THE TROPE OF PARITY♦

INTRODUCTION 181
I. TECHNICAL BACKGROUND 186
A. *Technological and Market Distinctions Between BIAS and Edge Providers* 186
B. *What the Distinctions Mean for Consumer Privacy* 189
II. COMPARISON OF THE FTC AND FCC APPROACH TO PRIVACY REGULATION 191
A. *Scope of Authority* 191
B. *Enforcement Mechanisms* 192
C. *Key Provisions of the FCC Broadband Privacy Order Compared to Provisions of the FTC 2012 Privacy Report* 195
1. Key Definitions and Provisions of the FCC Broadband Privacy Order 195
2. Key Definitions and Provisions of the FTC Privacy Report 198
3. Comparison of the FCC Broadband Privacy Order and the FTC Privacy Report 201
III. ANALYSIS 203
A. *The Goal of Online Advertising Regulation Should Not Be a Level Playing Field* 204
B. *The Goal of Online Advertising Regulation Should Be Consumer Privacy* 208
CONCLUSION 211

INTRODUCTION

From September to December 2015, the European Commission ("EUC") conducted a public consultation seeking views from its Member States and various other interested stakeholders on how it should modernize the European electronic communications regulatory framework.[1] Meanwhile, in the United States, the Federal

[1] EUROPEAN COMMISSION, Background to the Public Consultation on the Evaluation of the Regulatory Framework for Electronic Communications and on its Review, (Nov. 9, 2015),

Communications Commission ("FCC") similarly sought comment from April to May 2016 on its notice of proposed rulemaking ("NPRM"), which considered new rules to clarify the privacy duties of broadband Internet access service ("BIAS") providers.[2] In response to the EUC public consultation and the NPRM, comments were filed by some of the world's largest BIAS providers, including Vodafone[3] and Deutsche Telekom AG[4] in Europe, and Comcast[5] and AT&T[6] in the U.S.

These comments all make a similar argument, which can be summarized as: government regulation should operate to create a "level playing field" between BIAS providers and edge service providers (non-BIAS Internet companies, such as search engines, email, and social networks). This Note will refer to this common argument as the "trope of parity" because, at its core, it attempts to create a symmetry between BIAS providers and edge providers by saying the rules must apply the same to all actors.

In the U.S., where most privacy regulations are currently enforced by the Federal Trade Commission ("FTC") through a technology-neutral approach,[7] the trope of parity takes the form of BIAS providers asserting that the NPRM's proposed rules *should not* be adopted because they will create an uneven playing field by setting different privacy requirements for BIAS and edge providers.[8] On the other hand, in Europe, where the EUC already regulates BIAS providers more stringently than edge providers,[9] but is currently considering subjecting

http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=10824.

[2] Press Release, Federal Communications Commission, FCC Proposes to Give Broadband Consumers Increased Choice, Transparency and Security for their Personal Data, https://apps.fcc.gov/edocs_public/attachmatch/DOC-338679A1.pdf (Mar. 31, 2016); *See generally* Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. 23359 (proposed Apr. 20, 2016) (to be codified at 47 C.F.R. pt. 64), https://www.gpo.gov/fdsys/pkg/FR-2016-04-20/pdf/2016-08458.pdf [hereinafter NPRM].

[3] Vodafone Group PLC, Comment Letter on the Review of the Regulatory Framework for Electronic Communications Networks and Services, EUSURVEY, https://ec.europa.eu/eusurvey/publication/TelecomFrameworkReview2015 (search in "Please enter the name of your institution/organization/business" column for "Vodafone") (last visited Jan. 26, 2016).

[4] Deutsche Telekom AG, Comment Letter on the Review of the Regulatory Framework for Electronic Communications Networks and Services, EUSURVEY, https://ec.europa.eu/eusurvey/publication/TelecomFrameworkReview2015 (search in "Please enter the name of your institution/organization/business" column for "Deutsche Telekom") (last visited Jan. 26, 2016).

[5] Comcast Corporation, Comment Letter on Proposed Rule Protecting the Privacy of Customers of Broadband and Other Telecommunications Services (May 27, 2016), https://ecfsapi.fcc.gov/file/60002081094.pdf.

[6] AT&T Services Inc., Comment Letter on Proposed Rule Protecting the Privacy of Customers of Broadband and Other Telecommunications Services (May 27, 2016), https://ecfsapi.fcc.gov/file/60002080023.pdf.

[7] *See* 15 U.S.C. § 45 (2012).

[8] *See* Comcast Corporation, *supra* note 5; *see also* AT&T Services Inc., *supra* note 6.

[9] European Commission, *supra* note 1.

edge providers to the same rules,[10] the trope of parity takes the form of BIAS providers arguing that the EUC's proposed rules *should* be adopted because they will treat BIAS and edge providers the same, thereby creating a level playing field.

The question is: what "playing field" do BIAS providers want to have "leveled" by regulation? Usually, when one talks about "leveling the playing field" in a business sense, one is referring to the desire to avoid monopolies and sustain competition among companies in the same market. It does not make much sense to talk about a level playing field among companies in different markets. In a regulatory context, the market a company operates in matters because different markets have different regulatory structures, overseen by different entities, each with a specific scope of authority. For example, regarding enforcement of privacy regulations against BIAS and edge providers, the scope of the FTC's regulatory authority under section 5 of the FTC Act excludes "common carriers."[11] In contrast, under section 706 of the Telecommunications Act,[12] the FCC's scope of authority includes common carriers as long as they are classified as telecommunications services,[13] which is exactly how the FCC reclassified BIAS providers in its 2015 Open Internet Order.[14]

By definition, BIAS is "[a] mass market retail service . . . that provides the capability to transmit data to and receive data from all or substantially all Internet endpoints."[15] Without getting into market definition in the antitrust sense,[16] one can see that the BIAS market is easily distinguishable from the markets for applications and content, which are often characterized as edge markets. BIAS providers sometimes act as edge providers in the sense that they offer email services and smartphone applications. At the same time, edge providers sometimes enter into the BIAS market. For example, Google entered the

[10] *See generally* Commission Proposal for a Directive of the European Parliament and of the Council Establishing the European Electronic Communications Code, COM (2016) 590 final (Dec. 10, 2016), http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=comnat:COM_2016_0590_FIN.

[11] 15 U.S.C. § 45.

[12] 47 U.S.C. § 1302 (2012).

[13] *See* Verizon v. FCC, 740 F.3d 623, (D.C. Cir. 2014).

[14] In the Matter of Protecting and Promoting the Open Internet, 30 FCC Rcd. 5601 (2015) [hereinafter Open Internet Order] (upheld by United States Telecom Ass'n v. FCC, 825 F.3d 674, 690 (D.C. Cir. 2016)).

[15] Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, FTC REP. (Mar. 2012), at 15–16.

[16] *See* Darren S. Tucker & Hill B. Wellford, *Big Mistakes Regarding Big Data*, A.B.A.: THE ANTITRUST SOURCE 1, 5 (Dec. 2014), http://www.americanbar.org/content/dam/aba/publishing/antitrust_source/dec14_tucker_12_16f.authcheckdam.pdf ("The principal goal of market definition is to draw a line between products that substantially compete and those that do not."); *see also* Tampa Elec. Co. v. Nashville Coal Co., 365 U.S. 320, 328 (1961) (explaining that the relevant market is "the area of effective competition").

BIAS market with its Google Fiber project.[17]

However, the market for BIAS and the market for edge services are distinct. When a company is competing in either market, they compete with other players in the same market. Verizon may compete with Google Fiber in particular geographical markets as a BIAS provider. The playing field is level in the sense that Verizon and Google Fiber are playing by the same rules applicable to all BIAS providers, regardless of the specific rules established by the FCC. Similarly, when Verizon offers email services, it competes with other email service providers on a level field in the email services market. The whole discussion of a "level playing field" is a red herring; it is irrelevant to the idea of a regulatory parity in either the BIAS market or the various edge markets. There is actually a different market that is really at issue, the advertising market.

Online advertising has emerged as a core market of the Internet economy. BIAS providers and edge providers have the potential to compete on this playing field by using the incredible amounts of consumer data they can access to sell targeted advertising to third parties.[18] This is the playing field—or market—BIAS providers are really fighting about.[19]

Talking about regulatory symmetry between BIAS providers and edge providers is only relevant in this one market. Accordingly, this Note attempts to address that market directly and, in doing so, asks the normative question posed by the FCC's Broadband Privacy Rules:[20] should regulation in the online advertising context work to create a level playing field between all market participants, regardless of their technological differences, or should regulation work to level up consumer privacy in an era when the customer has become the product?[21] The first objective implies FTC-style regulation—a

[17] GOOGLE FIBER, https://fiber.google.com/about/ (last visited Jan. 26, 2017).

[18] *See infra* Section I.B.

[19] *E.g.*, Comcast Corporation, *supra* note 5, at 55 ("ISPs could compete with these incumbents [such as Google and Facebook] by offering advertisers the ability to reach consumers with targeted advertisements using much of the same data that online advertisers already use."). *See also* Deutsche Telekom AG, *supra* note 4 ("In a converging market environment where operating system providers, terminal equipment manufacturers, search engines, social platforms and traditional telecoms network operators compete for a higher share in the value chain, it is important and in the interest of the EU citizen that all play by the same rules and principles regarding transparency, openness and non-discrimination.").

