Testimony of

Jon Leibowitz

Co-Chairman, 21st Century Privacy Coalition

on

"FCC Overreach: Examining the Proposed Privacy Rules"

before the

House Energy & Commerce

Subcommittee on Communications and Technology

June 14, 2016

Chairman Walden, Ranking Member Eshoo, other distinguished Members of the Subcommittee, thank you for inviting me to testify at this important hearing. My name is Jon Leibowitz and, along with former Representative Mary Bono, I serve as co-chair of the 21st Century Privacy Coalition.

Our group is comprised of the nation's leading communications companies, which have a strong interest in bolstering consumers' trust in online services and confidence in the privacy and security of their personal information. We believe that consumers should enjoy the same robust protections throughout the internet ecosystem. I offer testimony today regarding the FCC's ongoing broadband privacy rulemaking on behalf of our group.

As consumers' online activity grows in size and scope, it is more important than ever for internet companies to protect us against hackers and disclose how they use our personal data. Since the internet's inception, the Federal Trade Commission ("FTC") has been the main privacy cop enforcing these essential consumer protections. But last year, the FTC's sister agency—the Federal Communications Commission ("FCC")—reclassified Internet Service Providers ("ISPs") as common carriers subject to Title II of the Communications Act, removing ISPs from the FTC's jurisdiction. Having assumed sole jurisdiction to protect consumer privacy in the ISP market, the FCC is currently engaged in a rulemaking to set out a privacy framework for ISPs.

The 21st Century Privacy Coalition was encouraged by FCC Chairman Wheeler's stated aim to craft the proposed broadband privacy rules in a manner "consistent with [the] FTC's thoughtful, rational approach," and with the core principles of the 2012 FTC Privacy Report: privacy-by-design, choice, and transparency. Our group believes that an FCC rulemaking consistent with the FTC's privacy framework would ensure that privacy enforcement remains both robust and technology neutral—that is, based on the sensitivity of data collected and how that data is used, rather than on the type of entity collecting the data.

Unfortunately, while some parts of the FCC's proposed rules are consistent with the FTC approach, in many important areas, the rules deviate sharply from that approach. The FCC has proposed 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 such rules seek to protect. Yet the FCC has failed to identify any harms or particular problems posed by ISPs that necessitate a divergence from the effective privacy framework that has applied to ISPs for years.

The FCC's proposed rules do not reflect the economic and technological realities of the internet ecosystem, in which myriad entities have access to and use consumers' online information to provide advertising-supported content and services and a wide array of customized capabilities and offerings. Data-driven insights and offerings are a key driver of the growth of the internet economy and the source of considerable innovation and benefits for consumers, but the FCC's proposed rules will make it much harder for ISPs to deliver these benefits, particularly compared to other online entities.

In fact, ISPs are new entrants in the online advertising market, where ten companies hold seventy percent of the market. The proposed rules would curtail ISPs' ability to enter that market and provide sorely needed competition.

The proposed rules also threaten to create not only consumer confusion, but also frustration and disruption of their online experiences. And, as a recent survey from the Progressive Policy Institute demonstrates, consumers overwhelmingly agree that "[a]ll companies collecting data online should follow the same consumer privacy rules so that consumers can be assured that their personal data is protected regardless of the company that collects or uses it." In addition, because the United States has highlighted the FTC's approach to privacy in its negotiations with the European Union regarding cross-border data transfers, including the so-called Privacy Shield, there are concerns on both sides of the Atlantic that FCC divergence from the FTC privacy framework could undermine the Privacy Shield in the European Court of Justice as well as other US international privacy negotiations.

A truly consistent approach is critical to the continued growth of the internet, to avoiding consumer confusion and misunderstanding regarding the uses of their data, as well as to permitting innovation to continue to flourish. The FCC's approach, as currently drafted, fails to achieve these goals.

The FTC Approach

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 worked to ensure both that consumer privacy is safeguarded while providing companies with the flexibility to use data in ways that benefit consumers and foster competition and innovation.

