

Jon Leibowitz¹
Davis Polk & Wardwell LLP
901 15th Street, NW
Washington, DC 20005

May 23, 2016

Re: Protecting the Privacy of Broadband and Other Telecommunications Services, WC
Docket No. 16-106

The Chairman and the Commissioners
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Dear Chairman Wheeler and Commissioners Clyburn, Rosenworcel, Pai, and O'Rielly:

Justice Louis Brandeis, one of the intellectual fathers of the Federal Trade Commission, the nation's foremost consumer protection agency, called the right to privacy, "the most comprehensive of rights and the right most valued by civilized men."² Indeed, privacy has long been a cornerstone of the FTC's consumer protection mission, and all of us who worked at the FTC are proud of the work we did to both protect consumer privacy and ensure that consumers continue to benefit from the high-tech innovation and competition that has revolutionized modern life. As consumers continue to migrate more and more of their lives online, the FTC has interceded not to erect stop lights dictating what companies and consumers can and cannot do, but rather to strike the right balance between privacy and innovation. Taking a comprehensive approach, the FTC has built a proven track record of success through robust enforcement, including over 400 successful privacy enforcement actions; occasional regulation like the initial 1999 and subsequent 2010 rulemakings on the Children's Online Privacy Protection Act; and thoughtful policy initiatives like the 2012 Privacy Report, "Protecting Consumer Privacy in an Era of Rapid Change,"³ a multi-year endeavor that incorporated the findings of iterative policy workshops beginning in 2006, a draft Privacy Report in 2010, and over 450 comments from consumer and industry advocates, technology and policy experts, and the public.

In the four years since the publication of the Privacy Report, the FTC has held more workshops and issued additional reports and guidance tailored to specific sectors, technologies and

¹ I served as an FTC Commissioner from 2004-2009, and as Chairman from 2009-2013. While I currently represent ISPs and technology companies in various contexts, I write this letter in my personal capacity and the views set forth herein are my own.

² *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

³ Protecting Consumer Privacy in an Era of Rapid Change – Recommendations for Businesses and Policymakers, FTC Report, (Mar. 2012) (the "2012 Privacy Report," the "FTC Report" or the "Privacy Report"), available at <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

practices to account for changes in the services offered over the Internet,⁴ and in the data collection and tracking technologies used by various entities within the Internet ecosystem.⁵ Additionally, there have been fundamental changes in the way consumers access and use the Internet itself.⁶ Despite these changes, the framework established in 2012 and the principles within the framework not only remain the same, but also are more applicable than ever, as proven through repeated testing and enforcement in the dynamic Internet marketplace.⁷

Consequently, those of us who worked at the FTC were heartened by the FCC and Chairman Wheeler's stated aim to craft its proposed broadband privacy rules in a manner "consistent with [the] FTC's thoughtful, rational approach,"⁸ and incorporating the core principles of the 2012 Privacy Report: privacy-by-design; choice; and transparency. FCC rulemaking consistent with the FTC's privacy framework would ensure that privacy enforcement remains technology neutral, based on the type of data being collected and how it is used, rather than turning on the type of entity collecting the data. Parts of the FCC's proposed rule are consistent with the FTC approach; however, in many important areas it overshoots the mark, proposing regulations for broadband providers that go well beyond those imposed upon the rest of the Internet economy and which, if adopted, would undercut benefits to the very consumers it seeks to protect. This

⁴ See Internet of Things: Privacy and Security in a Connected World, FTC Report (Jan. 2015) ("IoT Report"), available at <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>. The provision of Internet access services itself has changed, as long recognized by the FTC. See Broadband Connectivity Competition Policy, FTC Staff Report (June 2007), available at <https://www.ftc.gov/sites/default/files/documents/reports/broadband-connectivity-competition-policy/v070000report.pdf> (addressing net neutrality concerns and policy recommendations prior to reclassification of Internet access services to a Title II service, including discussions of new entrants to the marketplace and consumer protection issues of privacy and security).

⁵ Cross Device Tracking, An FTC Workshop (Nov 16, 2015), information available at <https://www.ftc.gov/news-events/events-calendar/2015/11/cross-device-tracking>; Data Brokers: A Call for Transparency and Accountability, FTC Report (May 2014), available at <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>.