[20] In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 31 FCC Rcd. 13911 (2016).

[21] The product being sold on the online advertising market is the consumer in the sense that the data collected about consumers allows companies to create detailed profiles about particular individuals, which are then sold to advertisers in order for them to target ads to the most likely customers. *See* Brett Frischmann & Evan Selinger, *Engineering Humans with Contracts*, 10 (Benjamin N. Cardozo Sch. of Law Faculty Research Paper No. 493, Sept. 15, 2016), http://ssrn.com/abstract=2834011 ("users are not really the consumers; rather, users are the product being consumed by all of the advertisers and other third-parties with whom Facebook and

technology neutral, ex post, standards-based approach. The second objective implies FCC-style regulation—a technology specific, ex ante, rulemaking approach. Either approach may make the online advertising playing field (un)even, but the real question is what the field of play should look like moving forward. The trope of parity, while appealing and egalitarian on its face, obscures and distracts from this question.

This Note argues for the FCC approach, and encourages state legislatures to pass laws affording consumers the same types of privacy protections set forth in the FCC's Broadband Privacy Order ("Broadband Privacy Order" or "Order").[22] On April 3, 2017, a Congressional Review Act measure reversing the FCC Broadband Privacy Rules was signed into law.[23] This measure also prevents the FCC from passing substantially similar broadband privacy rules in the future. While it is unlikely that FCC-style broadband privacy rules will be promulgated at the federal level in the short term, twenty-one states have already introduced bills to revive the consumer privacy protections that were repealed by Congress and the administration.[24]

I proceed in three parts. Part One provides some technical background to clarify the difference between BIAS and edge providers in terms of the consumer data they have access to and their markets. Part Two explores the differences between the FTC and FCC approaches to privacy regulation and compares some key provisions of the new FCC Broadband Privacy Order to provisions in the FTC's 2012 Privacy Report ("FTC Privacy Report" or "Report").[25] Part Three contains an analysis arguing in favor of the FCC approach because it will generate more positive externalities and be better for consumer privacy compared to the FTC approach. Finally, the Conclusion

Google have side-agreements."). *See, e.g.*, Mark Hachman, *The price of free: how Apple, Facebook, Microsoft and Google sell you to advertisers*, PC WORLD (Oct. 1, 2015, 3:00 AM), http://www.pcworld.com/article/2986988/privacy/the-price-of-free-how-apple-facebook-microsoft-and-googlesell-you-to-advertisers.html; Julia Angwin & Jeremy Singer-Vine, *Selling You on Facebook*, WALL ST. J. (Apr. 7, 2012), http://www.wsj.com/articles/SB10001424052702303302504577327744009046230. *See generally* Chris Jay Hoofnagle & Jan Whittington, *Free: Accounting for the Costs of the Internet's Most Popular Price*, 61 UCLA L. Rev. 606, 629–34 (2014) (discussing examples).

[22] In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 31 FCC Rcd. 13911 (2016).

[23] S.J. Res. 34, 115th Cong. (2017); Angelique Carson, *Trump signs bill killing FCC Rules: Is that really a big deal?*, IAPP PRIVACY ADVISOR (Apr. 4, 2017), https://iapp.org/news/a/trump-signs-bill-killing-fcc-rules-is-that-really-a-big-deal/.

[24] *See Privacy Legislation Related to Internet Service Providers*, NAT'L CONF. OF ST. LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-legislation-related-to-internet-service-providers.aspx (Aug. 4, 2017); Melanie Mason, *California bill aims to revive broadband privacy rules that were killed by Trump and Congress*, L.A. TIMES (June 19, 2017, 12:23 PM), http://www.latimes.com/politics/essential/la-pol-ca-essential-politics-updates-california-bill-aims-to-revive-1497898911-htmlstory.html.

[25] Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, FTC REP. (Mar. 2012), at 15–16 [hereinafter FTC Privacy Report].

summarizes the Note's main points.

I. TECHNICAL BACKGROUND

A. *Technological and Market Distinctions Between BIAS and Edge Providers*

To understand how the trope of parity obscures the underlying normative issues by failing to acknowledge the different markets occupied by BIAS and edge providers, we must first examine some Internet basics and the technological differences between the two kinds of companies. The Broadband Privacy Order defines BIAS as "[a] mass market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all Internet endpoints."[26] The "all Internet endpoints" part of the definition is what separates BIAS from edge providers. Unlike edge providers, which only have access to the information users share with them when using a particular service,[27] BIAS providers can track a customer's activity across the entire Internet and "thus have the ability to capture a breadth of data that an individual streaming video provider, search engine or even ecommerce site simply does not."[28] This difference is due to the layered architecture of the Internet.

The Internet has been conceptualized as having a five-layer architecture, starting with the physical infrastructure at the bottom (e.g., the physical cables that connect users to the Internet). Above that layer is the logical infrastructure (e.g., the standards and protocols that allow transmission of data across physical networks), then the applications layer (e.g., programs used by end users), then the content layer (e.g., information conveyed by and to end users). Finally, at the top, is the social layer (e.g., social relations among users).[29] A company operating at a lower level of the architecture can potentially view and manipulate transmissions to and from the higher layers but not vice versa.[30] As services that "transmit data to and receive data from all or substantially all Internet endpoints" and control the hardware that makes those transmissions possible, BIAS providers operate in the physical infrastructure layer.[31] By contrast, edge providers operate in the

[26] In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 31 FCC Rcd. 13911, 13925 n.69 (2016).
[27] NPRM, *supra* note 2, at 48.
[28] NPRM, *supra* note 2, at 3.
[29] PATRICIA L. BELLIA ET AL., CYBERLAW: PROBLEMS OF POLICY AND JURISPRUDENCE IN THE INFORMATION AGE, 21–23 (4th ed. 2011); BRETT M. FRISCHMANN, INFRASTRUCTURE: THE SOCIAL VALUE OF SHARED RESOURCES 317–57 (2012).
[30] BELLIA ET AL., *supra* note 29.
[31] In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 31 FCC Rcd. 13911, 13925 n.69 (2016).

applications and content layers.[32] Some supply applications, services, and programs like email, media players, browsers, and others supply content like video, music, and news.[33]

BIAS providers sometimes act as edge providers, for example, when they offer email services or a smartphone application.[34] Edge providers sometimes act as BIAS providers, for example, Google Fiber.[35] This does not provide a justification for regulating them in the same way. Regulatory authorities keep these distinctions in mind when creating and enforcing rules—they treat a company like Comcast as a BIAS provider when it is providing Internet access and as an edge provider when it is providing a smartphone application.[36] As such, this Note will focus on the main markets: BIAS providers operate in the market of "provid[ing] the capability to transmit data to and receive data from . . . all Internet endpoints"[37] and edge providers operate in the market of applications and content.[38]

Due to the technological and jurisdictional distinctions between the layers, companies at the same layer of the Internet architecture should all be similarly regulated. In their article, *The Layers Principle: Internet Architecture and the Law*, Lawrence B. Solum and Minn Chung argue that legal regulation of the Internet should respect "the integrity of layered internet architecture"[39] because this type of architecture has been fundamental to the explosion of innovation that has occurred on the Internet.[40] Regulations respect the Internet's layered architecture when they "attack a problem at a given layer with a regulation at that layer."[41] Solum and Chung justify this "layers principle"[42] by showing how, due to the nature of the Internet, regulations that violate the principle interfere with innocent uses of the Internet, fail to achieve their desired goal, and compromise the transparency of the Internet that has

[32] BELLIA ET AL., *supra* note 29.

[33] BELLIA ET AL., *supra* note 29.

[34] For example, Comcast offers customers a TV remote app. *Apps at home and on the go*, XFINITY, http://www.xfinity.com/apps.html (last visited Jan. 26, 2017).

[35] GOOGLE FIBER, *supra* note 17.

[36] *FCC Votes on Internet Service Regulation*, *in* HISTORIC DOCUMENTS OF 2015 76 (Heather Kerrigan, ed., 2016). ("[T]his Order concludes that the retail broadband Internet access service available today is best viewed as separately identifiable offers of (1) a broadband Internet access service that is a telecommunications service (including assorted functions and capabilities used for the management and control of that telecommunication service) and (2) various "add-on" applications, content, and services that generally are information services.").

[37] In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 31 FCC Rcd. 13911, 13925 n.69 (2016).

[38] BELLIA ET AL., *supra* note 29.

[39] Lawrence B. Solum & Minn Chung, *The Layers Principle: Internet Architecture and the Law*, 79 NOTRE DAME L. REV. 815, 815 (Apr. 1, 2004).

[40] *Id.* at 816.

[41] *Id.* at 818.

