush to be substantial enough. But the reach of the proposed definition for protected data is so expansive that it covers both sensitive material (e.g., information concerning personal finances, health, children, and geo-location) and non-sensitive information that many consumers do not consider confidential (e.g., shopping interests). The *Privacy Notice*'s relatively sparse discussion of concrete consumer concerns refers only to examples that most observers would agree involves *sensitive* data, such as geo-location data and financial data.[76] Moreover, the FCC recognizes that many consumers welcome online advertising targeted to their needs and interests.[77] Why, therefore, should the FCC seek to stringently protect consumers against targeted ads that draw upon non-sensitive data? Are such ads a real problem, much less a substantial one?

Moving to the next *Central Hudson* prong, how can the FCC's proposed restraint shield consumers from the alleged harm of the use of non-sensitive data for targeted advertising when they will continue to receive such data-driven ads from hundreds or thousands of edge providers not subject to FCC regulation? This issue—under-inclusiveness—is another weak point in the proposed regulatory scheme, for the FCC must demonstrate that the opt-in consent mandate would "directly advance" its goal.[78] Even if suppressing targeted advertising based on non-sensitive data were a valid objective, the proposed restrictions are not likely to slow or divert the overall flow of targeted online ads to consumers. The Supreme Court has repeatedly invalidated commercial speech restraints that constrain certain types or sources of speech while leaving others unaffected.[79] The FCC attempts to fend off this criticism by acknowledging that it cannot regulate edge providers' use of data,[80] but this is not a sufficient response—particularly given that the FCC plainly has another regulatory alternative available (i.e., the FTC approach).

The last prong of *Central Hudson* requires the FCC to demonstrate that that its proposed speech restraint is "narrowly tailored," meaning no more extensive than necessary to serve the purported goal.[81] The Supreme Court has explained that, while this prong does not require an agency to employ the least restrictive means possible to advance its objective, the agency still must show that it has considered alternatives before selecting one that "fits" the purpose while still being mindful of the speaker's—and the speech recipient's—constitutional rights.[82] The FCC's obstacle here is obvious: Adopting an opt-in consent mandate burdening the creation and delivery of nearly all targeted advertising by ISPs would require the agency to explain why adopting its own version of the FTC's more constitutionally sensitive approach would be insufficient. Because that approach has been employed for years and been well-accepted by consumers, the FCC would be hard-pressed to defend its more burdensome proposal as sufficiently tailored to serve a valid purpose.

The *Privacy Notice*'s cursory treatment of the commercial speech issues raises some red flags about the FCC's preference for opt-in consent in most circumstances; this means that the FCC's effort to distinguish ISPs from other online entities will be critically important to any future legal defense. As discussed above, the "uniqueness" of ISPs is in hot dispute, whether the claim concerns broadband providers' alleged ability to gather and use customer data or the purported lack of competition among ISPs. The FCC would have to prevail on at least one of these fundamental premises to avoid a serious risk of First Amendment challenge.

IV. Conclusion

The FCC's *Privacy Notice* proposes overly elaborate privacy rules for broadband providers that are likely to confuse consumers, dampen competition for innovative new services, and run afoul of First Amendment constraints. It is not too late for the FCC to pull back from its original proposals and fashion regulations consistent with the FTC's established approach. The latter applies a limited number of privacy principals—transparency, consumer choice, and data security—on a case-by-case basis, along with an appreciation of personal information generally understood to be sensitive, which should be subject to more protective measures than non-sensitive information. That approach also allows that agency to more quickly adapt to changes in technology, as well as trends in consumer uses of technology, than does a detailed rules-based regulatory framework. The attributes of the FTC system for privacy protection serve consumer interests well, and they merit continuation under the FCC's new privacy watch.

76 *E.g.*, *Privacy Notice*, *supra* note 1, ¶¶ 12 (discussing geo-location data), 20-21 (discussing whether Social Security numbers and financial account information should be subject to heightened protection).

77 *Id.* ¶ 12.

78 *See, e.g.*, Greater New Orleans Broadcasting Association, Inc. v. United States, 527 U.S. 173, 188-90 (1999).

79 *See, e.g.*, *Discovery Network*, 507 U.S. at 418-20; *Greater New Orleans*, 527 U.S. at 190, 194-95.

80 *Privacy Notice*, *supra* note 1, ¶ 132.

81 Board of Trustees of the State University of New York v. Fox, 492 U.S. 469, 479-80 (1989).

82 *See id.*