Before the

FEDERAL COMMUNICATIONS COMMISSION

Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of Broadband and Other Telecommunications Services	)	WC Docket No. 16-106
	)	
	)	

COMMENTS OF

James C. Cooper
Director, Program on Economics & Privacy
Associate Professor of Law
George Mason University School of Law

May 27, 2016

I. Introduction & Summary

In 2015, the FCC adopted the Open Internet Order (OIO), which subjected the provision of broadband Internet access service (BIAS) to regulation under Title II of the Communications Act.[1] As a result of this reclassification, the Federal Trade Commission (FTC) no longer has consumer protection enforcement jurisdiction over the provision of BIAS.[2] In an effort to fill the gap that it created, the FCC issued

[1] *Protecting and Promoting the Open Internet*, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601 (2015).
[2] The FTC is statutorily barred from jurisdiction over common carriers. 15 U.S.C. § 45(a)(2).

the Notice of Proposed Rulemaking on *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* (the "NPRM").[3]

The NPRM broadly sets out an *ex ante* regulatory approach that restricts the ability of BIAS providers to collect and use "customer proprietary information" ("CPI") by requiring certain levels of consumer consent depending on the type of data involved and with whom the data is to be shared.[4] The NPRM defines CPI quite broadly, not only encompassing "customer proprietary network information" (CPNI),[5] but also a panoply of data that may be available from consumers, including data that BIAS providers may not even collect.[6] Further, the NPRM contemplates that there may some practices that should be prohibited altogether due to their tendency to harm consumers. For example, the Commission places into this category of potentially suspect practices "offering customers . . . lower monthly rates for their consent to use and share their confidential information."[7]

The NPRM solicits comments on alternative regulatory approaches that should be considered.[8] This comment urges the FCC to retain a harm-based approach like the one that the FTC has applied to BIAS providers since the inception of broadband Internet.[9] It could do so by replacing the regulatory thicket it has proposed with a simple and flexible prohibition on BIAS providers engaging in "unfair and deceptive acts and practices."

Adopting a harm-based approach is likely to be more beneficial to consumers than the regime contemplated by the NPRM for two reasons.

First, there simply is no indication that rigid *ex ante* regulation of the type proposed is needed. The FCC offers no evidence that consumers are currently, or likely to be, harmed by BIAS providers' data practices.

Second, the harms-based approach that has been in place since the inception of BIAS provides important consumer benefits. Limiting enforcement to instances in which there is cognizable consumer harm assures that regulatory action will provide consumers with at least some benefits, which is a necessary (but not

---

[3] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, WC Dkt. No. 16-106, FCC 16-39 (Mar. 31, 2016) ("Privacy NPRM").
[4] *See* Privacy NPRM at ¶¶ 111-133.
[5] The FCC asserts that Section 222(a) provides it with independent authority to regulate BIAS providers with respect to "customer proprietary information," which includes "personally identifiable information," and "customer proprietary network information" under Section 222(h). *See* Privacy NPRM at ¶¶56-57. Although it is not the focus of this comment, there may be reasons to believe that this interpretation of FCC authority is an unreasonable statutory construction. *See*, *e.g.*, Peter Swire, *Comments to the FCC on Broadband Consumer Privacy*, at 2-4 (April 28, 2015), *at* http://peterswire.net/wp-content/uploads/Swire_FCC-testimony_CPNI_04_27_15.pdf.
[6] *See* Privacy NPRM at ¶62 n.117.
[7] Privacy NPRM at ¶¶259-263.
[8] *See id*. at ¶¶134-35.
[9] This approach is similar to the Industry and ITIF approaches. *See id*. at ¶¶280-82; 289.

sufficient) condition for a regulatory action to pass a cost-benefit test.[10] Additionally, an *ex post* harm-based approach is inherently more flexible than the type of *ex ante* regulation the FCC proposes—it would allow consumers with heterogeneous tastes to select into their desired combinations of privacy protection, price, and quality, and it also will allow regulators to more nimbly adapt to changing market conditions.