[42] *Id.* at 817.

enabled it to be a platform for low cost innovation.[43]

Internet "transparency" refers to the "end to end principle,"[44] which is a key feature of the Internet's architecture that keeps intelligence at the ends (i.e., in the applications layer and content layer) and keeps the network simple (in the sense that the network cannot discriminate between different packets of data).[45] By disabling the network's ability to differentiate a packet of data that is part of a website from a packet of data that is part of an email or MP3 file,[46] the original architects of the Internet created a decentralized platform where anyone can create an application on top of the TCP/IP protocol[47] and it will run on all computers running TCP/IP.[48] Without this feature, designers would need network administrators to reconfigure the network for each new application.[49] This means the rate of Internet innovation would not have been as great and the World Wide Web as we know it may have never developed.[50]

Solum and Chung show that there are rational justifications for regulations that treat companies differently based on the layer of the Internet architecture in which the company operates. A regulation that violates the layers principle by treating BIAS providers and edge providers the same, such as the FTC approach to consumer privacy, runs the risk of interfering with innocent uses of the Internet, failing to eliminate the targeted harm, and threatening the transparency of the Internet. For example, such a regulatory regime could result in BIAS providers developing technology that can inspect data packets in order to access the content of encrypted websites[51] and thereby create more detailed profiles of subscribers to be sold to advertisers. This eventuality would interfere with innocent uses of the Internet (e.g., by enabling BIAS to manipulate packets that are less useful for advertising purposes or that are traveling to places that advertisers do not care about), fail to eliminate the targeted harm (e.g., by being less protective of consumer privacy), and threaten the transparency of the Internet (e.g., by allowing the lower layer of the Internet to access or analyze content received from the upper layer). This example demonstrates the importance of

43 *Id.* at 819–20.

44 LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD 34 (2001).

45 Solum & Chung, *supra* note 39, at 829.

46 *Id.*

47 TCP/IP is the basic protocol of the internet that allows data transmission across physical networks. Layers are a key architectural feature of TCP/IP, and thus the internet. *Id.* at 822.

48 *Id.* at 846.

49 *Id.* at 834.

50 *Id.* at 847.

51 BIAS providers may also determine the destination of data packets. Aaron Rieke, et al., *What ISPs Can See: Clarifying the Technical Landscape of the Broadband Privacy Debate*, UPTURN (Mar. 2016), https://www.teamupturn.com/reports/2016/what-isps-can-see.

adhering to the layers principle in the context of answering the underlying normative question of how regulation should work in the online advertising context. Disregarding the layers principle is one of the ways in which the trope of parity is a distraction from this normative question.

B. *What the Distinctions Mean for Consumer Privacy*

Now that we have clarified the markets and Internet architecture layers in which BIAS and edge providers operate, we turn to a discussion of how these differences affect each player's access to consumer information.

First, when a website is unencrypted, a BIAS provider can see the detailed URL and the content of the web page requested by the user.[52] While edge providers may have access to some additional content when, for example, a customer uses their browser, social media network, or email platform, BIAS providers can track a customer's activity across the entire Internet and "thus have the ability to capture a breadth of data that an individual streaming video provider, search engine or even ecommerce site simply does not."[53]

Second, when online traffic is encrypted, Comcast and AT&T claim they can only see the top-level domain (for example, "www.nytimes.com") visited by a user as opposed to a detailed URL.[54] While Comcast and AT&T claim that "by the end of 2016 over 70% of all Internet traffic . . . will be encrypted,"[55] this figure is misleading because it is not referring to 70% of all websites but 70% of "Internet traffic"—i.e. the volume of bandwidth used.[56] For example, "Netflix . . . itself accounts for about 35% of all downstream Internet traffic in North America" because streaming videos use such a high volume of bandwidth.[57] However, "sensitivity doesn't depend on volume."[58] Streaming *The Amazing Spider-Man* may use 40GB of traffic, but it could potentially reveal much less sensitive data about a user compared to a visit to the WebMD page for "pancreatic cancer," which may use only 2MB of traffic.[59] Furthermore, "more than 85% of sites in each of the three areas [health, news, shopping] — still do not fully support encrypted browsing by default."[60]

---

[52] *Id.*
[53] NPRM, *supra* note 2, at 3.
[54] *See* Comcast Corporation, *supra* note 5, at 28; *see also* AT&T Services Inc., *supra* note 6, at 11, 14, 20.
[55] Comcast Corporation, *supra* note 5, at 5.
[56] Rieke et al., *supra* note 51, at 3.
[57] *Id.*
[58] *Id.*
[59] *Id.*
[60] *Id.* at 1.

Third, while Comcast and AT&T claim that BIAS providers obtain more fractured information about a user because she uses multiple BIAS providers in a given day,[61] a user still typically has a long-term relationship with her mobile and home BIAS provider, allowing BIAS providers to collect metadata about her activity over time.[62] Even when a website is encrypted, a BIAS provider can still almost always see the domain name a customer visits.[63] One can imagine how even a short sequence of visited domains can be sensitive, for example, abortionfacts.com, plannedparenthood.org, dcabortionfund.org, maps.google.com.[64] "Over a longer period of time, metadata can paint a revealing picture about a subscriber's habits and interests."[65]

Fourth, although Comcast and AT&T claim that only edge providers can access the content of encrypted websites (for example, by tracking scrolling through pages or mouse clicks),[66] research shows that BIAS providers can also access a lot of the content of encrypted traffic.[67] "By examining the features of the traffic — like the size, timing and destination of the encrypted packets — it is possible to uniquely identify certain web page visits or otherwise reveal information about what those packets likely contain."[68] Moreover, BIAS providers have other tools at their disposal that can potentially help them to access encrypted content, such as website fingerprinting, which examines the unique features of a website (including amount of content, third-party resources, and location) to uniquely identify the specific page.[69]

Given that BIAS providers have the potential to collect, use, and sell as much or nearly as much consumer data as edge providers and that doing so has huge revenue-generating potential,[70] it is clear that the playing field BIAS providers want leveled is the online advertising market. However, the trope of parity here is distracting from the fact that, even if BIAS and edge providers have the *potential* to compete in the same market, they still *currently* exist in two different layers of the Internet architecture and, thus, two different markets. The only

61 *See* Comcast Corporation, *supra* note 5, at 27 ("[A]ny one ISP is the conduit for only a fraction of a typical user's online activity . . . because consumers increasingly use a number of devices across multiple ISPs for Internet Access"); *see also* AT&T Services Inc., *supra* note 6, at 26–27.

62 Rieke et al., *supra* note 51, at 1.

63 *Id.*

64 *Id.*

65 *Id.* at 7.

66 Comcast Corporation, *supra* note 5, at 30; AT&T Services Inc., *supra* note 6, at 11–16.

67 Rieke et al., *supra* note 51.

68 *Id.*

69 *Id.*

70 *See* Comcast Corporation, *supra* note 5, at 53 ("[I]n 2014, Facebook's digital display ad revenues accounted for just under one-quarter of the US total market and Google's digital display ad revenues accounted for about one-fifth of total market revenues.").

generally-applicable federal regulatory scheme available to regulate the privacy practices of companies in two different markets is the FTC's authority under section 5 of the FTC Act to police "[u]nfair methods of competition . . . and unfair or deceptive acts or practices."[71]

Therefore, by arguing for symmetrical regulation across markets, the BIAS providers' trope of parity relies on the FTC approach to privacy regulation and thus obscures the possibility of the FCC approach. The real underlying normative issue is whether we think the goal of federal Internet regulation should be leveling the playing field in the online advertising market (which is better achieved through the FTC approach) or whether it should be optimizing consumer privacy (which is better achieved through the FCC approach).[72]

II. COMPARISON OF THE FTC AND FCC APPROACH TO PRIVACY REGULATION

A. *Scope of Authority*

While the scope of the FTC's privacy regulation enforcement authority arguably encompasses both BIAS and edge providers, the scope of the FCC's privacy regulation enforcement authority excludes edge providers.

The FTC gets its enforcement authority from section 5 of the FTC Act, which states "[t]he Commission is hereby empowered and directed to prevent persons, partnerships, or corporations . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."[73] The entities that are excluded from the FTC's jurisdiction under this section are "banks, savings and loan institutions . . . Federal credit unions . . . common carriers . . . air carriers and foreign air carriers."[74] However, the Communications Act of 1934 states that "[a] telecommunications carrier shall be treated as a common carrier under this chapter only to the extent that it is engaged in providing telecommunications services . . . ."[75] Hence, the FTC and FCC have agreed that the FTC has authority to regulate the non-common carrier activities of common carriers, such as unfair or deceptive advertising practices.[76]

---

71 15 U.S.C. § 45(a)(1) (2012).

72 *See infra* Section II.C.iii.

73 15 U.S.C. § 45(a)(2) (2012).

74 *Id.*

75 47 U.S.C. § 153(51) (2012).

76 Federal Trade Comm'n, FCC-FTC Consumer Protection Memorandum of Understanding (Nov. 16, 2015), https://www.ftc.gov/system/files/documents/cooperation_agreements/151116ftcfcc-mou.pdf. This interpretation of the FTC's authority was called into question by the recent Ninth Circuit case. FTC v. AT&T Mobility LLC, 835 F.3d 993 (9th Cir. 2016) (holding that the common carrier exemption in the FTC Act is based on an entity's status as a common carrier rather its activity). However, the same court released an order in May 2017 stating that the "three-

The FCC, on the other hand, grounds its authority to make privacy rules in section 222 of the Communications Act of 1934, which states, "[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."[77] The FCC points to other possible statutory support for its privacy authority, including sections 201 and 202 of the Communications Act ("which prohibit telecommunications carriers from engaging in unjust, unreasonable, or unreasonably discriminatory practices"), section 706 of the Telecommunications Act of 1996 ("which requires the Commission to use regulating methods that remove barriers to infrastructure investment"), and section 705 of the Communications Act, ("which restricts the unauthorized publication or use of communications").[78] However, compared to section 222, all of the other provisions limit the scope of the FCC's authority to regulate telecommunications services and common carriers.[79]

Although edge providers would not fall under the FCC's authority because they are considered neither telecommunications services nor common carriers, BIAS providers do fall within the FCC's scope of authority because they were reclassified as telecommunications services in the FCC's 2015 Open Internet Order.[80] After the FCC's authority was challenged in federal court, the District of Columbia Circuit Court of Appeals held that the FCC acted reasonably by reclassifying broadband service as a telecommunications service.[81] Acting on this authority, the FCC subsequently voted to adopt many important aspects of the NPRM's proposed rules in its final Broadband Privacy Order.[82] Given these differences in scope of authority, it is clear how the trope of parity, which argues for symmetrical regulations for companies in different markets, simply assumes a FTC-style approach without considering the possibility of a FCC-style, market-specific approach.

