United States of America

Federal Trade Commission

"The FTC, The FCC, and BIAS"
Remarks of Maureen K. Ohlhausen[1]
Commissioner, U.S. Federal Trade Commission

The George Mason University School of Law
Public Policy Briefing on Privacy Regulation after Net Neutrality

March 30, 2016

Thank you to James Cooper and George Mason Law School, its Law and Economics Center, and the Program on Economics and Privacy. I am a proud alum of George Mason Law School, just as James is a (hopefully) proud alum of the Federal Trade Commission. I am excited about the new Program on Economics and Privacy that James is leading. There is a serious need for rigorous economic thinking about privacy issues, so for you students in the audience, I hope you'll consider working in this area.

My standard disclaimer applies, as always: these thoughts are my own, and do not necessarily represent the views of the FTC or other Commissioners.

I'm pleased to be here to discuss the FTC's history of privacy enforcement, and the policy implications of the FCC's recent efforts in this space. By now, most of you likely know what triggered the FCC's new privacy efforts. But just to set the scene: When the FCC adopted

[1] The views expressed in these remarks are my own and do not necessarily reflect the views of the Federal Trade Commission or any other Commissioner.

its net neutrality rules, it chose to reclassify "Broadband Internet Access Service", or "BIAS" as a Title II common carrier service.[2] (I'll talk a lot more about BIAS later.) This affected the FTC's oversight of BIAS providers. Although the FTC has general jurisdiction, there are a few carve outs, including common carriers acting as common carriers.[3] Thus, the FCC's reclassification affected the FTC's long-standing authority to protect consumers' privacy in their interactions with their broadband internet service providers.

Subsequently, the FCC decided to step into the consumer protection gap that it created. In fact, tomorrow the FCC will vote on a proposal to set privacy rules for BIAS providers.[4] We haven't yet seen the full Notice of Proposed Rulemaking, but FCC Chairman Tom Wheeler did release a fact sheet summarizing the proposal at a very high-level.[5] Therefore, for today, when I talk about the FCC's proposal, I am referring to this high-level outline. We should have more details soon.

FTC Approach to Privacy. This change to the oversight of ISP privacy practices matters because the FTC is *the* primary privacy and data protection agency in the U.S., and probably the most active enforcer of privacy laws in the world. We have brought more than 150

---

[2] *See* Protecting and Promoting the Open Internet, Report and Order on Remand, Declaratory Ruling, and Order, FCC 15-24 (Mar. 12, 2015).

[3] 15 U.S.C. § 45(a)(2) (FTC authority does not reach "common carriers subject to the Communications Act of 1934"). "An entity is a common carrier … only with respect to services it provides on a common carrier basis." FED. TRADE COMM'N, BROADBAND CONNECTIVITY COMPETITION POLICY STAFF REPORT at 38 (June 2007), https://www.ftc.gov/reports/broadband-connectivity-competition-policy-staff-report, (citing 47 U.S.C. § 153(44). *See also*, FTC v. AT&T, No. C-14-4785 EMC, Order Denying Defendant's Motion to Dismiss at 23 (Mar. 31, 2015) (holding that the FTC's "common carrier exception applies only where the entity has the status of common carrier and is actually engaging in common carrier activity").

[4] Press Release, Fed. Comm. Comm'n, March 2016 Open Commission Meeting (Mar. 2016), https://www.fcc.gov/news-events/events/2016/03/march-2016-open-commission-meeting.

[5] Press Release, Fed. Comm. Comm'n, Chairman Wheeler's Proposal to Give Broadband Consumers Increased Choice, Transparency & Security With Respect to Their Data (Mar. 10, 2016), https://www.fcc.gov/document/broadband-consumer-privacy-proposal-fact-sheet.

privacy and data security related enforcement actions, including actions against ISPs and against some of the biggest companies in the Internet ecosystem.[6] We also conduct extensive consumer and business outreach and guidance, coordinate workshops to foster discussions about privacy in emerging areas, coordinate on privacy efforts internationally, and advocate for policies about privacy and data use that improve consumer welfare.[7] Despite this success, some have suggested that the FCC is the brawnier cop on the privacy beat.[8] Perhaps that makes the FTC the brainy-er cop? Indeed, I believe the success of the FTC's privacy and data security program is *because of* – not in spite of – our smart, restrained privacy approach, which maximizes consumer self-determination.

