Written Testimony of

Dean C. Garfield

President & CEO, Information Technology Industry Council (ITI)

Before the

U.S. Senate Committee on Commerce, Science, and Transportation

Hearing On

How will the FCC's Proposed Privacy Regulations Affect Consumers and Competition?

July 12, 2016

Written Testimony of

Dean C. Garfield
President & CEO, Information Technology Industry Council (ITI)

Before the

U.S. Senate Committee on Commerce, Science, and Transportation

Hearing on

How will the FCC's Proposed Privacy Regulations Affect Consumers and Competition?

July 12, 2016

Chairman Thune, Ranking Member Nelson, and members of the committee, thank you for the opportunity to testify today. I am Dean Garfield, President and CEO of the Information Technology Industry Council (ITI), and I am pleased to testify before your committee today on the important topic of how the Federal Communications Commission's (FCC or the "Commission") proposed broadband privacy regulations could impact consumers and competition.[1]

ITI shares the Commission's interest in, and respects its efforts to, protect the privacy of consumers of broadband internet access services. Privacy is of paramount concern to our member companies, many of whom are providers of information technology and internet services, because it is at the core of the trust relationship with our customers. Though the FCC lacks the authority to regulate our member companies who are the "edge providers" of "over the top" internet-based services referred to in its Notice of Proposed Rulemaking ("NPRM"), we are nonetheless concerned with the approach taken by the Commission in a number of respects. We therefore welcome your interest and engagement on this subject.

ITI is the global voice of the tech sector. We are the premier advocate and thought leader in the United States and around the world for the information and communications technology (ICT) industry, and this year we are pleased to be commemorating our centennial. ITI represents 61 of the world's leading ICT companies,[2] and we advocate globally for policies

[1] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, Notice of Proposed Rulemaking, FCC 15-138 (April 1, 2016) ("Broadband Privacy NPRM").

[2] For more information on ITI, including a list of its member companies, please visit: http://www.itic.org/about/member-companies.dot.

that advance U.S. leadership in technology, promote innovation, open access to new and emerging markets, protect and enhance consumer choice, and foster increased global competition. ITI's members comprise leading technology and innovation companies from all corners of the ICT sector, as well as companies using technology to fundamentally evolve their businesses, including wireless and wireline network equipment providers, computer hardware and software companies, mobile computing and communications device manufactures, internet and digital service providers, and network security providers. ITI's member companies are also at the forefront of developing next-generation wireless communications equipment, infrastructure, networks, and services, along with the content, applications, and new uses that will be enhanced as mobile service evolves and advances. In other words, many of our members are the "edge providers" referred to in the FCC's proposal.

Privacy is of paramount concern to our member companies. Protecting our customers' personally identifiable information (PII) and their privacy, along with providing robust security, are essential to earning citizens' trust in the global technology marketplace. Innovating to protect privacy and security and to strengthen consumers' trust in the global digital infrastructure and internet services are core to our companies' business practices and philosophies. Privacy is thus critical to our members' success, an essential component of our businesses, and impacts our ability to grow and innovate in a future heralding continued advances in the Internet of Things, Big Data, and beyond. Consequently, ITI has been a leading voice in advocating effective approaches to privacy, both domestically and globally.

The internet has thrived – and privacy has been protected – under the Federal Trade Commission's (FTC) approach to privacy, which is grounded in the Fair Information Practices Principles ("FIPPs"). This framework applies to all entities under the FTC's jurisdiction who collect and use consumer data. We believe the FCC's primary objective should be to closely harmonize with the existing FTC framework any Internet Services Provider (ISP) or broadband privacy rules it ultimately adopts. While the FCC has concluded that the regulation of Broadband Internet Access Services (BIAS) providers is uniquely within its purview following the FCC's decision to reclassify broadband as a Title II service, irrespective of whether that order is ultimately upheld in the courts, there is nothing in that decision that necessarily warrants a departure from the FTC's successful approach to privacy based on effective notice to consumers and a meaningful choice as to how their data is used. Unfortunately, the FCC intends to proceed in another direction, proposing a series of onerous privacy and data security rules that are out of step with established policy, law, and practice in this area.