⁶ For example, Internet traffic is becoming increasingly encrypted, thereby limiting visibility into user activity. Additionally, many users connect from multiple devices served by multiple ISPs preventing any one ISP from gaining a "comprehensive" view into user activity. See Peter Swire, Justin Hemmings, & Alana Kirkland, Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others, 3 (Feb. 29, 2016) available at <http://peterswire.net/wp-content/uploads/Online-Privacy-and-ISPs.pdf>.

⁷ The FTC has cited to its principles in hundreds of successful information privacy and security actions, including actions against many of the most well-known companies in the Internet ecosystem like Google, Facebook, and Twitter. See FTC, Privacy & Data Security Update (2015), available at <https://www.ftc.gov/news-events/blogs/business-blog/2016/01/2015-privacy-data-security-update>. Additionally, the FTC report released last year concluded, again after holding workshops and seeking comment, that the notice and choice approach included in the 2012 Privacy Report "applies equally to the Internet of Things." See IoT Report at 40.

⁸ Interview by Gary Shapiro, CEO, Consumer Technology Association, with Thomas Wheeler, Chairman, FCC, Las Vegas, NV (Jan. 6, 2016); see also Chairman Wheeler statement in response to question at the FCC Oversight Hearing before the House Energy and Commerce Subcommittee on Communications and Technology, July 28, 2015, transcript at 107-08 ("[W]e work closely with the FTC[,] we will do our best to harmonize so that there is a common set of concepts that govern privacy.").

Comment identifies areas of consistency with the FTC enforcement and guidance, and highlights those areas of the proposed rule that are inconsistent with the FTC approach. Before finalizing your proposed rules, I encourage you to take the time necessary to carefully evaluate how those rules would affect business practices, especially where they are in contrast with how those business practices would be treated under the FTC framework. A truly consistent approach is vital for the continued growth and economic benefits of the Internet, and serves to avoid consumer confusion and misunderstanding regarding the uses of their data. Most importantly, it vigorously and properly protects consumer privacy.

Fundamentals of the FTC Framework

The 2012 FTC Privacy Report (“FTC Report”) presents a single, yet comprehensive, framework of three principles that companies should consider and implement when collecting, using, and maintaining consumer data. These principles are:

Privacy by Design: This principle calls on companies to provide reasonable security for consumer data, to limit the collection of consumer data to what is consistent in a context of a particular transaction, to implement reasonable data retention and disposal policies, and to maintain reasonable accuracy of consumer data.⁹ Recognizing that one size does not fit all, the FTC offers concrete yet flexible guidelines for companies to follow. For example, with respect to data security, the FTC outlines a multi-layered approach: it calls for better consumer and business education, highlights data security improvement initiatives by individual companies, and asks Congress to enact federal data security and breach notification legislation.¹⁰

Consumer Choice: This principle encourages companies to offer consumers the ability to make decisions about the collection and use of their personal data at a relevant time and context. The FTC framework includes a tiered approach, based upon the sensitivity of the data being exchanged. For example, the FTC recognized that some collection and use practices do not necessitate consumer choice at all, including most first party marketing. Other practices, including the use of consumer information in a manner inconsistent with the context in which it was collected, require choice.¹¹ Only *two* practices, however, warrant a heightened level of consent: (1) using consumer data in a materially different manner than was disclosed to the consumer at the time the data was collected, or (2) collecting, using or disclosing “sensitive” data for marketing.¹²

⁹ FTC Report at i.

¹⁰ *Id.* at 25-26.

¹¹ *Id.* at 40-41.

¹² See *Id.* at 57-60; see also, the FTC's Children's Online Privacy Protection Rule, 16 C.F.R. § 312 (2013).

Transparency: In its third principle, the FTC encourages companies to increase the transparency of their information collection and use practices through easily-readable privacy statements, the provision of reasonable consumer access to certain information maintained about the consumer, and consumer education.

In addition to creating a comprehensive framework that encompasses both online and offline data collection and use, the FTC Report articulates the importance of applying its principles and the framework in a technology-neutral manner: “Any privacy framework should be technology neutral. ISPs are just one type of large platform provider [others are operating systems, browsers, and social media services] that may have access to all or nearly all of a consumer’s online activity.”¹³ The FTC reinforced this key conclusion after its December 2012 workshop on large platform providers, reiterating that government should avoid picking winners and losers, and instead should maintain a technology-neutral online privacy regime.¹⁴ As such, the FTC framework focuses on the sensitivity of the type of data collected and how those data are used. Such a consistent and holistic application of the principles is designed to provide consumers with privacy and data security protection across the Internet ecosystem and beyond.