FCC and BIAS. As I already mentioned, the FCC coined the acronym BIAS in its open internet order to describe ISPs subject to the new open internet rules. It's a curious choice of acronym for an expert agency to apply to an entire industry segment. After all, "bias" is the tendency to treat similarly situated things differently without a logically sound justification. Rules, including privacy rules, can be biased. In my experience, proposals to regulate privacy

---

[6] *See* FED. TRADE COMM'N, PRIVACY & DATA SECURITY UPDATE (2015) (Jan. 2016), https://www.ftc.gov/reports/privacy-data-security-update-2015.

[7] *See* FED. TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? UNDERSTANDING THE ISSUES (Jan. 2016), https://www ftc.gov/reports/big-data-tool-inclusion-or-exclusion-understanding-issues-ftc-report; FED. TRADE COMM'N, PRIVACYCON (Jan. 14, 2016), https://www ftc.gov/news-events/events-calendar/2016/01/privacycon; FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS (June 2015), https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.

[8] Letter from Access et al., to Tom Wheeler, Chairman, Fed. Comm. Comm'n, re: Broadband Privacy Rulemaking, 1 (Jan. 20, 2016) https://static newamerica.org/attachments/12311-oti-joins-coalition-calling-for-greater-protection-of-online-privacy-for-broadband-consumers/Broadband_Privacy_Letter_to_FCC.ab06f1ece7fa4d3c98f33b75910287fb.pdf (quoting Julie Brill, Commissioner, Fed. Trade Comm'n, Address at the Georgetown Institute for Public Representation and Center for Privacy and Technology Symposium on Privacy and Net Neutrality: Net Neutrality and Privacy: Challenges and Opportunities 1 (Nov. 19, 2015), https://www.ftc.gov/public-statements/2015/11/net-neutrality-privacy-challenges-opportunities.).

tend to be biased in at least three ways. Let me describe each of these three potential biases and how regulators can avoid such biases.

First, privacy rules ought to avoid a bias toward the privacy preferences of the few. We know that consumer privacy preferences differ greatly depending on the type of data and its use. On one hand, consumer preferences are fairly uniform with regard to certain uses of sensitive data. For example, the overwhelming majority of consumers object to unauthorized third parties using their financial data to debit their bank accounts or to open credit cards in their names. On the other hand, we know from experience as well as academic research – including a recent Pew study – that for other kinds of data and uses, people have widely varying privacy preferences.[9] Some people wish to minimize the information they share with others, even for advertising. Other people post their most embarrassing moments on Twitter or are glad to share information in exchange for free or reduced-cost services. And most consumers are open to some types of sharing but not to other types.

At the FTC, our privacy approach respects the autonomy of all consumers, including those with different privacy preferences than ourselves. As such, it seeks to enable consumers to match their privacy preferences with a company's privacy practices. In pursuit of this goal, the FTC protects privacy with a two-pronged approach, seeking to prevent both deception and unfairness.

---

[9] A recent Pew survey and focus groups testing consumer privacy preferences with regard to six different scenarios found 17% of polled rejected all the scenarios, 4% accepted all the scenarios, and the substantial majority indicated that at least one of the scenarios was potentially acceptable. *See* LEE RAINIE AND MAEVE DUGGAN, PEW RESEARCH CENTER , PRIVACY AND INFORMATION SHARING (Dec. 2015), http://www.pewinternet.org/2016/01/14/2016/Privacy-and-Information-Sharing/. *See also* CTA, BIOMETRIC TECHNOLOGIES: UNDERSTANDING CONSUMER SENTIMENTS (Mar. 30, 2016), http://www.cta.tech/CorporateSite/media/Government-Media/Biometrics_Research_key-findings_3-22.pdf.

