Before the
National Telecommunications and Information Administration
U.S. Department of Commerce
Washington, D.C. 20230

In the Matter of	)	
	)	
Developing the Administration's	)	Docket No. 180821780-8780-01
Approach to Consumer Privacy	)	RIN 0660-XC043
	)	

COMMENTS OF USTELECOM

USTelecom – The Broadband Association (USTelecom)[1] is pleased to submit its comments in response to the National Telecommunications and Information Administration's ("NTIA") Request for Comments ("RFC")[2] seeking input on ways to advance consumer privacy while protecting prosperity and innovation. NTIA seeks comment on specific user-centric privacy outcomes and a set of high-level goals that describe the outlines of the ecosystem that should be created to provide those protections so that the Administration can determine the best path toward protecting individual's privacy while fostering innovation.[3]

USTelecom applauds the Administration for addressing potential changes to United States privacy policy that would provide clear and strong protections to all American consumers while allowing for continued innovation within the internet ecosystem. USTelecom views the outcomes outlined in the

[1] USTelecom is the premier trade association representing service providers and suppliers for the telecom industry. Its diverse member base ranges from large publicly traded communications corporations to small companies and cooperatives – all providing advanced communications service to both urban and rural markets.

[2] *See Notice Request for Comment, NTIA, In the Matter of Developing the Administration's Approach to Consumer Privacy*, 83 FR 187, 48600-48604, Docket No. 180821780-8780-01, RIN 0660-XC043 (Sep. 26, 2018) (*RFC*).

[3] *Id.* at 48600.

RFC as a good foundation for a move towards a clear United States privacy policy, however, ultimately, in order to provide the greatest legal certainty to consumers and businesses, any changes to United States policy must be implemented through federal legislation. There is clear evidence of a need for federal legislation in the growing patchwork of state and sectoral-specific federal privacy laws that only serve to create more and more fragmentation in privacy protections which ultimately result in inconsistent protections for consumers. Federal legislation that preempts state laws and harmonizes federal regulation will provide the most uniform protections to American consumers regardless of where they live or how they access the Internet and avoid conflicting requirements. Additionally, legislation would serve as an opportunity to further clarify and enhance the Federal Trade Commission's ("FTC") authority to police privacy practices and protect consumers, while preventing duplicative and inconsistent regulations.

This view corresponds with the first of the high-level goals NTIA puts forth which is to harmonize the regulatory landscape.[4] This is only achievable through the application of consistent privacy protections. The adoption of federal legislation is the clearest method to establish consistent privacy protections that are technologically neutral, ensure consistent data protection that individuals and companies can rely upon, and apply uniformly to companies that collect, use, or share consumers' online personal data. And in turn, a unified privacy framework is the most effective way to protect consumers, avoid market distortions, and provide the single, national framework supportable by consumers. Federal legislation also has the added benefit of achieving NTIA's second high-level goal,[5] providing legal clarity while maintaining flexibility to innovate. National privacy legislation that preempts state privacy laws would avoid a patchwork of federal and state privacy laws that would provide consumers with uneven protections and force them to navigate a complicated menu of diverging state-specific privacy choices and controls. Federal legislation should also not permit a private right of action that would only further cloud

[4] *See RFC* at 48602.

[5] *Id.*

legal clarity and discourage innovation. Keeping these overarching goals in mind, we comment below on the seven outcomes upon which NTIA is seeking comment.

Firstly, NTIA submits that organizations should be transparent about how they collect, use, share, and store users' personal information, such that the result is a reasonably informed user, empowered to meaningfully express privacy preferences.[6] USTelecom supports any privacy policy or legislation that requires companies to have their own privacy policy that gives users clear and comprehensible information about the categories of data that are being collected, how consumer data is used, and the types of third parties with whom data may be shared. Our members have long supported transparency and have abided by the transparency policies in the FTC's privacy framework.[7] In fact, early last year a wide variety of broadband industry associations and companies publicly reaffirmed their commitment to FTC policies on transparency, consumer choice, data security and data notification in a published set of principles.[8]

Another suggested outcome is that users be able to exercise control over the personal information they provide to organizations.[9] USTelecom members have long respected consumer choice in protecting their customer's privacy as it is a key part of the existing FTC privacy framework.[10] Our members agree that any Administration policy or federal legislation should ensure that consumers have easy-to-understand privacy choices that are based on the sensitivity of the data and how the data is being used or shared, not the type of company or technology involved. Individual information that can be obtained through publicly available means for example, such as IP addresses and device identifiers, or does not pose a risk of financial harm or identity theft, should not be considered sensitive data. In order to ensure

---

[6] *Id.* at 48601.