B. *Enforcement Mechanisms*

Although the trope of parity presupposes a FTC-style approach to privacy regulation for BIAS providers, there is no a priori reason for

judge panel disposition in this case shall not be cited as precedent" and granted a rehearing en banc. FTC v. AT&T Mobility LLC, No. 15-16585, 2017 WL 1856836 (9th Cir. May 9, 2017). As of the writing of this paper, a final decision has not yet been rendered.

77 47 U.S.C. § 222(a) (2012).

78 NPRM, *supra* note 2, at 94.

79 *Id.*

80 Open Internet Order, *supra* note 14, at 20.

81 United States Telecom Ass'n v. FCC, 825 F.3d 674, 689 (D.C. Cir. 2016).

82 Cecilia Kang, *Broadband Providers Will Need Permission to Collect Private Data*, N.Y. TIMES (Oct. 27, 2016), https://nytimes.com/2016/10/28/technology/fcc-tightens-privacy-rules-for-broadband-providers.html. *See generally* In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 31 FCC Rcd. 13911 (2016).

taking that approach over the FCC-style approach. In fact, in November 2014, President Obama urged the FCC to classify broadband providers as common carriers and invoke its powers under Title II of the Communications Act,[83] suggesting the Obama administration's support for the FCC taking on a broader authority over broadband providers. However, we will look at some arguments in favor of each approach.

In her essay, *The FCC's Knowledge Problem: How to Protect Consumers Online*,[84] FTC Commissioner Maureen K. Ohlhausen argues that the FCC's approach to making ex ante general rules has a difficult time keeping up with technological innovation. Since the FCC will need to make predictions about the future in order to create ex ante rules, Ohlhausen claims that they, as centralized decision makers, have a hard time understanding fast-paced advances in the technology sector as they develop.[85] Ohlhausen also criticizes the FCC's technology-specific approach, saying that a framework that "distinguishes among services based on their physical platform, business model, and geographic characteristics" is "increasingly irrelevant" in a world where edge companies provide services that are essentially substitutes for telecommunications services.[86] Ohlhausen worries that the FCC's "rules are constantly falling out of sync with technological change—and, worse, forcing business and technological innovation to slow down to stay compliant."[87]

Furthermore, Ohlhausen supports the FTC's enforcement-centric rather than rulemaking-centric approach because it focuses on actual harms rather than future predicted harms.[88] She claims that the fact-specific nature of FTC enforcement means it is less vulnerable to the knowledge problem because it can adapt more quickly to technological advances, and a centralized agency does not need to know about an entire industry but rather just the parties in front of it.[89] Lastly, Ohlhausen raises concerns about how the FCC approach may reduce the FTC's authority because its classification of BIAS providers as common carriers places those companies outside of the FTC's jurisdiction.[90]

On the other hand, some academics have criticized the FTC's enforcement-centric approach because it does not provide companies with sufficient notice, and regulated parties do not understand the rules

[83] Press Release, The White House, Net Neutrality: President Obama's Plan for a Free and Open Internet (Nov. 10, 2014), https://obamawhitehouse.archives.gov/node/323681.
[84] Hon. Maureen K. Ohlhausen, *The FCC's Knowledge Problem: How to Protect Consumers Online*, 67 FED. COMM. L.J. 203 (2015).
[85] *Id.* at 206–07.
[86] *Id.* at 208.
[87] *Id.* at 209–10.
[88] *Id.* at 212.
[89] *Id.* at 213.
[90] *Id.* at 229–30.

they are subject to.[91] For one, under the FTC Act, the FTC purports to have authority over "every business in the country, no matter how large, how sophisticated, or otherwise regulated."[92] However, the United States Supreme Court has expressed skepticism over agency authority to regulate such a large portion of the American economy.[93]

Furthermore, recent court developments, specifically the only two cases out of fifty data security enforcement actions that did not settle with the FTC,[94] suggest the FTC's efforts do not provide sufficient notice for due process.[95] First, in *LabMD, Inc. v. FTC*, "the Judge rejected the FTC's claims against LabMD, finding . . . that the FTC's theory of the case—under which the fact of a data breach demonstrates a likelihood of consumer harm—'would not provide the required constitutional notice of what is prohibited.'"[96] Second, in *FTC v. Wyndham Worldwide Corp.*, the Third Circuit Court of Appeals affirmed the FTC's enforcement authority but expressed concern that the FTC's case by case approach does not provide sufficient notice where the FTC has not "informed the public that it needs to look at complaints and consent decrees for guidance."[97] Taken together, these cases demonstrate legitimate concern over the "common law" approach taken by the FTC in developing a body of data security law[98] and suggest that enforcement through Article III courts rather than FTC adjudications would result in more consistent constructions of the law.[99]

By talking about a level playing field between companies in different markets, the trope of parity assumes a FTC-style approach to privacy regulation in the online advertising market and thus obscures the fact that there is a normative choice between the FTC approach and the FCC approach.

---

91 Justin (Gus) Hurwitz, *Data Security and the FTC's UnCommon Law*, 101 IOWA L. REV. 955 (2016).

92 *Id.* at 959.

93 Util. Air Regulatory Grp. v. EPA, 134 S. Ct. 2427, 2444 (2014) ("When an agency claims to discover in a long-extant statute an unheralded power to regulate 'a significant portion of the American economy,' we typically greet its announcement with a measure of skepticism." (quoting FDA v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 159 (2000)).

94 *See* LabMD, Inc. v. FTC, 776 F.3d 1275 (11th Cir. 2015); *see also* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D.N.J. 2014).

95 Hurwitz, *supra* note 91, at 959.

96 *Id.* at 979 (quoting In the Matter of LabMD, Inc. Initial Decision, F.T.C. No. 9357, at 87 (Nov. 13, 2015)).

97 FTC v. Wyndham Worldwide Corp., 799 F.3d 236, n.23 (3d Cir. 2015); Hurwitz, *supra* note 91, at 979.

98 Hurwitz, *supra* note 91, at 959–60.

99 *Id.* at 967.

C. *Key Provisions of the FCC Broadband Privacy Order Compared to Provisions of the FTC 2012 Privacy Report*

1. Key Definitions and Provisions of the FCC Broadband Privacy Order

First, it is important to clarify the Broadband Privacy Order's use of some important terms. The Order defines BIAS as "[a] mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all Internet endpoints."[100] "Customer" in the Order does not just mean "current customer" as in section 222 of the Communications Act of 1934 but also includes former customers and applicants.[101]

The Order defines information that would be protected under section 222 as "customer proprietary information" ("customer PI"), and it includes in this definition customer proprietary network information ("CPNI"), personally identifiable information ("PII"), and content of communications.[102] The Order adopts the statutory definition of CPNI under section 222(h)(1): "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[103] PII is defined as "any information that is linked or reasonably linkable to an individual or device."[104] "Information is 'linked' or 'reasonably linkable' to an individual if it can be used on its own, in context, or in combination to identify an individual or device, or to logically associate with other information about a specific individual or device."[105] A BIAS customer's name, postal address, and telephone number are also considered PII.[106] Content of communications is defined as "any part of the substance, purport, or meaning of a communication or any other part of a communication that is highly suggestive of the substance, purpose, or meaning of a communication."[107]

Additionally, the Order sets out a non-exhaustive list of eight

---

100 In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 31 FCC Rcd. 13911, 13925 n.69 (2016).

101 *Id.* at 13926; *see also* 47 C.F.R. § 64.2002(e) (2016).

102 In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 31 FCC Rcd. 13911, 13925 (2016). *See also* 47 C.F.R. § 64.2002(f) (2016).

103 In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 31 FCC Rcd. 13911, 13914 n.2 (2016).

104 In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 31 FCC Rcd. 13911, 13944 (2016); 47 C.F.R. § 64.2002(m) (2016).

105 In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 31 FCC Rcd. 13911, 13944 (2016).

106 *Id.* at 13948–49.