The FTC has a proven track record of success, built on robust enforcement, including over 400 successful privacy enforcement actions; occasional regulation such as 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," 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. Indeed, when the FTC published its comprehensive Privacy Report in 2012, its approach received praised from many consumer and privacy groups and some criticism from businesses. For example, the privacy organization Electronic Frontier Foundation praised the FTC for "creat[ing] strong guidelines for protecting consumer privacy choices," while the Information Technology and Innovation Foundation criticized the FTC, raising concern about "important trade-offs and costs" associated with the FTC framework.

In the four years since the publication of the Privacy Report, in which there have been continued developments in the way consumers access and use the internet itself, the FTC has held more workshops and issued additional reports and guidance tailored to specific sectors, technologies and practices to account for changes in the services offered over the internet, and in the data collection and tracking technologies used by various entities within the internet ecosystem. Despite these changes, the framework established in 2012 and the principles within the framework not only remain the same, but are even more resonant.

The 2012 Privacy Report presents a single, comprehensive framework that companies should consider and implement when collecting, using, and maintaining consumer data. These principles are:

1) *Privacy by Design*: calling 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;

2) *Consumer Choice*: encouraging companies to offer consumers the ability to make decisions about the collection and use of their personal data in a timely and contextual manner; and

3) *Transparency*: encouraging companies to increase the transparency of their information collection and use practices through easily-readable privacy statements and consumer education.

The FTC furthers these principles through robust enforcement rather than prescriptive regulation. It goes after companies when they break their privacy commitments to consumers or take actions that cause consumers real harm. This approach is flexible and promotes high-tech innovation, and it has held hundreds of companies, large and small, accountable when they cause real harm to consumers without countervailing benefits to consumers or competition.

Importantly, in addition to creating a comprehensive framework for both online and offline data collection and use, the FTC Report highlighted the importance of a technology-neutral approach to privacy: "Any privacy framework should be technology neutral." In other words, privacy enforcement should not depend upon the type of company using or collecting consumer data or the particular technology being used to do so. Indeed, the FTC specifically examined the question of whether large platform providers – a category that includes, but is not limited to, ISPs – should be subject to more stringent privacy obligations and, after a comprehensive inquiry, declined to take such a step. Instead, the FTC framework focuses on the sensitivity of the data collected and how those data are used. Consistent application of the principles is designed to provide consumers with clear and uniform privacy and data security protections, regardless of the particular product or service being used. The Administration has supported the FTC's policy of technology neutrality for privacy and the goal of a harmonized privacy framework for the entire internet ecosystem.

Finally, it is worth noting that the comments the FTC filed last week in the FCC's privacy proceeding, based on its 2012 Privacy Report, were unanimously supported by all three sitting commissioners. There is more legitimacy, and more enduring impact, from bipartisan regulatory action.

The FCC's Proposed Rules

The FCC's stated principles of transparency, consumer choice, and data security are framed as matching the principles at the heart of the FTC's framework and other privacy regimes in the United States and globally. Certain specific proposals in the NPRM are also consistent with the FTC approach. For example, the proposal for broadband providers to take reasonable measures to protect customer data is similar to FTC guidance and enforcement. The FCC's goal of standardizing the delivery of broadband privacy notices echoes goals set by the FTC. Likewise, the FCC's call for notice and consent to consumers of retroactive material changes to data collection and use is consistent with the FTC's framework and enforcement.

But, as the FTC staff noted in its comments last month on the FCC's proposal, which was approved by a unanimous, bi-partisan vote of the Commissioners, "the FCC's proposed rules, if implemented, would impose a number of specific requirements on the provision of [broadband] services that would not generally apply to other services that collect and use significant amounts of consumer data. This is not optimal."