I will focus my testimony on four areas: (1) The FCC's lack of legal authority to regulate ITI's companies, including "OTT" or "Edge" providers; (2) the inconsistency of the FCC's

proposed privacy regulations with consumer expectations; (3) the broader inconsistency of the FCC's proposed privacy regulations with existing privacy authorities, frameworks and enforcement regimes, as embodied in the FTC's well-established approach to privacy; and (4) ITI's concern that the proposed rules will establish negative precedents that will ultimately adversely impact consumers, businesses, and the global policy ecosystem.

On this latter point, I will highlight our concerns regarding how several of the specific rules proposed by the FCC are out of step with current law and practice, including: (1) the unreasonably short and inflexible breach notification periods; (2) the overbroad and unnecessary definition of personally identifiable information; (3) the overly burdensome consumer choice and consent framework; and (4) the prescriptive, inflexible data security requirements that are misaligned with current industry practice and federal and state policymaking.

The FCC Lacks the Authority to Regulate ITI's Companies

By and large, ITI's companies do not offer broadband internet access service as a core part of their businesses, and could not be categorized as such given the definitions for BIAS and BIAS providers in the Open Internet Order and these proposed broadband privacy rules.

Given this, ITI's companies are not subject to the FCC's jurisdiction under Title II, even after the FCC reclassified broadband internet access service as a telecommunications service under Title II, nor is there a valid legal argument which could subject our companies to Title II regulation under the Open Internet Order adopted last year.

The FCC specifically defines BIAS to mean "[a] mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all Internet endpoints, including any capabilities that are incidental to and enable the operation of the communications service, but excluding dial-up Internet access service. This term also encompasses any service that the Commission finds to be providing a functional equivalent of the service described in the previous sentence, or that is used to evade the protections set forth[.]" The FCC defines a "broadband Internet access service provider" as a person or entity engaged in the provision of broadband internet access service. Furthermore, the Commission specifically notes over-the-top services and service providers – a category into which many ITI member companies fit – are not broadband internet access service providers and were not captured under the Open Internet Order nor the Broadband Privacy Notice of Proposed Rulemaking. In fact, in the Open Internet Order the Commission went out of its way to emphasize that while broadband internet access service providers may offer over-the-top services, over-the-top providers of voice over internet protocol, internet protocol messaging services, and internet video providers are separate and distinct from broadband internet access

providers.

There are well-founded consumer, business, and economic reasons to rationalize why internet and IT services providers and network operators including broadband services providers are treated differently from a regulatory perspective. From a consumer choice standpoint, there are significant differences between OTT services providers or internet companies and BIAS providers. Consumers have traditionally had limited choices when it comes to choosing a BIAS provider for purposes of acquiring broadband or internet service. Indeed, broadband access itself is increasingly considered a fundamental right by many – it is necessary for basic services at all levels of government, educational opportunities, workforce opportunities, and numerous other basic needs. Once a consumer has a broadband connection, however, consumers can easily choose amongst many different OTT applications and internet service options, including choosing to discontinue one service, switch to another service, or subscribe to several comparable services simultaneously. And certainly, these types of services are not considered a right; rather, inherent in their multiplicity is the very concept of choice.

Additionally, there are significant differences between the business and economic models of ISPs and edge service providers. Internet companies providing content or services to consumers have different economic interests than ISPs. For instance, consumers typically pay for broadband services whereas much of the content and many of the services provided to consumers over the internet are ad-supported and thus provided to consumers free of charge. This relationship has not changed under the reclassification of broadband internet access service, nor has the legal and regulatory authority governing that relationship. Internet companies' relationship with their customers and the use of their customers' data has been and remains subject to FTC enforcement.

ITI's perspective on this matter is solely driven by years of experience in engaging with, and helping to develop, the domestic and global privacy policy frameworks we operate under today.

The FCC's Proposed Data Privacy Rules are Inconsistent with Consumer Expectations

As I described above, ISPs and edge providers are very differently situated from the perspectives of consumers both in terms of how their business models are implemented and in terms of the regulatory reach of the FCC. The fact that there are fundamental differences between ISPs and internet companies and those differences have historically given rise to different regulatory and enforcement regimes, however, does not give license to creating data privacy rules that are inconsistent with consumer expectations. Rather, how the FCC regulates

data should be determined by what is best for consumers, whether consumers are suffering identifiable and quantifiable harms, and whether gaps exist in the current regulatory and enforcement regime.