107 *Id.* at 13950.

categories of information it considers "sensitive customer proprietary information" ("sensitive customer PI"), including (1) financial information, (2) health information, (3) information pertaining to children, (4) Social Security Numbers, (5) precise geo-location information, (6) content of communications, (7) call detail information, and (8) web browsing history, application usage history, and the functional equivalents of either.[108]

"Opt-out approval" essentially means that a customer is deemed to have consented to the use of her information unless she takes affirmative steps to opt out.[109] "Opt-in approval" means that a customer is not deemed to have consented to the use of her information unless she takes affirmative steps to opt in.[110]

The Order recognizes section 222's exception for "aggregate customer proprietary information," which is defined as "collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed."[111] However, in order for information to be considered "de-identified" (and thus not subject to the rules), it must first pass a three-part test.[112] Specifically, the carrier must:

> (1) determin[e] that the information is not reasonably linkable to an individual or device; (2) publicly commi[t] to maintain and use the data in a nonindividually identifiable fashion and to not attempt to re-identify the data; and (3) contractually prohibi[t] any entity to which it discloses or permits access to the de-identified data from attempting to re-identify the data.[113]

Lastly, the Order defines a breach of security as "any instance in which a person, without authorization or exceeding authorization, has gained access to, used, or disclosed customer proprietary information."[114] This definition is crucially different from the definition of breach in section 222 because "it does not include an intent element and it covers all customer PI, not just CPNI."[115]

---

[108] *Id.* at 13914; 47 C.F.R. § 64.2002(n) (2016).

[109] In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 31 FCC Rcd. 13911, 13991 (2016); 47 C.F.R. § 64.2002(k) (2016).

[110] 47 C.F.R. § 64.2002(j) (2016).

[111] In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 31 FCC Rcd. 13911, 13954 n.294 (2016); 47 U.S.C. § 222(h)(2) (2012).

[112] In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 31 FCC Rcd. 13911, 13952, 13954 (2016).

[113] *Id.* at 13952.

[114] *Id.* at 14019, 14024; 47 C.F.R. § 64.2002(c) (2016).

[115] NPRM, *supra* note 2, at 27; In the Matter of Protecting the Privacy of Customers of

The key provisions of the Order are categorized under the three core privacy principals—transparency, choice, and security.[116] In terms of transparency, the Order requires BIAS providers to provide customers with clear and accurate notice of their privacy policies. This notice is required both at the point of sale and through BIAS providers' websites, apps, and any functional equivalents in a way that is "persistently available and easily accessible."[117] Such notice must specify:

> 1) [t]he types of customer PI that the BIAS provider collects by virtue of its provision of service and how the carrier uses that information;
>
> 2) [u]nder what circumstances it discloses or permits access to each type of customer PI that it collects, including the categories of entities to which the carrier discloses or permits access to customer PI and the purposes for which the customer PI will be used by each category of entities; and
>
> 3) How customers can exercise their privacy choices.[118]

As for choice, the Order adopts a tiered approach based on the sensitivity of information, consumer expectations, and context, and outlines three categories of approval.[119] The order requires carriers to obtain:

> 1) customers' opt-in approval for use and sharing of sensitive customer PI (and for material retroactive changes to carriers' privacy policies)
>
> 2) customers' opt-out approval for the use and sharing of non-sensitive customer PI.
>
> 3) [no customer consent] to use and share customer data in order to provide broadband services . . . and for certain other purposes.[120]

BIAS providers also must "provide customers with easy access to a choice mechanism that is simple, easy-to-use, clearly and conspicuously disclosed, persistently available, and made available at no additional cost to the customer."[121]

Broadband and Other Telecommunications Services, 31 FCC Rcd. 13911, 14024 (2016).

[116] In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 31 FCC Rcd. 13911, 13914–15 (2016).

[117] *Id.*

[118] *Id.* at 13962.

[119] *Id.* at 13914.

[120] *Id.* These "certain other purposes" are limited to "Congressionally-directed exceptions to customer approval rights," for example, "to provide the underlying telecommunications service" and "to bill and collect payment for that service." *Id.* at 13977.

[121] *Id.*

In the interest of security, the Order "requires that every BIAS provider and other telecommunications carrier take reasonable measures to protect customer PI from unauthorized use, disclosure, or access" and, additionally, it sets forth data breach notification requirements.[122] To be in compliance with this rule, a BIAS provider must consider the following four factors when implementing data security procedures: "the nature and scope of its activities; the sensitivity of the data it collects; its size; and technical feasibility."[123] No factor by itself is determinative and these protections are required for both sensitive and non-sensitive customer PI.[124]

Regarding breach notification, the Order requires "BIAS providers and other telecommunications carriers to notify affected customers, the Commission, and the FBI and Secret Service unless the carrier is able to reasonably determine that a data breach poses no reasonable risk of harm to the affected customers."[125] Importantly, the Order construes "harm" broadly to encompass "financial, physical, and emotional harm,"[126] and its harm-based notification trigger applies to breaches of data in an encrypted form. Finally, the Order sets out a timeline for BIAS providers to follow when notifying customers and government authorities about a data breach.[127] Most importantly, BIAS providers must "provide notice to affected customers without unreasonable delay, but within no more than 30 days."[128]

2. Key Definitions and Provisions of the FTC Privacy Report

First, it is important to understand that the 2012 FTC Privacy Report[129] only recommends "best practices" as opposed to mandating legally enforceable rules.[130] As mentioned earlier, the FTC's enforcement authority primarily comes from Section 5 of the FTC Act, which, while empowering the Commission to prevent "unfair or deceptive acts or practices in or affecting commerce," also limits that power to situations where the unfair act or practice "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by

122 *Id.* at 14007.
123 *Id.* at 14009.
124 *Id.* at 14010.
125 *Id.* at 13915.
126 *Id.* at 14022.
127 *Id.* at 13915.
128 *Id.*
129 FTC Privacy Report, *supra* note 25.
130 *Id.* at iii (The final framework is intended to articulate best practices for companies that collect and use consumer data . . . To the extent the framework goes beyond existing legal requirements, the framework is not intended to serve as a template for law enforcement actions or regulations under laws currently enforced by the FTC.).

countervailing benefits to consumers or to competition."[131] This "substantial injury" requirement for unfair acts or practices is the first difference between the FCC and FTC approach that demonstrates how the FTC approach is less protective of consumer privacy. Jurisprudence has shown that it is difficult, in the context of unauthorized dissemination of consumer data, to show actual injury.[132] Furthermore, in a world where new technologies are regularly being developed to derive more information from aggregate data sets, it might be difficult to fully appreciate the scope of such an injury because it is impossible to know the future risks such data may pose once it gets out. With this landscape in mind, let us consider the substantive recommendations of the FTC Privacy Report.

The scope of FTC Privacy Report framework encompasses "all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device . . . ."[133] Instead of defining "reasonably linked," the report sets out three protections a company must implement for their data to be not "reasonably linkable to a particular consumer or device:"[134]

> 1. The company must take reasonable measures to ensure that the data is de-identified.
>
> 2. The company must publicly commit to maintain and use the data in a de-identified fashion, and not to attempt to re-identify the data.
>
> 3. If a company makes such de-identified data available to other companies—whether service providers or other third parties—it should contractually prohibit such entities from attempting to re-identify the data[135]

The FTC Privacy Report organizes its recommendations under three core principles—privacy by design, simplified consumer choice, and transparency.[136]

Regarding privacy by design, the FTC Privacy Report recommends that companies limit their data collection to "that which is consistent with the context of a particular transaction or the consumer's relationship with the business."[137] Further, "companies should implement reasonable restrictions on the retention of data and should

131 15 U.S.C. § 45(a)(1); § 45(n) (2012).
132 *See In re* iPhone Application Litigation, 6 F.Supp.3d 1004 (N.D.Cal. 2013) (granting summary judgment to Apple on the grounds that consumer plaintiffs, who brought action under the FTC-style California Consumer Legal Remedies Act, could not prove injury on a claim that Apple collected geolocation information even when location services setting was turned off).
133 FTC Privacy Report, *supra* note 25, at iv.
134 *Id.* at 20–21.
135 *Id.* at 21.
136 *Id.* at vii-viii.
137 *Id.* at 27.

dispose of it once the data has outlived the legitimate purpose for which it was collected."[138] In addition, the Report says companies should "incorporate substantive privacy protections into their practices,"[139] including data security, data accuracy, and data management procedures throughout the life cycle of their products and services.[140]

In terms of simplified consumer choice, the Report outlines five categories of data practices that do not require consumer choice "because they involve data collection and use that is either obvious from the context of the transaction or sufficiently accepted or necessary for public policy reasons:

1. Product and service fulfillment

2. Internal operations

3. Fraud prevention

4. Legal compliance and public purpose; and

5. First-party marketing.[141]

The Report provides examples of some practices that do not require consumer choice, such as cross-channel marketing[142] and data enhancement.[143]

On the other hand, practices that do require providing customers with meaningful choice include third-party tracking of customers across other parties' websites[144] and sharing or selling data to third-parties,[145] which includes affiliates unless the affiliate relationship is clear to consumers.[146] The Report clarifies that providing consumer choice should be done through a "consumer choice mechanism," but it leaves the details of such a mechanism up to the companies themselves.[147]

---

138 *Id.* at 28.
139 *Id.* at vii.
140 *Id.* at 32.
141 *Id.* at 36.
142 *Id.* at 42 ("*e.g.,* where a consumer makes an in-store purchase and receives a coupon—not at the register, but in the mail or through a text message").
143 *See id.* (Data enhancement is when "a company appends data obtained from third-party sources to information it collects directly from consumers").
144 FTC Privacy Report, *supra* note 25, at 41; *see also id.* at n.194 ("For example, a consumer visits an online sporting goods retailer, looks at but does not purchase running shoes, and then visits a different website to read about the local weather forecast. A first party engages in retargeting if it delivers an ad for running shoes to the consumer on the third-party weather site.").
145 FTC Privacy Report, *supra* note 25, at 39 ("[I]f the dealership sells the consumer's personal information to a third-party data broker . . . the practice would not be consistent with the car purchase transaction or the consumer's relationship with the dealership.").
146 *Id.* at 41.
147 *Id.* at 50 ("The Commission calls on industry to use the same type of creativity industry relies on to develop effective marketing campaigns and user interfaces for consumer choice mechanisms.").