In effect, the FCC proposal amounts to a *de facto* rejection of the FTC's determination that ISPs should not and need not be governed by a different set of standards with regard to how they handle broadband customer data. Instead, the FCC's proposed rules require a broad default opt-in requirement for the use and sharing of customer data, with limited exceptions, rather than narrowly tailoring its opt-in to the collection and use of sensitive customer data. The FCC is also much more restrictive with regard to first-party uses of information, which enable companies to improve their service and apprise their customers of offers and products of interest to them.

The breadth of data covered by the proposal, and the highly restrictive nature of the permissions regime employed by the FCC, creates a serious risk of unforeseen consequences that could adversely affect Internet capabilities and operations and disrupt consumer expectations. During the development of the 2012 Privacy Report, FTC staff addressed the potential impact of various proposals and ideas through extensive "stress testing," whereby staff held scores of meetings with industry and consumer groups alike to test particular components in order to determine whether the desired outcome would be achieved. The FCC should conduct similar meetings to fully understand the effects of its proposed requirements, which have the potential to disrupt not only the broadband industry, but the entire internet ecosystem, including competition in the online advertising market. What follows is a discussion of specific differences between the FCC proposed rules and the FTC approach.

Scope

The FCC's Notice of Proposed Rulemaking ("NPRM") applies onerous privacy and security requirements to sweeping a range of information that is not sensitive, such as IP or MAC addresses, as well as any other information that is "linked or linkable to" a user. This differs from the FTC approach, which sought to calibrate the framework's obligations to incentivize the strongest protections for the most sensitive data.

The FCC's treatment of de-identified data is particularly problematic. Because de-identified data does not present a risk to consumer privacy or security, 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 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. The NPRM would limit the exception for de-identified data only to data that is *both aggregated and de-identified*. By discouraging companies from investing in resources and tools to de-identify data, the FCC's proposal actually exacerbates – rather than mitigates – risks to consumer privacy.

Application

As noted above, in the 2012 Report, the FTC stated: "[A]ny privacy framework should be technologically neutral." There is widespread agreement on this point among consumer and industry advocates alike. At the FTC's December 2012 workshop, "The Big Picture: Comprehensive Online Data Collection," Maneesha Mithal, Associate Director of the Privacy Division at the FTC noted this consensus in her closing remarks, describing "the need for tech neutrality" as an area of consensus and emphasizing that "[w]e can't be picking winners and losers in this space."

Moreover, since 2012, the precipitous rise of encryption and the 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. For example, today, nearly half of Internet traffic is encrypted, dramatically limiting the information visible to ISPs, and an estimated 70% will be encrypted by the end of this year. This sea change in only four years' time drives home the importance of technology neutral privacy frameworks. 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 framework, and carefully consider the consequences of failing to do so.

Choice and Context

In its comments, FTC staff leveled criticism at the FCC's proposed consumer choice rules and recommended "that the FCC consider the FTC's longstanding approach, which calls for the level of choice to be tied to the sensitivity of data and the highly personalized nature of consumers' communications in determining the best way to

protect consumers." The FCC's proposed restrictive choice mandates that selectively target broadband providers prevent consumers from accessing new products and services and provide them no benefits, as well as potentially confuse them. They also, constrain ISPs' ability to compete with edge providers, and may discourage broadband investment in a manner contrary to the FCC's mandate to promote such investment.

Under the FTC framework, when a consumer does business with a company, there are certain uses of the consumer's information by the company for which consumer choice is implied because such use is consistent with "the context of interaction between a business and the consumer." This implied consent covers uses and disclosures for product or service fulfillment, internal operations, most first-party marketing, and more. Opt-in consent is limited to truly "sensitive data" and technologies that use "all or substantially all" customer data. The FTC framework calls for a consumer opt-out for almost all online tracking, not an opt-in. The FCC proposal is a vast departure from this guidance.

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 or disclosure 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 consent is implied. In doing so, the FCC's proposed rules disregard the context of the interaction between the consumer and the service provider. In today's economy, a company's relationship with its customers involves more than just providing service, but also requires understanding the ways in which services are used, identifying areas for improvement, and making consumers aware of product offers and enhancements that may interest them. By ignoring the balance between privacy and data-driven insights and innovation, the FCC's approach actually makes consumers worse off.