Additionally, sound privacy policy for one entity in the internet ecosystem should be sound policy for all others. The FCC has not made the case to justify the type of expansive and prescriptive regulatory regime contemplated by the NPRM – a significant departure from the current FIPPs-based approach undertaken by the FTC.

Fundamentally, if the FCC seeks to ensure the goals articulated in the NPRM of protecting consumer privacy, it must carefully weigh consumer interests and expectations. Unfortunately, the proposed regulations contain no indication that consumer interests - in particular whether they are suffering any harm under the current regulatory approach - demand expansive new regulations in this area. Consumers have embraced today's thriving internet, fueled by responsible data practices governed by the existing regulatory framework, and they have come to expect a seamless online experience across multiple devices that delivers convenience while also protecting their privacy. The current online ecosystem subsidizes online offerings that consumers value, promotes innovation, and grows the economy. There is simply no record of consumer harm supportive of the FCC's proposal for such restrictive regulations. In other words, the FCC's proposal should embrace a more measured approach. Consumer expectations have also not been factored into the FCC's analysis. Indeed, as Commissioner O'Reilly points out in his dissent, "there is no need for the Notice to describe consumer expectations because it is irrelevant to the FCC's analysis."

The FCC's Proposed Data Privacy Rules are Inconsistent with Existing Privacy Frameworks and Enforcement Regimes

We believe what would most benefit consumers is an approach that is consistent with existing privacy frameworks grounded in the FIPPs and consistent with existing privacy enforcement regimes. Consumers and industry benefit when one agency takes the lead on privacy regulation and enforcement because regulatory consistency permits continued innovation without bias among sectors. The FTC has a long history of addressing and enforcing privacy-related issues across industries. Indeed, the FTC has shown much leadership over the years as the enforcer on digital ecosystem issues, for both technical and legal reasons, and it remains well-situated to provide such leadership into the future.

Specifically, existing voluntary self-regulatory standards supported by FTC enforcement are the appropriate tool to govern the dynamic and interrelated online content and advertising ecosystem. Currently, online data collection and use are governed by robust industry self-

regulatory regimes that subject the industry to the jurisdiction of the FTC and state attorneys general. These regimes are regularly updated to reflect new business models, which reflect the responsible data practices so essential for the continued success of the internet economy. Enforceable, voluntary, self-regulatory codes remain best suited to promote consumer privacy protections while allowing these legitimate data practices to flourish.

Further, the FTC's enforcement authority provides effective legal safeguards for online data practices. In addition to industry self-regulation, the FTC robustly enforces consumer privacy and data security standards using its authority to address "unfair or deceptive acts or practices" under Section 5 of the FTC Act. The FTC has used this authority to enforce company commitments to customers, to comply with industry self-regulatory requirements, and to protect consumers from harmful practices. State attorneys general typically follow FTC positions to actively enforce similar laws at the state level. These legal frameworks already provide consistent, meaningful consumer protections which can apply across industries, including to the practices the FCC now seeks to regulate. There is no need to create a new framework such as that proposed by the FCC because the FTC has well-established principles in this area.

Nonetheless, if the FCC is ultimately found to possess the requisite authority to regulate broadband privacy and follows through on its intent to do so, it should make certain that any such efforts are consistent with existing robust privacy frameworks and enforcement authorities, particularly those of the FTC. One way to ensure this sort of consistency is for the FCC to work closely with the FTC to harmonize its privacy rules for broadband ISP consumers with the framework that protects consumers of those online businesses or services falling under the jurisdiction of the FTC. In addition, the FCC and FTC should work closely together to help the communities within their purview - broadband ISPs and businesses providing service over the internet, respectively - to clearly understand the applicable rules to enable good faith compliance.

The FCC's Privacy Proposal is Out of Step with Current Law and Practice, and would Establish Precedents that Will Negatively Impact Consumers, Companies, and the Internet Ecosystem

Rather than adopt a regime aligned with the FTC's well-established approach to privacy, the privacy regime proposed by the FCC in the NPRM departs from the FTC framework in significant and material respects. We are particularly concerned that the prescriptiveness of the proposed regulatory approach could have precedential effects that would negatively impact the rest of the internet ecosystem, including the tech sector. While it is hard to say for certain what the implications on other sectors will be if the FCC moves forward with the NPRM and adopts standards that diverge from those the FTC has already established for customer

information, we believe the existence of multiple sets of privacy rules will, at a minimum, send a troubling message to governments and businesses internationally. Additionally, I'd like to point out four specific components of the FCC's proposal that are out of step with currently established policy and practice and raise significant concerns for both consumers and businesses.