Furthermore, the Report says companies may seek "affirmative express consent"[148] from consumers before collecting sensitive data for any marketing, whether first or third-party.[149] "Sensitive data" is defined as "information about children, financial and health information, Social Security numbers, and precise geolocation data."[150] The FTC also recommends seeking affirmative express consent "before making material retroactive changes to privacy representations"[151] and before "using consumer data in a materially different manner than claimed when the data was collected."[152]

Lastly, the Report seeks to further the goal of transparency by recommending that companies "present choices to consumers in a prominent, relevant, and easily accessible place at a time and in a context when it matters to them."[153] This means that industry should "make privacy statements clearer, shorter, and more standardized; give consumers reasonable access to their data; and undertake consumer education efforts to improve consumers' understanding of how companies collect, use, and share their data."[154]

3. Comparison of the FCC Broadband Privacy Order and the FTC Privacy Report

Looking at the substantive provisions of the Broadband Privacy Order and the FTC Privacy Report, one can see how the Order's regulation-based approach is more protective of consumer privacy than the Privacy Report's competition-based approach.

First, the FTC Privacy Report does not make any rules but merely sets out recommendations for best practices, exemplifying the FTC approach of first relying on advice and cooperation from industry and then turning to penalties only when these methods fail.[155] As we previously discussed, such ex post, case-by-case regulation may not provide the appropriate level of consumer protection because it does not provide sufficient notice, and regulated parties do not fully understand the rules they are subject to.[156] Furthermore, the FTC's common law approach requires the Commission to start from a blank slate in each adjudication and argue why a given act is prohibited by section 5 of the FTC Act, rather than learn from its experience and prohibit behavior

148 *Id.* at 57, n.274 (Similar to the opt-in consent required by some FCC provisions, "affirmative express consent" means "presenting [customers] with a clear and prominent disclosure, followed by the ability to opt in to the practice being described").
149 *Id.* at 47, 58.
150 *Id.* at 59.
151 *Id.* at 57.
152 *Id.* at 60.
153 *Id.*
154 *Id.*
155 WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW 212 (2016).
156 *See supra* Section II.B.

routinely shown to be unfair or deceptive.[157] What is more troubling is that, faced with the threat of such burdensome litigation but with less notice and understanding of the rules companies may be subject to, the FTC approach may have the effect of discouraging investment in small start-ups, thus harming innovation.[158] In summary, by putting more trust in companies to regulate themselves, the FTC approach is competition-focused in that it leaves more of the determination of the appropriate level of consumer privacy protection up to market forces rather than establishing a baseline set of privacy rules.

Second, the FTC Privacy Report's substantive provisions are themselves less protective of consumer privacy than those in the Broadband Privacy Order. For example, the Report recommends companies provide an undefined "consumer choice mechanism"[159] in order to provide customers with a meaningful choice before (1) sharing non-sensitive consumer data with third parties[160] (including affiliates where the affiliate relationship is not clear to consumers)[161] and (2) third-party tracking of consumers across other parties' websites.[162] By contrast, the Order specifically requires opt-out consent before using and sharing non-sensitive customer PI[163] and opt-in consent for use and sharing of sensitive customer PI.[164] While the Report recommends opt-in consent in the context of particularly sensitive data, the Order provides heightened protection for sensitive customer information by expanding the Report's definition of "sensitive data"[165] to include "content of communications, call detail information, web browsing history, application usage history, and the functional equivalents of either web browsing history or application usage history."[166]

Additionally, in regard to transparency, the Report merely recommends that industry should "make privacy statements clearer, shorter, and more standardized . . . and undertake consumer education efforts to improve consumers' understanding of how companies collect,

157 Public Knowledge and Common Cause, Comment Letter on In the Matter of Open Internet Remand (Mar. 21, 2014), *found at* https://www.publicknowledge.org/assets/uploads/documents/Public_Knowledge_Common_Cause_Open_Internet_706_Public_Notice_Comments.pdf at 19.

158 *Id.* at 20.

159 *FTC Privacy Report*, *supra* note 25 at 50. The Report leaves it up to industry to decide what "mechanism" to choose—opt-in or opt-out.

160 *Id.* at 39.

161 *Id.* at 41.

162 *Id.*

163 In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 31 FCC Rcd. 13911, 13915 (2016).

164 *Id.*

165 *FTC Privacy Report*, *supra* note 25 at 59 ("[I]nformation about children, financial and health information, Social Security numbers, and precise geolocation data.").

166 In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 31 FCC Rcd. 13911, 13914 (2016).

use, and share their data."[167] The Order specifically requires BIAS providers privacy policies to "accurately specify and describe:[168]

> 1) The types of customer PI that the carrier collects by virtue of its provision of service, and how the carrier uses that information;
>
> 2) Under what circumstances a carrier discloses or permits access to each type of customer PI that it collects, including the categories of entities to which the carrier discloses or permits access to customer PI and the purposes for which the customer PI will be used by each category of entities; and
>
> 3) How customers can exercise their privacy choices.[169]

Lastly, unlike the Order,[170] the Report does not set forth any specific data breach notification requirements but instead calls on Congress to do so.[171]

The differences between the substantive provisions of the Order and the Report reflect how, compared to the FCC, the FTC takes more of a "light touch" approach to regulation. The FTC entrusts more to market forces to determine the appropriate balance between the benefits of consumer privacy protection and the burdens on companies to provide those protections.

III. ANALYSIS

Let us return to the trope of parity, the common regulatory-parity argument that rules must apply the same to all actors in order to level the playing field. This argument is a distraction from the real underlying normative issue of how we should go about regulation of the market for online advertising, in part because it begs the question: if a level playing field is the goal, why need regulation at all—why not just rely on antitrust law? Those concerned about a BIAS provider's use and sharing of their information can vote with their feet and select providers based on their privacy policies.[172] However, the market for Internet access has been conventionally viewed as insufficient to effectively monitor itself through private regulation because alternative BIAS providers are not always available[173] and, due to an inequality in bargaining power, most

---

167 FTC Privacy Report, *supra* note 25 at 60.

168 In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 31 FCC Rcd. 13911, 13962 (2016).

169 *Id.*

170 *Id.* at 97.

171 FTC Privacy Report, *supra* note 25 at 26.

172 BELLIA ET AL., *supra* note 29, at 215.

173 "74.7% percentage of homes only have 1 choice for broadband at 25 mbps down/3 mbps up, 82.4% only have 1 choice at 50 down/3 up." Tom Wheeler, Chairman, Fed Commc'n Comm'n, The Facts and Future of Broadband Competition, Prepared Remarks at 1776 Headquarters, Washington, D.C. (Sept. 4, 2014), *in* DAILY DIGEST at 1, 2

customers are unaware of the regulatory terms to which they have "consented" by signing up for service.[174]

As providers of Internet infrastructure, BIAS companies are in a market "affected with the public interest,"[175] which is the type of market where common carrier-style obligations have historically arisen.[176] In addition to concerns about monopolistic supply, common carrier-type regulation can be justified to deal with a variety of public interest concerns.[177] For example, in the context of net neutrality, intervention in the market for BIAS was justified by public interest concerns because "[n]ondiscriminatory access to infrastructure may be essential to public participation in a range of socially valuable activities, including economic, cultural, political, and other social systems."[178] Similarly, the FCC's approach to regulation of broadband privacy can be justified by public interest concerns because increasing customer confidence in BIAS providers' handling of their confidential information may be essential to the public's ability to fully participate in "a range of socially valuable activities" on the Internet.[179] In other words, the normative goal should not be a level playing field in the online advertising market, it should be consumer privacy that enables consumers to go online without worrying that a company has access to their information in ways they are not aware.

A. *The Goal of Online Advertising Regulation Should Not Be a Level Playing Field*

We have already seen, from the net neutrality debate, how leaving regulation of Internet transactions up to market forces can result in social harms and lead to large negative externalities. For example, Professor Tim Wu provides an example of such a scenario, where he describes a hypothetical deal between a major highway and Ford Motors to provide a special rush hour lane exclusively for Ford customers.[180] Wu claims that such an arrangement would change how car companies compete because "[t]he race is no longer to build a better car, but to fight for a better deal with the highway company," thus creating a market where "it would no longer be the best car tha[t] . . . wins, but the

https://apps.fcc.gov/edocs_public/attachmatch/DOC-329161A1.pdf.

174 BELLIA ET AL., *supra* note 29, at 215.

175 Walter H. Hamilton, *Affectation with Public Interest*, 39 YALE L.J. 1089, 1100–01 (June 1930); *see also* Munn v. Illinois, 94 U.S. 113, 126 (1876).

