DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

Request for Comment: Developing the Administration's Approach to Consumer Privacy

Docket No: 180821780-8780-01

COMMENTS OF THE 21ST CENTURY PRIVACY COALITION

November 9, 2018

National Telecommunications and Information Administration
U.S. Department of Commerce
Room 4725
1401 Constitution Avenue NW
Washington, DC 20230
Attn: Privacy RFC, Washington DC 20230

I. INTRODUCTION

The 21st Century Privacy Coalition ("Coalition")[1] appreciates the opportunity to respond to the National Telecommunications and Information Administration's ("NTIA") Request for Comment ("RFC") regarding "ways to advance consumer privacy while protecting prosperity and innovation."[2] The Internet has been a great source of prosperity and innovation, and clarifying consumers' online privacy protections will only enhance that prosperity and innovation.

The Internet has changed the way consumers communicate, learn, shop and entertain themselves. It has enabled the exchange of ideas, services and products across the country and around the globe. These incredible benefits to consumers have resulted from, among other things, innovative uses of consumers' information, often including personal information. Data-driven products and services have been integral to the transformative benefits delivered to consumers in the Internet age.

There is an increasing consensus in the United States and globally that the confidence consumers have in their use of the Internet can be enhanced by clarifying consumers' privacy protections. The Coalition agrees that "[t]he time is ripe for this Administration to provide the leadership needed to ensure that the United States remains at the forefront of enabling innovation with strong privacy protections."[3] As the RFC points out, an increasing number of regions,

[1] The Coalition is comprised of the nation's leading communications service providers, which have a strong interest in bolstering consumers' trust in online services and confidence in the privacy and security of their personally identifiable information.

[2] Dept. of Commerce, Nat'l Telecomm. and Information Admin., *Developing the Administration's Approach to Consumer Privacy*, 83 Fed. Reg. 48,600 (Sept. 26, 2018) ("RFC").

[3] *Id*.

countries and states have adopted their own distinct privacy frameworks, resulting in "a nationally and globally fragmented regulatory landscape."[4]

The United States should adopt a framework that "reduces fragmentation nationally and increases harmonization and interoperability nationally and globally."[5] In order for this framework to be effective and achieve the Administration's objectives, Congress needs to enact legislation that instills consumers with confidence in how their data will be used, and gives businesses certainty so that they can innovate. Such legislation would enable the United States to establish its global leadership in protecting consumer privacy while promoting prosperity and innovation.

II. THE UNITED STATES NEEDS A FEDERAL STATUTORY PRIVACY FRAMEWORK

While the RFC does not explicitly call for legislation, NTIA's stated goal in issuing the RFC is to "determine the best path toward protecting individual's privacy while fostering innovation."[6] The Coalition believes that this path requires a new federal statutory privacy framework.[7] While Administration policy could set a helpful tone for developing comprehensive US privacy protections, there is simply no substitute for clear statutory direction from Congress.

New federal legislation would achieve several key objectives. First, legislation would provide the greatest legal certainty to both consumers and businesses. Changes in Administration policies, in the absence of amending existing statutory authorities, would not legally bind companies, nor would they set clear safeguards for consumers' use of the Internet. Legislation

[4] *Id*.
[5] *Id*.
[6] *Id*.
[7] Our presumption is that this new framework would cover consumer privacy, not the interaction between companies regarding non-consumer-related information.

would achieve the Administration's goal of "ensur[ing] that organizations have clear rules that provide for legal clarity."[8]

Second, federal legislation is needed to address the growing patchwork of state and sector-specific privacy laws that is causing a fragmentation in US privacy protections, resulting in inconsistent protections and confusion for US consumers. As the RFC articulates, it is critical "to avoid duplicative and contradictory privacy-related obligations" and to "harmonize the regulatory landscape."[9]

Federal legislation that preempts these laws while strongly safeguarding consumer privacy would provide uniform protections to US consumers regardless of where they live or access the Internet, and regardless of the legacy privacy requirements that apply to different components of the Internet ecosystem. Federal legislation should preempt state and sector-specific requirements,[10] thus preventing confusion for consumers and businesses alike resulting from multiple agencies and layers of government imposing requirements on the same entities and information. The consistent application of the new law will be critical to its success. It would also achieve the "comprehensive application" sought by the Administration.[11]

Third, 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, which is another key Administration goal.[12] The FTC is the nation's foremost privacy enforcement agency, with decades of expertise derived from the over 500 enforcement actions it has brought to protect the privacy of consumer information, including cases against many of the largest

[8] *RFC*, at 48602.
[9] *Id*.
[10] The coalition recognizes that Congress may make exceptions for the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act.
[11] *RFC*, at 48602.
[12] *Id*.

companies operating online.[13] In addition to enforcement, the agency also issues reports, including its landmark 2012 Privacy Report,[14] and routinely conducts workshops and provides guidance to address developments in the consumer privacy and data security landscape.[15]

The Coalition agrees with the Administration that "[i]t is important to take steps to ensure that the FTC has the necessary resources, clear statutory authority, and direction to enforce consumer privacy laws in a manner that balances the need for strong consumer protections, legal clarity for organizations, and the flexibility to innovate."[16] Legislation should clarify the FTC's legal authority and mandate to protect consumer privacy, and enhance the tools at the FTC's disposal in such efforts.