Some Parts of the FCC’s Approach Reflect the FTC Framework

The FCC’s stated principles of transparency, consumer choice, and data security match the same principles at the heart of the FTC’s framework and other privacy regimes in the United States.¹⁵ Within those broad principles, the FCC’s Privacy NPRM also contains some specific proposals for implementation that are consistent with the FTC’s framework and approach. For instance, the proposal for broadband providers to ensure customers receive “clear and conspicuous notice of their privacy practices at the point of sale and on an on-going basis through a link on the provider’s homepage, mobile application, and any functional equivalent” is similar to FTC guidance.¹⁶ The FCC’s goal of standardizing the delivery of broadband privacy notices echoes the goals set in the FTC Report and the multi-stakeholder proceedings that preceded and followed. Likewise, the FCC’s call for prior notice and consent to consumers of

¹³ See *Id.* at 56.

¹⁴ See Maneesha Mithal, Associate Director, Division of Privacy and Identity Protection, Bureau of Consumer Protection, FTC, Closing Remarks in Washington, DC: The Big Picture Comprehensive Online Data Collection at 273(Dec. 6, 2012).

¹⁵ See Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Notice of Proposed Rulemaking, WC Docket No. 16-106 ¶ 2 (rel. April 1, 2016) (“Privacy NPRM”); FTC Report at i; 15 U.S.C. §§ 6801-6809 (“Gramm-Leach-Bliley Act”); Pub. L. No. 104-191, 110 Stat. 1936 (1996) (“HIPAA”).

¹⁶ Privacy NPRM ¶ 64; FTC Report at 61-64.

material changes to data collection and use practices is consistent with the FTC's framework and enforcement.¹⁷

The FTC and FCC share heightened concerns for:

- the collection of "sensitive" data for marketing purposes or sharing with third parties (although the FCC's proposal would include a very broad range of information that the FTC has never considered sensitive and would include practices, such as incidental collection and use, that would not be subject to heightened consent under the FTC framework);¹⁸ and
- the ability of any provider with access to "all or substantially all" of a user's online activities to comprehensively track the consumer's activities for marketing purposes, including a broadband provider's use of technologies such as "deep packet inspection" or similar technologies used by other large platform providers.¹⁹

The effect of the FCC's proposal would be to require opt-in consent for the use of such information or tracking technologies, which in theory is consistent with the FTC's approach, but in practice would go much further, as described below.

Additionally, the proposal to require that broadband providers take reasonable measures to protect customer data is consistent with the FTC approach, both in its 2012 Report and subsequent enforcement actions.²⁰ For example, the Privacy NPRM holds that the broadband Internet providers should take into account "the nature and scope of the BIAS provider's activities and the sensitivity of the underlying data" with respect to data security measures.²¹

At a high level, the FCC's stated goals sound generally reasonable and in line with consumer expectations and the FTC guidance. But at a more granular level, the FCC's proposed

¹⁷ See FTC, Privacy & Data Security Update (2015), available at <https://www.ftc.gov/news-events/blogs/business-blog/2016/01/2015-privacy-data-security-update>.

¹⁸ The FTC has a more limited view of what constitutes "sensitive" data that is more aligned with a new category of data the FCC's proposal calls "highly sensitive" data as discussed *infra* at pp. 7-8. *Id.* at 47; Privacy NPRM at ¶ 136. The FCC's broader definition results in a disproportionate amount of data being subjected to heightened opt-in requirements. Additionally, while the FTC Principle calls for affirmative express consent before collecting sensitive data for certain purposes, including first party marketing, is also recognizes that "the risks to consumers may not justify the potential burdens on general audience businesses that *incidentally collect* and use sensitive information." *Id.* at 47. In the current context, broadband providers must collect all kinds of information in order to provide service.

¹⁹ Privacy NPRM ¶¶ 264-266; FTC Report at 55.

²⁰ *Id.* at ¶ 217; FTC Report at 23-30; Start with Security – A Guide for Business – Lessons Learned from FTC Cases, (June 2015) at 11.