176 BELLIA ET AL., *supra* note 29, at 220.

177 Frischmann, *supra* note 29.

178 *Id.*

179 *Id.*

180 *See* Network Neutrality: Competition, Innovation, and Nondiscriminatory Access: Hearing Before the Task Force on Telecom and Antitrust of the H. Comm. on the Judiciary, 109th Cong. 49–50 (2006) (testimony of Tim Wu, Professor, Columbia Law School).

one that signs the best deals and slows down their competitors."[181] This would be bad for consumers not only because cars would not improve but also because a market that is no longer meritocratic becomes less efficient, allowing incumbents to use their position to make threats, extract payments, and choose favorites.[182]

The same dangers of choosing market forces over agency regulation exist in the context of regulating broadband privacy. Yes, BIAS providers stand to make a lot of money if they were allowed to compete in the online advertising market, but such schemes would discourage them from extracting revenue through means with more social benefits, like developing faster broadband networks, innovative apps, or service-bundling deals. Rather than make the best product, they would battle to make the best deals to provide targeted advertising—"a transformation from a market where innovation rules to one where deal-making rules."[183]

Furthermore, the net neutrality debate demonstrated how leaving regulation of Internet infrastructure up to antitrust law could lead to negative externalities.[184] The same is true in the context of regulating broadband consumers' privacy. Since the customer is the product in the online advertising market, reliance on market forces alone would encourage BIAS providers to collect, use, and share as much customer data as possible. However, when someone knows she is being watched, especially in a way she does not fully understand and which she cannot control, her behavior changes, resulting in chilling effects on the type of website she visits or speech she makes. Such effects may have the end result of keeping people from doing "a range of socially valuable activities" on the internet.[185] While such schemes may be extremely profitable, they are not in the best interests of industry or the country.

While there is little reason to think leaving things up to market forces will not lead to large negative externalities, there is even less reason to think optimal privacy protection comes from optimal markets. One problem with relying on market forces in the online advertising context is that a knowledge asymmetry between BIAS providers and the public prevents the market from effectively regulating itself and, thus, requires an expert regulatory authority that understands the market well

181 *Id.* at 49.

182 *Id.* at 49–50.

183 Tim Wu, *Why You Should Care About Net Neutrality*, SLATE (May 1, 2006, 4:35 PM), http://www.slate.com/id/2140850.

184 BELLIA ET AL., *supra* note 29, at 221. For example, by allowing an incumbent broadband provider to favor its affiliate media company through blocking, throttling, or paid prioritization, the market is less open for service providers offering a range of services under different pricing models.

185 FRISCHMANN, *supra* note 29.

enough to protect consumer privacy.[186] If regulation were left up to market forces in this situation, no one other than those directly involved with a specific agreement[187] would know whether the agreement provided sufficient consumer privacy protection.[188]

There is room for concern because while BIAS providers only claim to have access to information such as their customers' IP addresses and the top-level domains they visit,[189] recent technological developments suggest BIAS providers may have the capacity to examine the features of encrypted information packets (and thus their contents) through deep packet inspection,[190] website fingerprinting,[191] and deriving search queries.[192] Such capacities pose serious privacy risks, are easily hidden from consumers, and are poorly understood outside the companies directly party to potential future online advertising agreements. This suggests the need for a centralized authority to take on a regulatory role that requires them to lean more about these forces in order for consumers to be protected.

Furthermore, if there is no problem with the level of competition in the online advertising market (and without more details on how the FCC approach will impact BIAS providers), the trope of parity argument for a level playing field is a red herring. BIAS providers claim that edge providers like Google and Facebook have a particularly strong incumbent position in the online advertising market[193] "because the barriers to entry appear to be significant . . . to compete, firms must have access to . . . a sufficiently large audience and the technical expertise to navigate the complex web of firms in the advertising ecosystem."[194] Implicit in this claim is the belief that market entrants are at a severe disadvantage in accessing data, and Facebook and Google

186 *See* Public Knowledge and Common Cause, *supra* note 157, at 4.

187 For instance, a hypothetical contract between a BIAS provider and a third party company where the BIAS provider agreed to the collection, use, retention, and sharing of customer data with the third party company for the purposes of online advertising.

188 *See* Public Knowledge and Common Cause, *supra* note 157, at 4.

189 *See supra* Part I.

190 *See* Rieke, et al., *supra* note 51 ("By examining the features of the traffic—like the size, timing and destination of the encrypted packets—it is possible to uniquely identify certain web page visits or otherwise reveal information about what those packets likely contain.").

191 *Id.* ("This technique leverages the fact that different web sites have different features: they send differing amounts of content, and they load different third-party resources, from different locations, in different orders. By examining these features, it's often possible to uniquely identify the specific web page that the user is accessing, despite the use of strong encryption when the web site is in transit.").

192 *Id.* (Many popular search engines have an auto-suggest feature. "By analyzing the distinctive size of these encrypted suggestion lists that are transmitted after each key press, researchers were able to deduce the individual characters that the user typed into the search box, which together reveal the user's entire search query.").

193 Comcast Corporation, *supra* note 5, at 53–54 ("Google and Facebook together control almost 55% of the digital ad market.").

194 *Id.* at 54.

have significant market power due to their possession of vast data collections.[195] However, while Facebook and Google currently dominate the online advertising market (in part due to their vast data collections), this does not mean that there is not vibrant competition in this market, or that competition will not continue to grow. For one, the cost of collecting big data is very low and continues to decline.[196] Furthermore, data collection is non-rivalrous, which means collecting one piece of data does not prevent other companies from collecting the same piece of data through similar means.[197] It is also inexpensive to buy, store, and analyze big data.[198] As one commenter put it, "[t]hese characteristics—ubiquity, low cost, wide availability, and fleeting value—make big data different from the industry structures typically seen as conducive to competition problems."[199]

Additionally, newcomers' disruption of incumbent companies with vast data collections is not an uncommon occurrence among Internet firms:

> [H]istory has shown that entry barriers generally. . . . are low in the online space, as evidenced by the tremendous amount of entry and rapid gains often enjoyed by innovative new challengers . . . [f]or example, Google replaced Yahoo as the leading general search engine within a few years of its entry despite Yahoo having user data on several hundred million users and offering personalized search results prior to Google.[200]

The same thing could happen in the online advertising market: a company could buy a large set of data (maybe setting itself apart from the pack by buying higher-than-average-quality data or developing a better way to analyze the data), use that data to sell targeted advertisements, and then, as they gained more customers, begin to self-generate data, thereby gradually expanding into the space of larger firms. Volume of data is not the only factor determining a company's

195 Tucker & Wellford, *supra* note 16, at 1.

196 Tucker & Wellford, *supra* note 16, at 3; *see also* EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 1 (2014), https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf (showing how big data expansion is made possible by "the cratering costs of computation and storage"); Edith Ramirez, Chairwoman, Fed. Trade Comm'n, Keynote Address at the Technology Policy Institute Aspen Forum: The Privacy Challenges of Big Data: A View from the Lifeguard's Chair 2, 3 (Aug. 19, 2013), https://www.ftc.gov/sites/default/files/documents/public_statements/privacy-challenges-big-data-view-lifeguard%E2%80%99s-chair/130819bigdataaspen.pdf (recognizing that the "phenomenal growth in storage and analytic power" has resulted in a staggering reduction in costs).

197 Tucker & Wellford, *supra* note 16, at 3.

198 *Id.*

199 *Id.* at 4.

200 *Id.* at 7–8.

success in the market for online advertising.[201] Other factors include: "investment in engineering resources, an attractive user interface, speed, ease of use, quality of content, marketing, distribution arrangements, and complementary services—not to mention having a good idea."[202] The bottom line is: competition in the online advertising market is already quite vibrant, with low barriers to entry and plenty of newcomers to the space. Hence, this is another reason why the trope of parity is a solution in search of a problem.

B. *The Goal of Online Advertising Regulation Should Be Consumer Privacy*

Having shown that the goal of online advertising regulation should not be a level playing field because antitrust law alone does not provide sufficient protection for consumer privacy in the online advertising context,[203] we next turn to the alternative approach of FCC-style government regulation and discuss why it is more protective of consumer privacy.

Let us begin by explaining what BIAS providers really mean when they proffer the trope of parity argument. The reason BIAS providers care about the online advertising market is because they are seeking to grow revenue.[204] Since they do not foresee as great a potential for revenue growth in any other market, they want to enter this one and thus regulation is seen as impeding entry.[205] However, as we have already shown, there is no a priori reason to think equal access on equal terms to the online advertising market (essentially the FTC approach) will be better for society.[206] In fact, in a market where the consumer is the product,[207] there are good reasons to believe we should raise the barriers to entry in order to protect consumer privacy. To clarify, this Note is not arguing that we should not have regulatory restrictions just as strict on

---

[201] Concerning Google/DoubleClick, F.T.C. File No. 071-0170, 12 (Dec. 20, 2007) https://www.ftc.gov/system/files/documents/public_statements/418081/071220 googledc-commstmt.pdf (The FTC seems to agree. In its Google/DoubleClick investigation, the agency explained that "neither the data available to Google, nor the data available to DoubleClick, constitutes an essential input to a successful online advertising product.").

[202] Tucker & Wellford, supra note 16, at 9; see also Andres V. Lerner, The Role of "Big Data" in Online Platform Competition 5, 28 (Working Paper, 2014), https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2482780, ("[T]he firm with the most data does not necessarily win, and often does not win").

[203] *See supra* Section III.A.