For types of data and uses where consumers have widely varying privacy preferences – such as advertising – we use our deception authority to promote marketplace competition to satisfy this wide range of consumer preferences. A functioning market requires companies to keep their promises. Under our deception authority, then, we bring a case when a company makes privacy promises to consumers that materially affect consumers' actions, but the company does not keep those promises. This deception-based approach encourages companies to develop privacy practices that accommodate widely varying consumer privacy preferences.

Under our unfairness authority, however, we have found certain privacy practices to be unfair, even if a company has made no promises to a consumer. Specifically, our unfairness authority prohibits practices that cause substantial harm that is unavoidable by consumers and which is not outweighed by benefits to consumers or competition.[10] Practices that the FTC has found unfair consistently match practices that consumers generally reject. For example, we brought an unfairness case against a data broker that sold sensitive financial information to individuals whom the data broker knew or should have known were identity thieves.[11] Other privacy violations with substantial harm involve accessing medical information, real time location data, and information about children without consumers' express consent.

Thus, unfairness establishes a baseline prohibition on practices that the overwhelming majority of consumers would never knowingly approve. Above that baseline, consumers are free to find providers that match their preferences, and our deception authority governs those arrangements.

---

[10] *See* 15 U.S.C. § 45(a)(1) (2012) (providing that"[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful").

[11] Fed. Trade Comm'n, In the Matter of Sequoia One, LLC, https://www ftc.gov/enforcement/cases-proceedings/132-3253/sequoia-one-llc.

In establishing the proper baseline of prohibited practices, regulators must avoid bias. If regulators set the baseline too low, it would not stop harmful practices that most consumers oppose. Too high, and it would prohibit services many consumers would prefer. Indeed, too-high a privacy baseline – a biased baseline – imposes the privacy preferences of the few on the many.

How can one avoid this bias toward the preferences of the few? At the FTC, our unfairness test's emphasis on real consumer harm and cost-benefit analysis helps ensure that the baseline is in the right place. Thus, privacy practices found by the FTC to be unfair are those that reflect consumer consensus.[12]

As described in the recently released fact sheet, the FCC's proposed privacy rules for ISPs appear to be more restrictive than the rules for other players in the internet ecosystem. The FCC's proposal divides potential ISP data uses into three categories with corresponding mandatory practices. The first category is first-party use of data for the purposes of providing broadband services to consumers. ISPs do not need further customer notice to engage in this use. For the second category of use, marketing of communications-related services by the BIAS provider and its affiliates, ISPs must provide an opt out. At this point, it is difficult to know how the requirements in these first two categories lines up with the FTC's approach because the fact sheet isn't clear about what types of data are covered. Personally identifiable data? Sensitive data such as financial information or location information? Or all data that happens to cross the ISP's network? The fact sheet uses a wide variety of terms for data, including "information,"

[12] *See* Maureen K. Ohlhausen, Commissioner, Fed. Trade Cmm'n, Privacy Regulation in the Internet Ecosystem (Mar. 23, 2016), https://www ftc.gov/public-statements/2016/03/privacy-regulation-internet-ecosystem.

"personal information," "data," and "personal data." We will have to see what the NPRM proposes on this.

The third, catch-all category in the FCC's proposal includes any uses of data not in the other two categories. The proposal would require ISPs to get consumers to opt in for any use in this category. Thus, the FCC's proposal appears to prohibit any data use *except* for the few uses covered by the previous two prongs, absent express consumer consent. This opt in requirement appears to go beyond the obligations faced by other companies in the internet ecosystem.

Some privacy advocates, apparently frustrated with the privacy practices offered in today's marketplace, applaud the FCC's proposed precautionary approach to data use.[13] Such an approach matches these advocates' privacy preferences. But for the reasons discussed above, baseline privacy rules ought to reflect the preferences of the many, not the few. And where consumer preferences vary greatly, any rules should promote a wide range of options rather than a single solution.

So, first, privacy rules ought to avoid bias toward the privacy preferences of the few.