²¹ Privacy NPRM ¶ 217.

implementation of its own core principles appears in some tension with its own professed goals, and goes far beyond the FTC recommendations, as described below.

The FCC Proposal Parts Ways from the FTC and Other U.S. Privacy Regimes

The Privacy NPRM, if adopted as proposed, would result in a detailed set of burdensome data-privacy rules with no precedent in the FTC or other U.S. privacy regimes,²² and is inconsistent with the privacy obligations applied to the rest of the economy. Moreover, the NPRM does not identify any harms that necessitate rules that are different from the FTC framework. This divergence merits additional study and consideration.

Between the release of the Preliminary Staff Report in 2010 and the 2012 FTC Report, FTC staff conducted extensive “stress testing” where staff held scores of meetings both internally and with industry and consumer groups alike to test the proposed rules against specific use cases in order to determine whether the desired outcome was achieved. As a result of these meetings, changes were made to account for normal business operations and to encourage innovation in new products and services. Similarly, the FCC should conduct meetings to fully understand the effects of its proposed requirements before potentially causing disruption to an entire industry and the Internet ecosystem, particularly in areas where the FCC relies on FTC precedent in contextually inaccurate ways, as discussed below.

Scope

The FTC framework does not govern the notice, use, disclosure, security, or notification of breach of anonymized or de-identified individual data, as long as such data cannot be reasonably linked to a particular consumer, computer, or device. The FTC excluded de-identified data because it does not present a risk to consumer privacy or security. The FCC’s proposal appears to confuse the FTC’s guidance on the “reasonable linkability” standard and the appropriate steps companies can take to minimize such linkability with a standard for aggregation, which is but one way to de-identify data.²³

²² Indeed, the proposed FCC rules are more akin to and actually go beyond an EU-like privacy structure, with a broad scope, rigorous notice and consent requirements, and a strong burden of proof for any processing of personal data. This approach can only work comprehensively and it should be done at the direction of Congress. If the proposal moves forward as currently drafted, it is likely to yield fragmented rules that are incompatible with all other industries.

²³ Although the NPRM proposal attempts to use the FTC’s definition of de-identified data, it appears to add a further requirement that those data also be aggregated to be exempt from the requirements of the proposed rule. Privacy NPRM ¶ 154. When drafting the Report, the FTC was concerned with linkability in light of public re-identification attacks; however the FTC was clear that companies should be provided with flexibility in determining how to ensure de-identified data stays protected. FTC Report at 21; *see also, e.g.*, Michael Barbaro & Tom Zeller, A Face Is Exposed for AOL Searcher No. 4417749, N.Y. Times (Aug. 9, 2006), which was a topic of much discussion among FTC Commissioners and staff.

Application

In the 2012 Report, the FTC stated:

[A]ny privacy framework should be technologically neutral. ISPs are just one type of large platform provider that may have access to all or nearly all of a consumer's online activity. Like ISPs, operating systems and browsers may be in a position to track all, or virtually all, of a consumer's online activity to create highly detailed profiles.²⁴

This point was further emphasized in the FTC's December 2012 workshop, "The Big Picture: Comprehensive Online Data Collection," in which consumer and industry advocates alike expressed support for a technology-neutral approach.²⁵ After conducting the workshop and considering the comments, the FTC did not alter the 2012 Principles or guidance, and it did not propose different rules for such providers. Moreover, since 2012, the precipitous rise of encryption and proliferation of networks and devices have limited the scope of customer data available to broadband providers, while other companies operating online have gained broader access to consumer data across multiple contexts and platforms.²⁶ Today, more than 49% of Internet traffic is encrypted, and an estimated 70% will be encrypted by the end of this year.²⁷ This sea change in only four years' time drives home the importance of technology neutral privacy rules. Because the FCC is not in a position to dictate privacy rules for the entire Internet ecosystem, it should strive to harmonize its proposed rules with the FTC approach and other U.S. privacy laws, and carefully consider the consequences of failing to do so.

Choice and Context

At the time the FTC released its 2012 Report, there was heightened concern regarding the "invisible" collection and use of consumer data across the Internet generally, but especially with respect to collection and use by entities that had no direct (or even indirect) relationship with the

²⁴ FTC Report at 56.