II. The NPRM Offers No Evidence that BIAS Providers' Practices Create Privacy Harms

It is beyond debate that limits on collection and use of consumer data will deprive consumers of benefits.[11] If the FCC is to impose stringent limitations on data flows for a major sector of the information economy, it should provide some empirical indications that consumers are suffering privacy harms under the status quo sufficient to justify this regulatory burden. As laid out below, the evidence cited in the NPRM falls short of this threshold.

First, although the NPRM throughout discusses how BIAS providers have potential access to a vast array of consumer data, it never attempts to identify the exact privacy values that may be at stake, or any nexus between BIAS provider data collection and privacy harms.

For example, it is clear that certain data (e.g., social security and credit card numbers, bank account information, drivers' license numbers, insurance information) may raise the risk of new- or existing-identity theft, and geolocation data may increase safety risks from stalking. Less clear, however, is the theory by which data, such as browsing histories, shopping records, MAC address, and application usage statistics, threaten privacy.[12] People clearly value being free from unwanted observation and intrusions into their private spheres, although this value varies across the population and contexts.[13] Further, revelation of certain sensitive

---

[10] It is not sufficient because although a regulation may provide benefits, they may be too small to offset countervailing costs.

[11] *See*, *e.g.,* Privacy NPRM at ¶¶263. EXECUTIVE OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES, at 39-42 (May 2014), *at* https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf. Economic studies have shown how restrictive privacy policies can have negative impacts on consumers. *See*, *e.g.*, Amalia Miller & Catherine Tucker, *Can Healthcare Information Technology Save Babies,* 119 J. POL. ECON. 289 (2011); Jin-Hyuk Kim & Liad Wagman, *Screening Incentives and Privacy Protection in Financial Markets: Theoretical and Empirical Analysis*, 46 RAND J. ECON. 1 (2015).

[12] *See* Privacy NPRM at ¶62.

[13] *See* Maureen K. Ohlhausen, *The FTC, The FCC, and BIAS*, George Mason University School of Law, Program on Economics & Privacy Briefing on Privacy Regulation after Net Neutrality, at 4 (March 30, 2016), *at* https://www.ftc.gov/system/files/documents/public_statements/942823/160331gmuspeech1.pdf.

information can dull incentives to engage in production of useful knowledge.[14] Finally, ubiquitous surveillance and predictions from the resulting data can lead to wasteful privacy-protective behavior.[15] The NPRM, however, never articulates how BIAS providers' collection and use of such CPI has the potential to be harmful in any of these dimensions. Instead, it appears to *assume* that mere access to these data is *ipso facto* harmful, asserting that "legally binding principles" are needed to temper BIAS providers' motivations to "use and share personal information about their customers."[16]

Not only does the NPRM fail to articulate a theory of privacy harm, more importantly, it also lacks *any* empirical evidence that BIAS providers' conduct is harming consumers. In fact, the NPRM offers little to support the case to regulate BIAS providers beyond hypotheticals and citations to various FTC reports—which themselves contain no empirical evidence—law review articles, surveys, and popular press articles.[17] This is a slim reed upon which to hang such an ambitious regulatory endeavor.

When considering this rule, the FCC must take into account the available empirical evidence, which tends to suggest (1) consumers generally are comfortable with the tradeoffs of data for content and lower prices; (2) consumers generally are willing to reveal information for small amounts of compensation; and (3) consumers have fewer privacy concerns with observation by anonymous servers than humans.

First, revealed preference strongly suggests that consumers are comfortable with the data they are sharing online. For example, the percentage of online adults engaging in social media rose from 8 percent in 2005 to 72 percent in 2013,[18] and the health tracking market has exploded in recent years.[19] Further, very few people

---

[14] For example, publication of HIV status may dull incentives to become tested in the first place, although such knowledge clearly is valuable. *See, e.g.*, Benjamin E. Hermalin & Michael L. Katz, Privacy, *Property Rights and Efficiency: The Economics of Privacy as Secrecy*, 4 QUANT. MKT'G & ECON. 209, 212 (2006). *See also* Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2386-87(1996); Joel Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877 (2003); Daniel Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1892 (2013); Julie Cohen, *What Privacy is For*, 126 HARV. L. REV. 1904, 1911 (2013); Neil Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 407 (2008).