III. KEY COMPONENTS OF FEDERAL PRIVACY LEGISLATION

The Coalition also agrees with the Administration that "mechanisms that focus on managing risk and minimizing harm to individuals arising from the collection, storage, use, and sharing of their information" can help achieve the goals of balancing flexibility, protecting consumers and providing legal clarity.[17] New federal legislation should create a uniform, national privacy framework based upon the sensitivity of information being collected, used or shared and the risk of consumer harm posed by such collection, use, or sharing. These foundational components are inter-related: For example, the more sensitive the information, the more likely that its use or disclosure risks harming consumers. In addition, companies should have the flexibility to use data consistent with their relationship with the consumer.

---

[13] FTC, *Privacy and Data Security Update: 2017*, 2 (Jan. 8, 2018).
[14] *See* FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 5, 2012).
[15] *See, e.g.*, FTC, *Internet of Things: Privacy & Security in a Connected World* (Jan. 27, 2015); FTC, *Connected Cars Workshop: Staff Perspective* (Jan. 9, 2018).
[16] *RFC*, at 48602.
[17] *Id*. at 48601.

Privacy legislation should apply these principles uniformly to all entities that interact with consumers' information; a new statute must be technology-neutral and not create different consumer protections depending upon a company's business model. Consumer privacy should not be based upon who is collecting the information, but rather on what is being collected and how it is being used. This new law must apply consistently to all entities to avoid confusing consumers or creating uneven consumer privacy protections.

Transparency

Legislation should require companies to provide consumers with clear and comprehensible information about the categories of data that are being collected, used or shared, and the types of third parties with which information may be shared. Legislation should provide consumers with easy-to-understand privacy choices based upon the sensitivity of information and the risk of consumer harm presented when such information is used or disclosed in different ways.

Consumer Choice

Consumers should be "empowered to meaningfully express privacy preferences."[18] A sensitivity and risk-based approach would provide consumers with privacy options appropriate to the type of information being collected, used and shared. For example, consumers expect sensitive information about their health, finances, children, precise geolocation and Social Security numbers to receive heightened protection. Conversely, a sensitivity and risk-based approach would not impose requirements on information where there is a significantly reduced risk that such information could be associated with an individual, such as de-identified or

[18] *Id*.

anonymized information. Similarly, information that is publicly available does not present a risk of exposure.

Within this framework, consumers should control the collection, use and sharing of their information through their exercise of meaningful choice that is appropriate for the data collection, use or sharing at issue and is consistent with the relationship between the business and the consumer. The method of consent will not be the same for all types of information or all types of uses. For example, consumers should have to opt in prior to an entity sharing their sensitive information with a third party for the latter's own commercial purposes. And consumers should be able to opt out of the use or sharing of non-sensitive personally identifiable information for targeted third-party advertising.

For operational purposes, however, and other uses of the data that are consistent with the relationship and nature of the interaction between the consumer and the business, consent should be inferred. These uses include, but are not limited to, service fulfillment and support, first-party marketing, network management, security and fraud prevention, product development and market research. Consent should also be inferred when disclosure of certain information is required or authorized by law.

While consent standards could vary depending upon the sensitivity of the information, different consumers have different privacy preferences. Therefore, legislation should not limit consumer choice by inhibiting consumer-friendly incentive programs tied to privacy choices such as grocery-store rewards programs. As long as consumers are provided with clear and comprehensible information about the nature of such programs, they should be allowed to make their own choices.

Data Security and Breach Notification

Legislation should require companies to take reasonable technical, administrative and physical measures to protect the security of consumer's personally identifiable information based upon the sensitivity of the information and the risk of consumer harm if such information is acquired by an unauthorized person. Companies should also contractually require vendors to likewise adopt protective measures. But legislation should not mandate particular security solutions or measures.

In addition, legislation should include a data breach notification regime based upon a reasonable risk that the unauthorized acquisition of personally identifiable information would result in identity theft or other financial harm to consumers. As with the legislation's privacy provisions, the new law should preempt the patchwork of state and other federal data security and breach notification requirements.

Enforcement

Congress should designate the FTC as the sole federal agency responsible for enforcing the new privacy law.[19] The FTC should have clear authority to impose fines on companies that violate the new law. State Attorneys General ("State AG") could be authorized to enforce the new statute, although the legislation should allow companies to seek consolidation of multiple State AG actions arising from the same violation, and the FTC should have the authority to intervene in any such action. The legislation should also prohibit private rights of action.

Legislation should also encourage voluntary privacy programs and standards developed through public-private partnerships. Such programs and standards, especially if they serve as a safe harbor for compliance with legislation, could allow companies the flexibility necessary to

[19] Exceptions could be made for entities subject to the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act.

protect consumers as technology and best practices evolve. Congress could require the FTC to evaluate and authorize companies' use of voluntary privacy programs and an independent third-party to certify a company's compliance with such a program.

IV. CONCLUSION

The Coalition commends NTIA for undertaking the RFC and for engaging the public in this transparent process to evaluate how to advance both consumer privacy as well as prosperity and innovation. The United States needs to assert global leadership in establishing privacy protections for consumers while preserving the vibrancy of the Internet. The Coalition believes that new federal legislation would provide the greatest clarity and certainty regarding the rights of consumers and the responsibilities of companies that collect, use or share consumers' personally identifiable information.

The United States would benefit from a unified, technology-neutral federal privacy framework that applies to all entities in the Internet ecosystem, regardless of their business model. And new federal legislation that preempts other state and sector-specific requirements would eliminate the confusion resulting from multiple regimes applying to the same entities and information.