²⁵ Maureen Ohlhausen, Commissioner, FTC, Remarks in Washington, DC: The Big Picture Comprehensive Online Data Collection at 134 (Dec. 6, 2012) ("Government privacy regulation shouldn't pick winners and losers based on technology or business models, particularly in a rapidly evolving and expansive internet marketplace."); Christopher Calabrese, Legislative Counsel, ACLU, Panel in Washington DC: The Big Picture Comprehensive Online Data Collection - Consumer Attitudes about and Choice with Respect to Comprehensive Data Collection at 198 (Dec. 6, 2012) ("I think if you listen to all the areas where we agree, try to make it tech neutral and pass some general legal prohibitions that are protections that are based on these areas of agreement..."); Maneesha Mithal, Associate Director, Division of Privacy and Identity Protection, Bureau of Consumer Protection, FTC, Closing Remarks in Washington, DC: The Big Picture Comprehensive Online Data Collection at 273 (Dec. 6, 2012) ("Fourth area of consensus [from the participants in today's workshop] is the need for tech neutrality. We can't be picking winners and losers in this space.").

²⁶ Peter Swire, Justin Hemmings, & Alana Kirkland, *Online Privacy and ISPS: ISP Access to Consumer Data is Limited and Often Less than Access by Others*, at 3-4 (2016).

²⁷ *Id.* at 3.

consumer. The Framework was designed to apply to both first and third parties, but recognized that in some instances, “data collection and use [] is either obvious from the context of the transaction or sufficiently accepted or necessary for public policy reasons.”²⁸ Specifically, when a consumer does business with a company, there are certain uses of the consumer’s information by the company that do not require consumer choice because such use is consistent with “the context of the interaction between a business and the consumer.”²⁹ This implied consent covers uses and disclosures for product or service fulfillment, internal operations, most first party marketing, and more.³⁰ Although broadband providers have direct relationships with their customers, the FCC’s proposal takes a baffling departure from FTC guidance by treating them (and some of their affiliates) as third parties.³¹

Rather than narrowly tailoring a requirement for opt-in consent to truly “sensitive data,” the proposed rules would impose a broad opt-in requirement upon broadband providers for the use of a wide swath of consumer data for an extensive range of practices – *including practices for which the FTC requires no choice at all because implied consent is presumed*. In doing so, the NPRM completely ignores the critical context of the interaction between the consumer and the service provider, which would make consumers the losers in this policy choice.

The FTC would not require companies to provide any choice to present advertising to their own customers, except where that advertising was presented by tracking a user’s online activity across other companies’ websites or intentionally using sensitive information collected from its customers. Under the FCC’s proposal, however, any use of customer information that is not relevant to marketing a communications-related service would require opt-in consent from the customer.³² *Indeed, under one reasonable reading of the NPRM, a broadband provider would not be able to market its own non-communication-related products—like a home security system, cloud services, or music streaming—to its own customers without their prior opt-in consent, regardless of the marketing channel used and despite the fact that this type of first party*

²⁸ FTC Report at 36.

²⁹ Citing the Consumer Privacy Bill of Rights proposed by the White House, the FTC Report describes the “Respect for Context” principle as requiring “companies to limit their use of consumer data to purposes that are consistent with the company’s relationship with the consumer and with the context in which the consumer disclosed the data, unless the company is legally required to do otherwise. If a company will use data for other purposes it must provide a choice at a prominent point, outside of the privacy policy.” *Id.* at 39, n. 184.

³⁰ *Id.* at 36-37. The FTC lists “fulfillment, fraud prevention, internal operations, legal compliance and public purpose, and most first-party marketing” as “illustrative guidance regarding the types of practices that would meet the revised standard and thus would not typically require consumer choice.” *Id.* at 39. Note, however, that the FTC requires first parties to obtain consent for the intentional use of sensitive data and tracking “all or substantially all” Internet traffic when there are not enough choices in the marketplace. *Id.* at 47, 55-56.

³¹ Under the FTC approach, affiliates are considered first parties when the relationship is clear to the consumer – such as when a company offers home-security services with the same brand as its communications services. *Id.* at 41-42.

³² Privacy NPRM ¶ 221.

marketing is certainly consistent with consumer expectations. The FCC's opt-in requirement for any use of consumer information that is not related to communications services will quickly lose its meaning to consumers who are not expecting to be constantly bombarded with notices and requests for use of information.