[15] For example, to avoid the consequences of being predicted to be at risk for diabetes, one may attempt to conceal their suspect grocery purchases, such as by purchasing sugary foods with cash.

[16] Privacy NPRM at ¶3.

[17] For example, the NPRM cites the following in support of its proposal to ban consumers' ability to trade personal information used for discounts: the FTC's 2016 Big Data Report; an issue of *InfoSecurity Magazine*; two law review articles; a *New York Times Magazine*; and a Pew survey that finds that almost a majority of consumers (47%) are comfortable with sharing data for discounts in grocery store loyalty programs. *See* Privacy NPRM at ¶¶ 260-61, n.406-07.

[18] Joanna Brenner & Aaron Smith, *72% of Online Adults are Social Networking Site Users*, PEW RESEARCH CENTER, at 2-3 (Aug. 5, 2013), http://www.pewinternet.org/2013/08/05/72-of-online-adults-are-social-networking-site-users/.

[19] Susannah Fox, *The Self-Tracking Data Explosion*, PEW RESEARCH CENTER (June 4, 2013), http://www.pewinternet.org/2013/06/04/the-self-tracking-data-explosion/.

bother to opt-out of online tracking or adopt privacy-protecting technology.[20] A recent survey of the literature on the economics of privacy finds that the adoption of privacy enhancing technologies has lagged substantially behind the use of information sharing technologies.[21] These data seem to belie the notion that more stringent privacy regulation is required to instill the trust necessary to foster broadband use.[22]

Second, most researchers who have examined the issue find that privacy valuations are highly variable, and consumers generally are willing to accept small discounts and purchase recommendations in exchange for personal data.[23] For example, one study finds that consumers are willing to pay an additional $1-$4 for a hypothetical smartphone app that conceals location, contacts, text content, or browser history from third-party collectors.[24] Further, experimental literature finds that consumers' willingness to divulge private information also appears to depend on context and cues.[25]

Finally, research also suggests, not surprisingly, that people are more concerned with proximate observation by individuals than distant observation by computers.[26] For example, one study finds that self-checkout in libraries has increased the number of LGBT books checked out by students, suggesting that privacy concerns are reduced when human interaction is removed from the situation.[27]

The NPRM also argues that BIAS providers enjoy unique access to consumer data, which necessitates a more stringent regulatory regime. Recent empirical work, however, suggests that many of the concerns that BIAS providers deserve

---

[20] *See* Maurice E. Stucke & Allen P. Grunes, *No Mistake About It: The Important Role of Antitrust in the Era of Big Data*, ANTITRUST SOURCE at 8-9 (April 2015).
[21] *See* Alessandro Acquisti et al., *The Economics of Privacy*, J. ECON. LIT. at 38-39 (forthcoming, 2016).
[22] *See* Privacy NPRM at ¶3.
[23] *See* Dan Cvrecek, Marek Kumpost, Vashek Matyas & George Danezis, *A Study on the Value of Location Privacy*, Proceedings of the 5th ACM Workshop on Privacy in the Electronic Society (2006); Hal R.Varian, Glenn Woroch & Fredrik Wallenburg, *Who Signed Up for the Do Not Call List? (2004), http://eml.berkeley.edu/~woroch/do-not-call.pdf*; Ivan P. L. Png, *On the Value of Privacy from Telemarketing: Evidence from the "Do Not Call' Registry* (2007), at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1000533; Michael Kummer & Patrick Schulte, *Money and Privacy: Andriod Market Evidence* (2016) (finding consumers are willing to trade money for data used in targeted ads in Andriod app market), *at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2567164. *See also* Acquisti *et al*, *supra* note 21, at 41 for a review of the empirical literature.
[24] Scott Savage & Donald M. Waldman, *The Value of Online Privacy* (2013), *at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2341311.
[25] *See* Alessandro Acquisti, Leslie K. John, and George Lowenstein, *Strangers on a Plane*, 37 J. CONSUMER RES. 858 (2011).
[26] Benjamin Wittes & Jodie Liu, *The Privacy Paradox: The Privacy Benefits of Privacy Threats*, CENTER FOR TECHNOLOGY INNOVATION AT BROOKINGS (May 2015), http://www.brookings.edu/~/media/research/files/papers/2015/05/21-privacy-paradox-wittes-liu/wittes-and-liu_privacy-paradox_v10.pdf.
[27] Stephanie Mathson & Jeffry Hancks, *Privacy Please? A Comparison Between Self-Checkout and Book Checkout Desk for LGBT and Other Books*, 4 J. ACCESS SERVS. 27, 28 (2007).