[7] "Protecting Consumer Privacy in an Era of Rapid Change; Recommendations for Businesses and Policymakers FTC Report, March 2012 Report, pp.60-__. (*2012 FTC Report*)

[8] *See "Protecting Consumer Privacy Online Internet Companies Reaffirm Consumer Privacy Principles as FCC Reviews Flawed Wheeler Era Broadband Rule"(Jan. 27, 2017)*.

[9] *RFC* at 48601.

[10] *2012 FTC Report*, pp.35-60.

continued innovation and to continue to provide consumers with information they want to receive as part of that choice framework, policy makers should not require an opt-in selection when consumer data that is reasonably de-identified is collected, used or shared because it has been shown that information that is reasonably de-identified reduces present privacy risks for consumers.[11]

The current FTC opt-in regime protects sensitive data in this way by giving them greater control over how that data is used. USTelecom members view the current regime as drawing the right balance between the need for customer privacy, and the value of data in providing consumers with expected services. The value of protection and control that a tailored opt-in regime can provide with respect to sensitive data, evidence can be derived from the economic analysis provided in a white paper by former FTC Commissioner Joshua Wright which explains that overbroad opt-in rules generate costly market failures because, when consumers decline to opt in, most do so out of inertia or indifference rather than any considered objection.[12] These non-choices fail to internalize the larger social costs of that non-choice for the rest of the internet ecosystem.[13] Dr. Wright reports that when opt-in choice is used more broadly the requirements exert upward pressure on retail broadband prices by shutting off a potentially significant source of revenues on the other side of this inherently double-sided market and therefore, opt-in is only appropriate with respect to the most sensitive data.[14] In stances where the overly broad use of opt-in would potentially cause market failures, opt-out consent is a viable option. Opt-in consent allows consumers to have a choice with respect to non-sensitive data without putting unnecessary economic pressure on broadband. It should also be noted that all members of the internet eco-system, due to

---

[11] *See NISTIR 8053* by Simson L. Garfinkel, Information Access Division, Information Technology Laboratory, NIST, (Oct. 2015) which says, "De-identification removes identifying information from a dataset so that individual data cannot be linked with specific individuals. De-identification can reduce the privacy risk associated with collecting, processing, archiving, distributing or publishing information. De-identification thus attempts to balance the contradictory goals of using and sharing personal information while protecting privacy." https://nvlpubs.nist.gov/nistpubs/ir/2015/nist.ir.8053.pdf (last viewed 10/29/2018).

[12] *See*, "An Economic Analysis of the FCC's Proposed Regulation of Broadband Privacy" by Joshua D. Wright (May 27, 2016) at 19 (*Wright White Paper*).

[13] *See Id.*

[14] *See Id* at 10.

marketplace competition have unusually strong incentives to deal fairly with end users on notice-and-choice issues, making it a business imperative to maintain consumer goodwill.

Consistent with this framework is the concept that no affirmative consent should be required in instances where consumer consent can be inferred based on the reason for the consumer's interaction with the business – for example, when a company uses or shares any consumer data for operational purposes (including with third parties and agents), such as service fulfillment and support, first party marketing, network management, security and fraud prevention, product development, and market research. Consumer consent can also be inferred when the use of data is reasonably compatible with a transaction or a consumer's interaction with a company, or required or authorized by law. In the same way, federal policy should not interfere with choice as it relates to consumer-friendly incentives, such as loyalty/rewards programs and discounts, because such prohibitions are profoundly anti-consumer and would affect established practices such as rewards and incentive programs.