For online tracking, *the FTC framework calls for a consumer opt-out in almost all cases, not an opt-in.*³³ The NPRM, by contrast, would require an opt-in without regard to the sensitivity of the data used in tailoring the advertising. The FCC's overbroad opt-in approach has the potential to stifle innovation and competition in the online advertising marketplace, and undermine benefits to consumers. As the FTC has recognized, the ability to effectively monetize online data has yielded astounding benefits.³⁴ Consistent with the FTC's technology-neutral approach, broadband providers should be able to use information in a manner consistent with consumer expectations and in a way that correlates to how the rest of the Internet ecosystem provides choice – on an opt-out basis. Requiring over-inclusive opt-in choice would unduly restrict broadband providers from participating in the same Internet marketplace the FTC has found to provide benefits to both consumers and competition.

Additionally, affiliates are considered first parties when the relationship is clear to the consumer – such as when a company offers services or products with the same brand as its communications services. The FCC's proposed rules appear to contain no such exceptions, and arguably would require anonymization of customer data before sharing with certain appropriate affiliates and service providers, absent a customer's opt-in consent, which could not possibly be the FCC's intent.

The FCC also proposes, perhaps inadvertently, to apply its formula for de-identification and aggregation in the context of marketing to an ISP's own customers – an activity which is exempt from consumer choice altogether under the FTC framework, making de-identification in this circumstance wholly unnecessary. Instead, under the FTC framework, de-identification avoids a consumer choice requirement.³⁵

The Privacy NPRM also departs fundamentally from FTC guidance and undermines the core principle of customer notice and choice by suggesting that it could be appropriate to prohibit broadband providers from offering discounted services in exchange for greater access to consumer data. Many of us may decide that the price to pay to avoid personalized advertising is

³³ Without regard to tracking, intentional use of sensitive data outside the context of the transaction would require affirmative express consent under the FTC framework. FTC Report at 47.

³⁴ See Big Data: A Tool for Inclusion or Exclusion?, FTC Report (Jan. 2016) at 5-6, *available at* <https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf>.

³⁵ FTC Report at 22 (stating data that is de-identified does not require choice because it is out of scope).

worthwhile, but so long as broadband providers provide sufficient information to enable an informed choice, consumers should be able to choose for themselves how to value privacy.

Ultimately, while the FCC Privacy NPRM attempts in principle to follow the framework set forth by the FTC, it goes farther by proposing measures that would target broadband providers selectively, without clear benefit to consumers.

Transparency

The FTC's framework calls on companies to increase the transparency of their data practices by providing consumers with clear privacy notices, reasonable access to their own data, and education. The FCC's proposal regarding consumer privacy notices is perhaps the most consistent section of the NPRM. However, flexibility in this regard has been the touchstone of FTC guidance.³⁶ When the FCC finalizes its rules, it should adopt a flexible approach, recognizing that companies often need to craft notices to consumers in new ways and through new channels to accommodate changing technologies and evolving consumer understanding of business practices.³⁷

Similarly, while both the FTC and FCC approach require clear consumer notice, the FTC calls for "clearer, shorter" notices to enable "better comprehension" of privacy policies (as well as standardized notices to enable comparison of privacy policies).³⁸ Unlike the Privacy NPRM's proposal, the FTC does not require any specific text or specific notice as to the use and disclosure practices of "each type of covered information,"³⁹ as this would lengthen and further complicate privacy notices.

Data Security and Breach Notification

The proposed data security provisions, requiring broadband providers to take reasonable measures to protect customer data, are consistent at a high level with the approach set out in the FTC Report, but their prescriptive and static nature are at direct odds with the Administration's Cybersecurity Framework, as implemented by NIST, which has been voluntarily adopted by a

³⁶ *Id.* at 62 (noting that while privacy policies should contain some standardized elements, "[p]rivacy statements should account for variations in business models across different industry sectors, and prescribing a rigid format for use across all sectors is not appropriate"); Mobile Privacy Disclosures Building Trust Through Transparency, FTC Report (Feb. 2013) at 13-14, *available at* <https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf> ("2013 FTC Mobile Transparency Report") (mobile transparency standards "are intended to be sufficiently flexible to accommodate further innovation and change").