Second, privacy regulation ought to avoid bias against future data uses. People persistently overvalue existing conditions and over discount future benefits.[14] Similarly, we have a tendency

---

[13] *See* Letter from Access et al., to Tom Wheeler, Chairman, Fed. Comm. Comm'n, re: Broadband Privacy Rulemaking, 1 (Jan. 20, 2016) https://static newamerica.org/attachments/12311-oti-joins-coalition-calling-for-greater-protection-of-online-privacy-for-broadband-consumers/Broadband_Privacy_Letter_to_FCC.ab06f1ece7fa4d3c98f33b75910287fb.pdf ; Letter from American Civil Liberties Union et al., to Tom Wheeler, Chairman, Fed. Comm. Comm'n, re: Broadband Privacy Rulemaking (Mar. 7, 2016), https://www.epic.org/privacy/consumer/Broadband-Privacy-Letter-to-FCC.pdf; Letter from Freepress, to Tom Wheeler, Chairman, Fed. Comm. Comm'n (Mar. 14, 2016), http://www.freepress.net/resource/107342/free-press-letter-section-222-and-privacy-rights.

[14] *See* Allison Schrager, "The behavioral economics behind Americans' paltry nest eggs," *Quartz* (Jan. 13, 2014), http://qz.com/165894/the-behavioral-economics-behind-americans-paltry-nest-eggs/. *See also* Gregory S. Berns et al., "Intertemporal choice--toward an integrative framework," 11 Trends in Cognitive Sciences 11 (2007), 482-488 https://dash.harvard.edu/bitstream/handle/1/4554332/Laibson_IntertemporalChoice.pdf?sequence=2

to overestimate potential future harm.[15] Regulators, too, face this same problem.[16] Regulation, therefore, often reflects the status quo, and, in extreme cases, unintentionally precludes future beneficial developments. In the area of privacy, notice and choice frameworks can be biased against future uses of data. For example, an effective and transparent opt-in framework typically requires that companies know at the time of collection how they will use the collected information. Yet data, including non-sensitive data, often yields significant consumer benefits from uses that could not be known at the time of collection. Mandating opt in consent for uses of certain types of sensitive data such as credit card numbers or SSNs may reflect consumer preferences, and I have supported such requirements in my time at the FTC. But if such mandates are applied to non-sensitive data, the inherent bias of such frameworks against future uses likely will reduce future benefits.

This inherent bias of notice and choice frameworks against future beneficial uses is part of why I and many others, including the President's Council of Advisors on Science and Technology and the White House's own report on Big Data, have urged a shift in focus toward a use-based or harms-based approach to privacy.[17]

As I described earlier, it appears the FCC proposal would prohibit all but a few uses unless consumers opt in, however. Thus, this approach appears to be biased against beneficial future uses of data. Moreover, this approach is more tilted against future data uses by ISPs than

---

[15] Ann Cavoukian, "2011: The Decade of Privacy by Design Starts Now," *ITBusiness* (Jan. 15, 2011), http://www.itbusiness.ca/blog/2011-the-decade-of-privacy-by-design-starts-now/20298.

[16] *See generally* W. Kip Viscusi and Ted Gayer, *Behavioral Public Choice: The Behavioral Paradox of Government Policy*, MERCATUS WORKING PAPER (Mar. 2015), http://mercatus.org/sites/default/files/Viscusi-Behavioral-Public-Choice.pdf.

[17] PRESIDENT'S COUNCIL OF ADVISORS ON SCIENCE AND TECHNOLOGY, REPORT TO THE PRESIDENT: BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE x-xi (May 2014) ("[A] policy focus on limiting data collection will not be a broadly applicable or scalable strategy – nor one likely to achieve the right balance between beneficial results and unintended negative consequences (such as inhibiting economic growth."); Executive Office of the President, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 56 (May 1, 2014).

are the requirements that other internet companies face. Which brings me to my third concern about bias.

Privacy regulation ought to treat like-situated companies alike. Economists (and common sense) tell us that if different sets of rules govern competitors, companies subject to the more onerous or unpredictable regime are disadvantaged compared to those outside that regime. This may damage competition or artificially distort the market as companies seek to avoid the more onerous regime.