NTIA's third outcome is that the collection, use, storage and sharing of personal data should be reasonably minimized in a manner proportional to the scope of privacy risks.[15] NTIA posits that using a risk based approach, the collection, use, storage and sharing of personal data should be reasonable and appropriate to the context which will afford organizations flexibility and innovation in how to achieve these outcomes.[16] USTelecom argues that through best practices in the areas of data security and data de-identification, risk associated with the use of personal data is effectively minimized. Moreover, data used for marketing purposes often is aggregated or anonymized to give consumers information and services they expect to receive from their service provider. As noted herein data de-identification reduces privacy risks, and in combination with aggregation, the amount of personal data that is available is also significantly reduced. Utilizing these sorts of techniques consistent with the FTC's flexible approach, is the best way to achieve reasonable data minimization while not impeding continued innovation.

---

[15] *See RFC* at 48061.

[16] *Id.*

This dovetails with the desired outcome that seeks to ensure that U.S. privacy policy result in organizations employing security safeguards to protect the data that they collect, store, use, or share. USTelecom supports not only sound data security and breach notification policy but more importantly, federal legislation in this area. Any privacy policy or legislation should require companies to take "reasonable" technical, administrative, and physical measures to protect the security of consumer's personally identifiable information without prescribing a checklist of regulatory requirements. Companies should require vendors to comply with such obligations via contract. As with privacy, data security and breach notification legislation should establish a consistent national framework and preempt the existing patchwork of state requirements that cause consumer confusion, and create needless cost and complexity for companies. In addition, FCC data security and breach notification authority should be expressly preempted. Notification of breaches of consumer data stored or maintained by companies should be triggered by a determination that a breach has occurred that poses a reasonable risk of consumer financial harm. It is important that security and breach notification be included in federal privacy legislation or codified in stand-alone legislation.

Additionally, NTIA would like consumers to be able to reasonably access and correct personal data they have provided and require organizations to manage the risk of disclosure or harmful uses of personal data. USTelecom agrees that some level of access is a good idea, however, the right to access should be carefully crafted. The FTC has for years successfully managed the risk associated with data use by focusing on the net welfare of the consumer welfare as well as the sensitivity of the data at issue and the potential harm to consumers deriving from disclosure or misuse of that data. In addition, the sensitivities that may be associated with identified data are avoided when data is de-identified, aggregated, or does not otherwise identify a known individual, but through which can insights derived to offer great benefits to consumers and society and such use. These methods successfully balance both the consumers need for control and access with risks that may be present in the collection and use of data. Indeed, the internet economy has thrived under the FTC enforcement regime which has served to

effectively safeguard consumer privacy across industries by providing predictability and uniform regulatory oversight.[17] Any right of access should not require companies to re-identify consumers and should include strong protections to avoid security and fraud risks. USTelecom supports reasonable requirements that provide consumer the opportunity to correct data that is not otherwise already in the public domain should it be deemed to be inaccurate.

The final outcome is that organizations should be accountable for the use of personal data that has been collected, maintained or used by its systems. The current FTC framework derives from the agencies longstanding principles of Unfair and Deceptive Acts or Practices (UDAP)[18] which provides for FTC enforcement when a provider acts unfairly if its act or practice (1) causes or is likely to cause substantial injury to consumers (2) which is not reasonably avoidable by consumers themselves, and (3) is not outweighed by countervailing benefits to consumers or to competition or when a provider acts deceptively if (1) it makes a statement or omission, or engages in a practice, that is likely to mislead a customer, (2) viewed from the perspective of a consumer acting reasonably under the circumstances, and (3) the deceptive statement, omission, or practice is material—meaning that the misrepresentation or practice is likely to affect the consumer's conduct or decision with regard to a product or service.[19] USTelecom supports the continued used of this standard for holding companies accountable.

In addition, USTelecom supports giving the FTC additional resources necessary to continue to enforce consumer privacy laws. Indeed, one of the high-level goals noted in this RFC is to ensure that the FTC has the necessary resources as well as direction to enforce consumer privacy laws, "in a manner that

---

[17] *See Wright White Paper* at 6.

[18] *Section* 5 of the Federal Trade Commission Act (FTC Act), 15 USC 45(a)(1) (UDAP), prohibits "unfair or deceptive acts or practices in or affecting commerce."