³⁷ See 2013 FTC Mobile Transparency Report at 13-14.

³⁸ FTC Report at 61.

³⁹ Privacy NPRM at ¶ 83.

wide swath of the industry and reflects flexible and reasonable standards that accommodate changing threats.⁴⁰ In addition these requirements should be more narrowly tailored to customer information that carries a risk of harm to the customer in the event of a breach, and in no case should apply to simple IP addresses, MAC addresses, or individually de-identified or aggregate data. The NPRM's requirements for risk assessments and audits of non-sensitive information divert resources away from protecting truly sensitive information and maintaining the security of networks, which are critical infrastructure. Companies are better positioned to assess evolving risks to their systems; rules requiring specific processes or special treatment of certain data are often not adaptable to diverse and changing business models or technologies and quickly become outdated.

The proposed FCC breach notification rules would require broadband providers to notify consumers of a breach of broadly defined "customer proprietary information" no later than ten days after the discovery of a breach. Again, while the concept of breach notification is consistent with the approach the FTC and most states have taken, the proposed implementation is not consistent. In the NPRM, the Commission asks questions about what should trigger such notifications and what timing should be required. Both FTC precedents and state breach notification laws can be instructive on these points.

The FTC has long supported requirements for companies to notify consumers of security breaches in *appropriate* circumstances, such as when information has been compromised that can lead to harms such as financial loss or identity theft.⁴¹ It has advocated that "any trigger for providing notification should be sufficiently balanced so that consumers can take steps to protect themselves when their data is at risk, while avoiding over-notification, which may confuse consumers or cause them to ignore the notices they receive."⁴² To this end, it has been supportive of state laws that require notifications when there is a breach of information such as a consumer name coupled with financial account information or social security numbers, or usernames and associated passwords. In its current NPRM, the Commission should refrain from

⁴⁰ Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, National Institute of Standards and Technology (Feb. 12, 2014) *available at* <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>.

⁴¹ See, e.g., Prepared Statement of the FTC, Data Security: Hearing Before the H. Comm. on Energy and Commerce, Subcomm. on Commerce, Manufacturing, and Trade, 112th Cong. (June 15, 2011), *available at* <http://www.ftc.gov/os/testimony/110615datasecurityhouse.pdf>; Prepared Statement of the FTC, Protecting Social Security Numbers From Identity Theft: Hearing Before the H. Comm. on Ways and Means, Subcomm. on Social Security, 112th Cong. (Apr. 13, 2011), *available at* <http://ftc.gov/os/testimony/110411ssn-idtheft.pdf>; FTC, Security in Numbers, SSNs and ID Theft (Dec. 2008), *available at* <http://www.ftc.gov/os/2008/12/P075414ssnreport.pdf>; and President's Identity Theft Task Force, Identity Theft Task Force Report (Sept. 2008), *available at* <http://www.idtheft.gov/reports/IDTRReport2008.pdf>.

⁴² Prepared Statement of the FTC, on Discussion Draft of H.R. ___, Data Security and Breach Notification Act of 2015: Hearing Before the H. Comm. on Energy and Commerce, Subcomm. on Commerce, Manufacturing, and Trade, 114th Cong. (Mar. 18, 2015), *available at* https://www.ftc.gov/system/files/documents/public_statements/630961/150318datasecurity.pdf.

requiring broadband providers to over-notify consumers for any breach of “customer proprietary information,” as the FCC has proposed that term to be defined.

Even when notification is required, law enforcement may request a delay in such notification in order to advance its investigation. There may also be practical limitations as to how quickly an investigation can be completed, individuals can be identified, and required notifications can be prepared and sent. The FTC’s Health Breach Notification Rule requires companies to notify affected consumers “without unreasonable delay” and within 60 calendar days after the breach is discovered.⁴³ Under the most restrictive time requirements among the general state breach notification laws – there is currently a patchwork of 47 state laws – an entity is required to provide notice “as expeditiously as practicable and without unreasonable delay but no later than 30 days after determination of breach, consistent with time necessary to determine scope of the breach, identify individuals affected, and restore the reasonable integrity of the system,” and with a 15 day extension granted for “good cause shown.”⁴⁴ When finalizing its breach notification rules, the FCC should take these realities into consideration, rather than the peculiarities of its current CPNI security rules, which are in no way statutorily required.