special privacy attention are unfounded.[28] For example, this study finds that most consumers use multiple BIAS providers throughout the day, suggesting that most BIAS providers lack a global view of their consumers' data habits.[29] Further, the increasing use of encryption and VPNs also reduces BIAS providers' ability to have visibility into consumer data flows.[30]

III. A Harms-Based Approach to Privacy Regulation Provides Consumers Important Benefits

Until the OIO, the FTC enjoyed consumer protection jurisdiction over the provision of BIAS, having the ability to charge BIAS providers with violations of Section 5 of the FTC Act if they engaged in "unfair or deceptive acts or practices."[31] Section 5 is a harm-based statute. A practice is considered unfair if: 1) it creates a substantial likelihood of consumer injury; (2) that is not outweighed by any benefits to consumers or to competition; and (3) it is not reasonably avoidable by consumers.[32] The FTC's deception statement requires that a statement be "false or misleading" and "material," in the sense that it impacted the consumer's purchasing decision.[33] In this manner, the concept of materiality acts as an indirect harm requirement—when a false statement is material, it can be assumed to cause harm because it triggered a consumer purchase that otherwise would not have happened.[34]

---

[28] *See* Peter Swire, Justin Hemmings, and Alana Kirkland, *Online Privacy & ISPS: ISP Acess to Consumer Data is Limited and Often Less than Access by Others* (Feb. 29, 2016), *at* http://www.iisp.gatech.edu/working-paper-online-privacy-and-isps.

[29] *Id*. at 9-10.

[30] *Id*.

[31] 15 U.S.C. § 45(a).

[32] The Commission first issued the Unfairness Policy Statement in 1980, and later made it binding precedent by appending to the International Harvester decision. *See* FTC Policy Statement of Unfairness, appended to *In re* International Harvester Co., 104 F.T.C. 949 (1984), *available at* http://www.ftc.gov/bcp/policystmt/ad-unfair.htm. Congress eventually codified the Unfairness Policy Statement with the 1994 FTC Reauthorization Act. 15 U.S.C. § 45(n).

[33] *See* FTC Policy Statement on Deception, appended to *In re* Cliffdale Assoc., Inc., 103 F.T.C. 110, 175–183 (1984), *available at* http://www.ftc.gov/bcp/policystmt/ad-decept.htm. The Commission also issued a statement on advertising substantiation in *Thompson Medical*. FTC Policy Statement Regarding Advertising Substantiation, appended to *In re* Thompson Medical Co, 104 F.T.C. 648, 839 (1984), *available at* http://www.ftc.gov/bcp/guides/ad3subst.htm.

[34] If the unfairness test lays out a quasi-negligence standard (liable only when costs are greater than the benefits), the deception test is one of strict liability for false claims, under the assumption that false claims are never beneficial. *See* J. Howard Beales III, Director of Bureau of Consumer Protection, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, Remarks at The Marketing & Public Policy Conference (May 30, 2003) ("deception analysis essentially creates a shortcut, assuming that, when a material falsehood exists, the practice would not pass the full benefit/cost analysis of unfairness, because there are rarely, if ever, countervailing benefits to deception"), *at* https://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection.