The Breach Notification Periods are Unreasonably Short and Inflexible. The FCC proposes extremely short data breach notification periods in the NPRM – entities suffering a breach would be required to provide notice within seven days to the Commission, FBI, and Secret Service, and within 10 days to customers (NPRM ¶ 75), without regard to whether the breach creates a significant risk of customer harm. Such notices would need to be provided regardless of whether a breach is malicious or inadvertent, which is an element in determining whether a risk of harm exists (NPRM ¶ 75).

First, the FCC's data breach proposal fails to include a risk analysis, and therefore will contribute to notice fatigue at best or incite unnecessary panic at worst. Additionally, the proposal fails to account for breaches of data that are rendered not actionable through technology, such as encryption, or for inadvertent but innocent breaches, such as an employee accidentally opening the wrong file. Notifying individuals that their information has been compromised is an important step that enables them to take protective measures. Notification to consumers, however, is not productive if all data breaches result in notifications. If over-notification becomes commonplace, consumers will have difficulty distinguishing between notices and determining which ones warrant them to take action. Notification should be made to consumers if an organization has determined there is a significant risk of identity theft or financial harm. Upon receipt of such a notice, consumers can then implement measures to help avoid being financially damaged.

Second, the proposal does not afford organizations adequate time to remediate any discovered vulnerabilities or to conduct thorough investigations to ascertain the nature and scope of any breach before notifying customers or government agencies of a breach of data. Unless vulnerabilities are addressed prior to making the breach incidents public, organizations and their customers are susceptible to further harm by wrongdoers. Because the NPRM does not afford organizations adequate time to investigate the scope and nature of breach incidents, the NPRM not only encourages over-notification by organizations, but it creates a standard of notification that would be counterproductive should the alleged breach prove a false alarm or if the breach does not create a significant risk of identity theft. A tremendous amount of forensics, decision-making, and clerical and legal work is required before ascertaining the

nature and scope of a breach, assessing the risk of harm, or in determining the appropriate form of notification based on the organization's relationship with the effected customer.

More fundamentally, the FCC proposes to regulate breach notification in a way that is contrary to the existing state notification regimes and the proposals under consideration by Congress. Recognizing the sophistication of today's hackers and the challenging nature of a post-data breach forensic investigation, a breach notification regime must provide realistic, flexible, and workable time requirements. ITI has long advocated for Congress to establish a uniform but flexible approach to data breach notification that notifies customers where there is a significant risk of identity theft or other financial harm. Such a uniform approach not only eases compliance burdens for businesses, but it reduces or eliminates confusion for consumers.

The Proposed PII Definition is Overbroad and Unnecessary. The FCC proposes to define PII as "any information that is "linked or linkable to an individual." (NPRM ¶ 60). This is an overly broad definition that subsumes the entirety of the Customer Proprietary Network Information ("CPNI") category that the FCC proposes to expand elsewhere in the NPRM. As a result, both the proposed PII and CPNI definitions expansively include data elements that have never before been considered PII under U.S. law, such as internet protocol addresses or other unique identifiers necessary for the functioning of connected internet devices, application usage data, persistent online identifiers (cookies), and internet browsing history – data that is highly unlikely to contribute to a risk of concrete harm such as identity theft. (NPRM ¶¶ 62-63).

First, it is unclear why the Commission endeavors to define PII at all, rather than just focusing on the CPNI data clearly within its statutory ambit. Further, the Commission acknowledges that BIAS providers may not actually collect all of the categories of information included within the proposed expansive definitions, yet the FCC proposes to regulate the collection of such data anyway. The potential unintended consequences of these overly and unnecessarily broad definitions are quite concerning, particularly since many of the types of data captured by the proposed definitions are integral to providing internet services to consumers, including securing internet transactions.