The FCC proposal would regulate how broadband ISPs may use subscriber data. It appears to impose stricter rules on ISPs than those under which edge providers, such as Google, Yahoo, or Facebook, for example, operate. Some have argued that it makes sense for the rules to differ. They claim that ISPs are uniquely situated to collect consumer information because all of a consumers' communications travels over the ISP's network. If this was ever true, it is not true today. As Peter Swire's recent working paper concludes, ISPs have neither a comprehensive nor unique window into consumer data.[18] Consumers multi-home, using multiple ISPs throughout the day. They connect to the internet through their home broadband connection, their mobile device connection, their employer's network, or their local coffee shop's Wi-Fi. Each of these different ISPs has only a fragment of the users' total internet traffic. Thus I question the assumption that an ISP has more comprehensive data than, say, a mobile device that a consumer carries constantly, or a browser that syncs across computers, or a web service that interacts with the same consumer on many different devices. Furthermore, any data that crosses an ISP's

[18] PETER SWIRE, ONLINE PRIVACY AND ISPS: ISP ACCESS TO CONSUMER DATA IS LIMITED AND OFTEN LESS THAN ACCESS BY OTHERS 4 (Feb. 29, 2016), http://www.iisp.gatech.edu/working-paper-online-privacy-and-isps.

network comes from a piece of hardware or software that has perhaps an equally comprehensive view of the consumer's activities. And as internet services increasingly encrypt their traffic, the data which ISPs can access diminishes. In short, I remain unconvinced that ISPs have access to types or volumes of consumer data so unique that it justifies a special set of particularly strict rules.

Privacy advocates have been seeking for years to impose stricter privacy obligations across the Internet ecosystem, including on edge providers and ad networks, the Googles and Facebooks of the world.[19] Yet some now argue that ISPs are specially situated and therefore must be subject to stricter rules.[20] Given this history, it shouldn't be surprising that some advocates have already suggested that an FCC-led beachhead of restrictive privacy requirements could support similar requirements for edge providers.[21] Thus, all companies that wish to use consumer data for innovative new products and services should pay close attention to the FCC proceeding to set privacy rules for ISPs.

Conclusion

At its core, protecting consumer privacy ought to be about effectuating consumers' preferences. If privacy rules don't accommodate consumers' varying privacy preferences,

---

[19] *See generally* Online Tracking and Behavioral Profiling, https://epic.org/privacy/consumer/online_tracking_and_behavioral.html; ELECTRONIC PRIVACY INFORMATION CENTER, PRETTY POOR PRIVACY: AN ASSESSMENT OF P3P AND INTERNET PRIVACY (June 2000), https://www.epic.org/reports/prettypoorprivacy.html; *Testimony and Statement for the Record of Marc Rotenberg, Director, Electronic Privacy Information Center on Communications Privacy before the Subcommittee on Courts and Intellectual Property House Judiciary Committee* (Mar. 26, 1998), https://epic.org/privacy/internet/rotenberg-testimony-398.html; *In re* Facebook, Electronic Privacy Information Center, https://epic.org/privacy/inrefacebook/.

[20] HAROLD FELD ET AL., PUBLIC KNOWLEDGE, PROTECTING PRIVACY, PROMOTING COMPETITION: A FRAMEWORK FOR UPDATING THE FEDERAL COMMUNICATIONS COMMISSION PRIVACY RULES FOR THE DIGITAL WORLD (Feb. 16, 2016), https://www.publicknowledge.org/documents/protecting-privacy-promoting-competition-white-paper.

[21] Harold Feld, Remarks at Preserving Broadband Network Privacy (Feb. 17, 2016) https://www.publicknowledge.org/events/preserving-broadband-network-privacy; @haroldfeld, TWITTER (Mar. 31, 2016, 12:28 PM), https://twitter.com/haroldfeld/status/715576443401469954 ("Totally. Am hoping @FCC action permits @FTC 2 go further despite limits of Sec. 5(n) in areas under its jurisdiction").

consumers' choice will be limited and consumers will be worse off. If privacy rules prevent beneficial future uses of data, innovation will suffer. And if privacy rules hamper one group of competitors to the benefit of another group, competition will be reduced.

When the FCC releases its privacy NPRM, I hope it will analyze how it can accommodate varying consumer preferences regarding different types of data, permit future beneficial uses of data, and avoid the negative competitive effects of disparate regulation.

Thank you again for having me, and I'd be glad to take any questions you might have.