The FTC does 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. Indeed, under one reasonable reading of the proposed rules, 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 marketing is certainly consistent with consumer expectations.

The FCC's overbroad opt-in proposal 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 to consumers. 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. 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.

The FCC's NPRM also departs fundamentally from FTC guidance and questions 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 worthwhile, and 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.

The application of a broad opt-in for non-sensitive information as proposed by the FCC would create an isolated privacy regime for ISPs that bears little correlation with consumer data practices used in virtually every other sector. Deviating from the FTC's privacy framework overall, but especially from the FTC's emphasis on determining consumer choices based upon the sensitivity of the information, the context of a consumer's interaction with a company, and the consumer's expectations, will inevitably result in consumer confusion over illogical, disparate standards applied to the same set of data. Ultimately, while the FCC Privacy NPRM purports to be based significantly on the FTC privacy framework, it is far more restrictive in all of the above respects, without providing clear benefits to consumers.

Data Security and Breach Notification

The FCC's 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. However, their prescriptive and static nature are at direct odds with the Administration's Cybersecurity Framework, which has been voluntarily adopted by a wide swath of industry and reflects flexible and reasonable standards that emphasize business-driven responses and solutions to cyber threats over prescriptive regulatory measures. In addition, these requirements should be more narrowly tailored to apply to customer information that carries a risk of harm in the event of a breach.

The proposed FCC breach notification rules would require broadband providers to notify consumers of a breach of a very broad new definition of "customer proprietary information," much of which includes categories of data that do not pose a risk of harm to customers in the event of a breach, such as IP and MAC addresses and de-identified data. While the concept of breach notification is consistent with the approach the FTC and most states have taken, the proposed implementation by the FCC for innocuous data and to notify only ten days after discovery of the breach is very different and far more cumbersome.

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. The FTC 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."

The proposed rules, as currently drafted, would mandate over-notification. As the FTC staff notes in its comments on the proposed rule, the FCC should limit its notification requirement to a "narrower subset of personal information than 'customer proprietary information'" as the FCC has proposed that term to be defined in order to avoid over-notification to consumers. As the FTC staff asserts, "when consumers receive 'a barrage of notices' they could 'become numb to such notices, so that they may fail to spot or mitigate the risks being communicated to them.'" That is an outcome that the NPRM states that the FCC intends to avoid, but major changes are required to the breach notification provision to achieve this goal.

The proposed rules also contain an unrealistic timeline for customer notification. 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. 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." The FTC staff comments suggest an outer limit of between 30 and 60 days, which it views as "adequate for companies while protecting consumers." When finalizing its breach notification rules, the FCC should take these realities into consideration.

Conclusion

Mr. Chairman, thank you for holding this hearing today. Our Coalition commends you for devoting the Subcommittee's attention to this critically important issue. It is through the exercise of your crucial oversight authority that Congress can right the course of agency rulemakings that have veered away from mainstream policy goals.

As the FCC formalizes its privacy and data security rules, the agency 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 the rest of the internet ecosystem.

A truly consistent approach will ensure a comprehensive, technology-neutral privacy framework that provides consumers the strong protections and choices they need and deserve, while reducing consumer confusion regarding what protections apply. At the same time, a consistent approach will promote the types of competition and innovation that fuel our economy. Such an approach will also demonstrate that the United States views the FTC approach to privacy as the preeminent model for consumer

protection, which will help provide confidence to our trading partners that their own consumers will enjoy robust privacy protections under U.S. law.

As someone who was involved in more than a handful of rulemakings, it is important to point out that final rules are often more balanced than proposed ones. But the FCC's current proposal fails to achieve its own goals. Instead, it would create inconsistent standards across the internet, harm and confuse consumers, and undermine innovation. For all these reasons, the 21st Century Privacy Coalition's view is that the FCC should adopt the FTC's time-tested and proven approach.