Exhibiting some awareness of the potential unintended consequences that could flow from such a broad PII definition, the FCC proposes a number of exceptions to the definition of PII. For example, the NPRM exempts from the definition of PII data collected by entities "to protect themselves or others from cybersecurity threats or vulnerabilities." (NPRM ¶117). We are concerned this exception may not be nearly broad enough to adequately help protect the internet ecosystem. To illustrate, the definition suggests that companies would only be allowed *to collect* such information to counteract specific threats. This belies the reality that some of this information, such as unique IDs, must be collected *and shared* by companies as part of

their cybersecurity risk management programs in order to prevent cybersecurity intrusions from happening. Indeed, the trajectory of federal policymaking in this area over the past several years has been to encourage both continuous monitoring by organizations and the sharing of cybersecurity threat information to counteract cyber threats. The approach here is illustrative of the overall flawed approach to, and treatment of, PII in the FCC's proposal.

The Proposed Consumer Choice and Consent Framework is Overly Burdensome and Restrictive. The consent standard proposed by the FCC is both overly burdensome and restrictive. Generally, the FCC has proposed to restrict most collection, use, and disclosures of data with an "opt-in" consent standard, which it acknowledges may cause "notice fatigue" for consumers (NPRM ¶141). The Commission further acknowledges the "burden of [their] proposed customer choice framework" on businesses, particularly on smaller entities (NPRM ¶151). The proposed choice framework is also out of step with current policy and practice.

Experience shows that an opt-out or implied consent standard is an effective mechanism to effectuate consumer privacy preferences with respect to non-sensitive online data while allowing legitimate practices, including advertising, to continue. We urge the FCC to follow the FTC approach of permitting an opt-out approach for use of consumer data in most instances, with an opt-in approach reserved for uses of the most sensitive consumer data.

The Proposed Data Security Requirements are Prescriptive, Inflexible, and Misaligned with Both Industry Approaches and Federal Cybersecurity Policies. In the NPRM, the FCC proposes both general data security requirements for BIAS providers and "specific types of practices they must engage in to comply with the overarching requirement." (NPRM ¶167).

While the Commission acknowledges any proposed security requirements must "allow for flexibility for practices to evolve as technology advances," and claims it does not propose "to specify technical measures for implementing the data security requirements," (NPRM ¶176), it nonetheless proposes a series of increasingly prescriptive security requirements. For example, the Commission proposes to not only require regular Graham-Leach-Bliley-like risk assessments (NPRM ¶180) at a frequency to-be-determined (NPRM ¶183), but it also asks whether the FCC should prescribe specific risk-management requirements on BIAS providers, and how the risk assessments themselves should be conducted. (NPRM ¶182) These proposed requirements contradict existing cybersecurity public policy - such as that embedded in the Framework for Improving Critical Infrastructure Cybersecurity ("Cybersecurity Framework") - that risk management is a continuous process demanding flexibility in order to provide reasonable protections in light of the nature and scope of the activities of a given company, including the sensitivity of the data it handles, its threat profile, and the size and complexity of the relevant data operations of the company. Another example can be found in the series of

proposed specific authentication measures the Commission proposes to prescribe (NPRM ¶¶ 191 - 200).

Indeed, the structure of the entire security section appears contrary to many of the core concepts of risk management (e.g., voluntariness, flexibility, etc.) as throughout the NPRM the Commission asks a series of "should we require this" and "should we require that" questions. This is a fundamentally flawed approach, out of step with the approach embodied in the Cybersecurity Framework and the consensus standards and best practices included within. We agree with Commissioner O'Reilly's dissenting statement that the proposed prescriptive security rules are inconsistent with the voluntary approach embodied in the Framework and are indeed "alarming."

Conclusion

Members of the committee, ITI and our member companies are pleased you are examining the important issue of how the FCC's proposed broadband privacy regulations may impact consumers and competition. We share both the FCC's and your interest in protecting the privacy of consumers of broadband internet access services. As noted above, however, we are concerned with the approach taken by the Commission in a number of respects. We have raised our concerns directly with the Commission by submitting comments on the NPRM, urging the agency to reconsider promulgating data privacy rules that are inconsistent with consumer expectations or existing privacy authorities, frameworks and enforcement regimes, such as embodied by the FTC's longstanding approach to privacy. We appreciate the opportunity to reiterate these concerns today, including our belief that the privacy regime proposed by the FCC is out of step with current law and practice and would establish precedents that will negatively impact not only consumers but companies and the internet ecosystem as a whole. Please consider ITI a resource on these important issues moving forward, and do not hesitate to contact us with any questions regarding this submission.

Thank you for the opportunity to appear before you today.