The FCC Should Adopt the FTC and CFPB Unfairness and Deception Statements for Enforcement Actions

No matter the final rules adopted, the FCC should strongly consider incorporating into its rules the unfair or deceptive acts and practices standard applied by the FTC, Consumer Financial Protection Bureau (“CFPB”) and some State Attorneys General, which incorporates a harm or materiality requirement.⁴⁵

Early FTC enforcement of “unfair” acts and practices was sometimes met with criticism of the Commission’s failure to apply its unfairness criteria consistently and systematically. The Commission, in turn, issued a policy statement in 1980,⁴⁶ setting out the current test for unfairness, now codified, which requires that an act or practice must be one (1) that causes or is likely to cause substantial injury to consumers, (2) which is not reasonably avoidable by

⁴³ 16 C.F.R. § 318.

⁴⁴ Fla. Stat. § 501.171.

⁴⁵ See Section 5 of the Federal Trade Commission Act codified as 15 U.S.C. § 45; Dodd-Frank Act, §§ 1002, 1031 & 1036(a), codified at 12 U.S.C. §§ 5481, 5531 & 5536(a); see e.g., Nev. Rev. Stat. § 598.0923(2) (defines deceptive trade practice as “knowingly fail[ing] to disclose a material fact in connection with a sale of goods or services”); Ariz. Rev. Stat. § 44-1522(A) (defines unlawful practices as “[t]he act, use or employment by any person of any deception, deceptive or unfair act or practice, fraud, false pretense, false promise, misrepresentation, or concealment, suppression or omission of any *material fact* with intent that others rely on such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise whether or not any person has in fact been misled, deceived or damaged”) (emphasis added).

⁴⁶ FTC Policy Statement on Unfairness (Dec. 17, 1980), available at <https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness>.

consumers themselves, and (3) not outweighed by countervailing benefits to consumers or to competition.⁴⁷ Similarly, the FTC holds an act or practice to be deceptive when: (1) the act or practice misleads or is likely to mislead the consumer; (2) the consumer's interpretation is reasonable under the circumstances; and (3) the misleading act or practice is material.⁴⁸

To my mind, the FTC has come to view these clear standards as liberating, and as a benefit rather than a detriment to consumer protection enforcement. The FTC's hundreds of successful privacy actions illustrate that the standards do not undercut an agency's ability to prevail against bad actors in enforcement actions. Rather, the materiality and harm standards help to focus an agency's limited enforcement resources on those practices directly impacting actual consumers. For this reason, those of us at the FTC were pleased to see Congress build the FTC unfairness and deception standards into the CFPB's enforcement mandate through the Dodd-Frank Act.⁴⁹ The FCC should consider doing the same in its broadband privacy and data security rules.

Conclusion

As the FCC formalizes the privacy and data security rules, it should hold broadband providers to the same robust privacy standards to which the FTC successfully held them for many years—and to which the FTC still holds all other companies. A truly consistent approach will ensure a comprehensive, technology-neutral privacy framework that provides consumers the strong protection and choices they need and deserve, while reducing consumer confusion regarding what protections apply. At the same time, it will promote the types of competition and innovation that fuel our economy. For all these reasons, my own view is that the FCC should adhere as closely as possible to the FTC's time-tested and proven approach.

Sincerely,


Jon Leibowitz

cc: Ruth Milkman, Chief of Staff to Chairman Wheeler
Matthew DelNero, Chief, Wireline Competition Bureau
Jonathan Sallet, General Counsel
Phil Verveer, Senior Counselor to Chairman Wheeler
Lisa Hone, Associate Bureau Chief, Wireline Competition Bureau

⁴⁷ 15 U.S.C. § 45(n) (2011) (codified by Congress in 1994); see also *FTC v. Wyndham Worldwide Corp.*, No. 14-3514, 2015 WL 4998121 (3d Cir. Aug. 24, 2015) at *5.

⁴⁸ See FTC Policy Statement on Unfairness (Oct. 14, 1983), available at https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.

⁴⁹ See Prohibition of Unfair, Deceptive, or Abusive Acts or Practices in the Collection of Consumer Debts, CFPB Bulletin (July 10, 2013), available at http://files.consumerfinance.gov/f/201307_cfpb_bulletin_unfair-deceptive-abusive-practices.pdf.