[19] *Also* see FTC Statement on Unfairness, Letter from the FTC Commissioners to Senators Ford and Danforth, Chairman and Ranking Minority Member of the Consumer Subcommittee of the Senate Committee on Commerce, Science and Transportation (Dec. 17, 1980) (appended to International Harvester Co., 104 F.T.C. 949, 1070 (1984)) and FTC Statement on Deception, 103 F.T.C. 174, 175 (1984) (appended to Cliffdale Assocs., Inc., 103 F.T.C. 110 (1984)).

balances the need for strong consumer protections, legal clarity for organizations, and the flexibility to innovate."[20] The FTC has a proven history of privacy enforcement and for decades has been the nation's lead privacy and consumer protection cop on the beat. The FTC has brought more than 500 enforcement actions for privacy and data security violations, including cases involving major internet companies. Once Congress establishes a core set of privacy requirements in legislation, the FTC can evolve enforcement to address changing practices, business models, technologies, and consumer preferences through its long-standing and effective case-by-case enforcement authority. With the FTC as the exclusive federal authority to enforce the law, it would allow for the flexibility necessary in this changing landscape while also avoiding duplication and inconsistent outcomes.

Precisely because the FTC's approach to safeguarding privacy has been consistently applied across the internet ecosystem, consumers have received both the benefits and protections the framework provides while still allowing technology companies the freedom to innovate and responsibly use data in ways that result in new products, lower prices, and increased consumer welfare. USTelecom members support continued application of this approach across the internet ecosystem which also meets NTIA's high-level goals of ensuring continued data innovation as well as employment of a risk and outcome-based approach.[21]

With respect to the other high-level goals identified in the RFC, USTelecom supports an effort to ensure that policy development heads in a direction that includes a focus on interoperability[22] and scalability.[23] With respect to interoperability, because the internet ecosystem is no longer constrained by borders, but instead part of a global economy, it is necessary that any U.S. policy or federal legislation include mechanisms to bridge differences across borders while ensuring data remains protected. This is precisely one of the reasons that even within the United States it is important that consumer privacy not

---

[20] *See RFC* at 48602.

[21] *See Id.*

[22] *See Id.*

[23] *See Id. at 48602-03.*

be regulated on a state-by-state basis so that consumers know their privacy is guaranteed across the country, not through different laws in various states. USTelecom also supports considerations that take into account the size of the entity impacted by the rule. Just as some companies operate solely within the United States and others operate globally, there are also companies serving rural parts of the U.S. that are considerably smaller than the larger companies that first come to the average consumer's mind. Therefore, USTelecom supports a model for any policy or laws that accounts for the burden of its applicability on smaller providers.

USTelecom also supports the Administration's efforts to establish a collaborative public-private partnership that encourages privacy research[24] and voluntary privacy programs and standards developed through public-private collaboration that could serve as a safe harbor in legislation, while enabling companies to adapt to rapidly changing technology and market developments. In particular, USTelecom supports the development of a safe harbor that can act as guideposts for companies to follow and know that they are meeting the requirements of a particular law.

The key to ensuring consumers are adequately protected is to make sure consumers know what data is being collected, how it is being used, and giving them the opportunity to exercise choice in the matter, while at the same time balancing the need not to interrupt beneficial uses of information. The imposition of restrictions on data uses that would not result in material harm to consumers will stifle innovation and eliminate everyday customer conveniences. As the Internet has grown up and become part of everyday commerce, consumers have come to expect that in order to engage in commerce and conduct everyday activities, such as making purchases, paying utility bills, signing up for activities, etc. requires the sharing of some non-sensitive information. The current FTC regime allows for any uses consistent with the purpose of the transaction or relationship with the customer, or uses required or authorized by law which allows for all first-party marketing, except for where there is highly

[24] *See RFC* at 48602.

"sensitive" data (e.g., health, financial and precise location). NTIA should take the time to truly analyze all of the comments and data filed in this proceeding for their fact-based merits and should harmonize any policies it adopts with those that are time-tested.

Respectfully submitted,

USTELECOM

By: _____

B. Lynn Follansbee
Jonathan Banks
Its Attorneys

601 New Jersey Avenue, NW, Suite 600
Washington, D.C. 20001
202-326-7300

November 9, 2018