There is no reason to believe that the FTC's harm-based approach failed to protect consumers' privacy prior to the OIO. It has used its Section 5 authority in over 150 enforcement actions involving privacy and data security, including actions against BIAS providers.[35] It has used its deception authority against firms who have violated their material promises in their privacy policies, and has used its unfairness authority to declare certain practices—such as surreptitious recording of intimate activities—unfair.[36]

Further, an *ex post* harm-based approach offers at least three advantages over the *ex ante* regulatory approach offered by the NPRM. First, by focusing on harm, one can be sure that government action is actually providing consumers with some benefits. There clearly are consumer benefits from BIAS providers' use of data. For example, targeted advertising brings more revenues, which can lead to lower prices and improved content.[37] Thus, absent offsetting consumer benefits in terms of increased privacy protection, consumers are unambiguously worse off with regulation. Requiring harm to trigger action at least guarantees that the necessary (but not sufficient) condition for regulation to provide net consumer benefits is met.

Second, heterogeneous privacy preferences increase the costs associated with a common standard.[38] As noted above, empirical evidence suggests that most consumers are willing to trade information for free services, and are likely have heterogeneous demands for privacy, especially as it relates to non-sensitive information.[39] Accordingly, a harm-based approach that relies on deception authority to enforce promises made in privacy policies will allow consumers to self-select into their preferred combination of privacy protection, price, and quality; it harnesses consumers' private information about their privacy values rather than having the FCC attempt to fashion a common rule to cover everyone.[40] What's more, it has the potential to enhance competition over the dimension of privacy by allowing firms to attract consumers with various bundles. Further, unfairness authority can be used to set a baseline level of privacy protection, by prohibiting a

---

[35] *See* Ohlhausen, *supra* note 13, at 2-3; *see also Examining the Proposed FCC Privacy Rules*, Prepared Statement of the Federal Trade Commission, Before the Senate State Senate Subcommittee on Privacy, Technology, and the Law (May 11, 2016), *at* https://www.ftc.gov/system/files/documents/public_statements/948633/160511fccprivacyrules.pdf.

[36] *See, e.g.*, Compliant, *In re Designerware, LLC*, Docket No. C4390 (F.T.C. April 15, 2013), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415designerwarecmpt.pdf.

[37] *See* Avi Goldfarb & Catherine E. Tucker, *Privacy Regulation and Online Advertising*, 57 MGM'T SCI. 57 (2011); J. Howard Beales, III, *The Value of Targeted Advertising* (2010), *at* http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf.

[38] *See* James C. Cooper, *Separation, Pooling, and Big Data*, at 41-43 (April 2016), *at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2655794.

[39] *See* Ohlhausen, *supra* note 13, at 4.

[40] *See* Howard Beales et al., *The Efficient Regulation of Consumer Information*, 24 J.L. & ECON. 491, 513 (1981) ("informational remedies allow consumers to protect themselves according to personal preferences rather than place on regulators the difficult task of compromising diverse preferences with a common standard.").

limited set of practices to which all consumers are likely to object, for example those involving collection and use of sensitive health information or children's information without consent.[41]

Finally, a harms-based approach has the advantage of being more nimble than relying on prescriptive rules. Indeed, the FTC has deftly applied its capacious statutory language to all manner of firms and practices, including BIAS providers. If technology or other market conditions change to make certain practices more or less harmful, under a harm-based approach, the FCC could avoid a cumbersome new rulemaking, and instead merely calibrate its enforcement efforts.[42] This consideration should weigh heavily, as one could hardly think of a more rapidly evolving industry than that of BIAS providers.

IV. Conclusion

The framework laid out in the NPRM stands to severely limit the ability of BIAS providers to use consumer information in beneficial ways. The harm the FCC's proposal would inflict on consumers could be justified if there were evidence that it would ameliorate privacy harms sufficient to offset these costs. But at this point, there is simply no evidence to suggest that the regulatory regime the NPRM contemplates comes close to meeting this burden. Accordingly, the FCC should abandon the prescriptive rules in the NPRM, and instead adopt a harm-based standard fashioned after the FTC's approach to consumer protection.

[41] *See* Ohlhausen, *supra* note 13, at 5; Privacy NPRM at ¶136.
[42] *Id*. at 210-11.