[204] Sandra Fulton, *Pay-for-Privacy Schemes Put the Most Vulnerable Americans at Risk*, FREE PRESS (May 10, 2016), http://www.freepress.net/blog/2016/05/10/pay-privacy-schemes-put-most-vulnerable-americans-risk, ("ISPs are increasingly finding new revenue streams too, by taking part in the multibillion-dollar market that's evolved out of selling users' personal information to online marketers.").

[205] Interview with Brett M. Frischmann, Professor, Benjamin N. Cardozo Sch. of Law, in N.Y.C., N.Y. (Nov. 7, 2016).

[206] *See supra* Section III.A.

[207] *See supra* note 24.

edge companies; it is merely arguing that the trope of parity is not a conclusive argument against applying the FCC's regulatory approach to BIAS providers.

Historically, there have been many different contexts in which regulatory authorities, in the interest of privacy protection, have not allowed equal access on equal terms to a market for consumer data. For example, in response to a mandate from Congress in the 1996 Health Insurance Portability and Accountability Act ("HIPAA"), the Department of Health and Human Services ("HHS") created the HIPAA Privacy Rule.[208] Just like the FCC's Order, the HIPAA Privacy Rule restricted how covered entities could collect, use, retain, and share certain information, in this case, protected health information ("PHI").[209] Even though such a restriction would not allow certain health care providers to have equal access on equal terms to a market for patient data, HHS found that more stringent protection of this sensitive information was necessary for the benefit of society.[210] Similarly, the FCC has found that more stringent protection of consumer data is necessary in the broadband context:

> ISPs are "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." This is particularly true because a consumer, once signed up for a broadband service, simply cannot avoid that network in the same manner as a consumer can instantaneously (and without penalty) switch search engines . . . surf among competing websites, and select among diverse applications . . . [t]o those who say that broadband providers and edge providers must be treated the same, this NPRM proposes rules that recognize that broadband networks are not, in fact, the same as edge providers in all relevant respects.[211]

As we have shown,[212] BIAS providers and edge providers are in fact different in terms of how they interact with consumer data, so there is a rational basis for the FCC to believe greater privacy protections are needed in the broadband context. Although the same trope of parity argument could be made in the context of HIPAA (i.e., the rules about health information must apply the same to all actors to level the playing field), regulators instead favored a rule more protective of consumer

---

208 45 C.F.R. § 164 (2013).

209 *See* 45 C.F.R. § 164.502(a) (2013) ("A covered entity or business associate may not use or disclose protected health information, except as permitted or required by this subpart.").

210 U.S. Dep't Health & Human Serv., Off. for Civil Rts., Summary of HIPAA Security Rule (2013), http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/ (explaining how the HIPAA rules were created in response to the data privacy risks associated with the health care industry adopting new electronic information technologies).

211 NPRM, *supra* note 2, at 3.

212 *See supra* Section I.A.

privacy because of the heightened sensitivity and security risks involved with patient data.[213] Faced with similarly heightened privacy concerns, the FCC Broadband Privacy Rules tried to do the same thing in the context of BIAS providers attempting to access the online advertising market.

While it is clear that equal access on equal terms to a given market is not always in the best interest of society, there are additional reasons why raising barriers to entry through the FCC's approach to regulation of the online advertising market can yield social benefits. For one, preventing BIAS providers from using their incumbent position to bully their way into this market will encourage them to seek revenue through means with more positive externalities, such as building up their broadband networks so more people can have Internet access at higher speeds.[214] Another alternative revenue source for BIAS providers could be in developing innovative applications at the edge layer, producing revenue not just through the application itself, but also through the user data it generates (which a BIAS provider could still profit from if it were operating in the capacity of an edge provider).[215] Also, BIAS providers stand to benefit from the "virtuous cycle" of new applications driving up the demand for broadband services,[216] no matter whether they (1) themselves develop a hot new app or (2) are kept out of the online advertising market, thereby creating more fertile ground for newcomers with the next big idea.[217] Lastly (although this list is not exhaustive), the FCC approach may encourage BIAS providers to seek revenue through innovative bundling of services, such as bundling cable TV service with solar energy, saving customers time and money.

Furthermore, by increasing consumer confidence in the handling of sensitive customer information, the FCC approach "also promote[s] the virtuous cycle of innovation in which new uses of the network lead to increased end-user demand for broadband, which drives network improvements, which in turn lead to further innovative network uses, business growth, and innovation."[218]

Providing equal access on equal terms and leveling the playing field of the online advertising market should not be the goal of regulation in the broadband context. Since the FTC's approach would

213 U.S. Dep't Health & Human Serv., *supra* note 210.

214 More access to higher speeds is sorely needed in America, where "74.7% percentage of homes only have 1 choice for broadband at 25 mbps down/3 mbps up, 82.4% only have 1 choice at 50 down/ 3 up." Wheeler, *supra* note 173.

215 *See* FTC Privacy Report, *supra* note 25.

216 Wheeler, *supra* note 173, at 3.

217 Conversely, if the FCC approach were not adopted and BIAS providers were allowed to bolster their affiliate edge providers by sharing mass amounts of data with them, the market will be less open to a range of service providers and innovation would suffer.

218 In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 31 FCC Rcd. 13911, 13913 (2016).

further this goal by regulating BIAS providers and edge providers the same, it is not appropriate in a world where BIAS providers threaten to enter and expand an already vibrant advertising market where the consumer is the product and revenue is generated at the expense of consumer privacy. In short, the FTC approach would lead to "a transformation from a market where innovation rules to one where deal-making rules."[219]

Instead, the FCC approach would create more social benefits and positive externalities because it recognizes that consumer privacy should outweigh the broadband industry's interest in generating revenue. Such a perspective is crucial not only for future economic development, but also future social, cultural, and political development. As the amount of data collected from consumers is increasing exponentially and new technologies are being developed to aggregate data sets in ways that give companies more and more detailed information about who we are and, thus, how our preferences and personalities can be manipulated, it is better for society to tip the normative scale in favor of these heightened privacy interests.

CONCLUSION

This Note has attempted to lift the veil from the trope of parity, the argument often heard from incumbent industries when they face the threat of regulation: "the rules must apply the same to all actors in order to level the playing field." While this argument sounds appealing and egalitarian on its face, it is a distraction from the real underlying issue of whether society's normative goal should be a level playing field (i.e., optimized markets) or some other public policy motive. In the context of the future of broadband regulation, the playing field BIAS providers want leveled is the market for online advertising and the countervailing public policy motive is consumer privacy. Seen from this perspective, it is clear why we should prefer a regulatory scheme that prioritizes privacy protection over an optimal advertising market, especially given that this market cannot effectively regulate itself,[220] and BIAS providers stand to generate a lot of revenue by exploiting consumers' privacy interests.

Currently, the best regulatory scheme to achieve this goal is the FCC's ex ante, technology-specific, regulation-based approach, as outlined in the Broadband Privacy Order.[221] The FTC's ex post, technology-neutral, standards-based approach,[222] on the other hand, would threaten consumer privacy and lead to fewer social benefits

[219] Wu, *supra* note 183.
[220] *See supra* Section III.A.
[221] *See supra* Section II.C.i.
[222] *See supra* Section II.C.ii.

because its strategy favoring market forces over regulation will likely lead us toward an economy based more on advertising deals than innovation. For these reasons, state legislatures should pass laws affording consumers the same types of privacy protections set forth in the FCC's Broadband Privacy Order. Anything less will set a precedent for policy makers to favor industry's ability to generate revenue over consumer privacy and autonomy.

The dangers of ceding to the trope of parity and making a normative choice that allows companies to use their desire to grow revenue by entering a new market as a justification for usurping privacy regulations go beyond unwanted advertisements and spam email. Favoring deal-making between companies (whose practices are difficult for outsiders to understand or even ascertain) over consumer protection could have serious cultural, social, and political consequences in the future because it could lead to a gradual erosion of individuals' ability to make their own choices about which widget they buy, show they watch, or candidate they vote for in an election. As one commentator put it:

> If an online ecology of information that purports to be based on one mode of ordering is actually based on another, it sets an unfair playing field whose biases are largely undetectable by lay observers. Stealth marketing generates serious negative externalities that menace personal autonomy and cultural authenticity. Moreover, the degree of expertise necessary to recognize these externalities in the new online environment is likely to be possessed by only the most committed observers.[223]

Such a landscape, where companies are free to profit from the public's lack of knowledge and use data to manipulate consumer choice, would threaten the personal autonomy that is at the very foundations of our democracy. Therefore, now, more than ever, we as a society must ask *quis custodiet ipsos custodies*—"who will watch the watchers?"

Michael Del Priore[*]

---

[223] Frank Pasquale, *Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries*, 104 NW. U. L. REV. 105, 170 (2010).

[*] Michael Del Priore is a third-year student at Benjamin N. Cardozo School of Law, where he is pursuing a concentration in Data Law. In addition to being a Certified Information Privacy Professional/United States (CIPP/US), Mr. Del Priore is President of the Cardozo Data Law Society and a member of the Information Technology and Cyber Law Committee of the New York City Bar Association. Mr. Del Priore looks forward to a career as a data privacy attorney, helping clients operationalize privacy laws while maximizing the value of information.

I would like to thank my note advisor, Professor Brett M. Frischmann, for his insight, inspiration, and encouragement. I am also deeply grateful for my wife, Tonia, who helped me untangle strands of arguments on many occasions. Last but not least, I could not have done this without the support of the *AELJ* staff, as well as my mom, dad, and three brothers.