Before the
DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS
AND INFORMATION ADMINISTRATION

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

COMMENTS OF VERIZON

In its Request for Comment (RFC), the National Telecommunications and Information Administration (NTIA) correctly recognizes the need to advance consumer privacy in the United States.[1] Ensuring that the Internet remains an engine for continued innovation and economic growth is one of NTIA's missions—and only with consumer trust can the digital economy continue to flourish. Consumer trust hinges on individuals having confidence that when using products and services their personal information isn't being misused. Through this proceeding, NTIA can help develop a path forward that provides strong consumer privacy protections while also fostering innovation.

Verizon is one of the world's leading providers of communications, information and entertainment products and services to consumers, businesses and governmental agencies. With a presence around the world, we offer voice, data, and video services and solutions on our wireless and wireline networks that are designed to meet customers' demand for mobility, reliable network connectivity, security and control. Verizon provides services to enterprises operating on a global basis, including voice, data, and video communications products, and enhanced services,

[1] *See Developing the Administration's Approach to Consumer Privacy,* Request for Comment, Docket No. 180821780-8780-01, RIN 0660-XC043, 83 Fed. Reg. 48600 (September 26, 2018) (RFC).

such as broadband video and data services, Internet of Things (IoT), corporate networking solutions, security, and managed network services. Throughout, we place paramount importance on privacy and security to protect our customers and our own core business.

I. Comprehensive Privacy Legislation is Needed to Achieve NTIA's Privacy Outcomes and High-Level Goals for Federal Action

Verizon agrees with the NTIA's threshold "desired outcome" for a privacy framework in the United States, namely:

> **"a reasonably informed user, empowered to meaningfully express privacy preferences, as well as products and services that are inherently designed with appropriate privacy protections, particularly in business contexts in which relying on user intervention may be insufficient to manage privacy risks."[2]**

To achieve this desired outcome, it is critical for the United States to establish comprehensive federal consumer privacy legislation. Verizon has long supported the need for such legislation, dating back to 2011. Even then, it was clear to Verizon that the existing framework for privacy in the United States was too fragmented to offer users the level of trust they needed to embrace all that our digital economy has to offer. Developments over the years have reinforced our support for strong, comprehensive privacy legislation, which should be simple to understand and should be targeted to users' needs and today's digital reality. Legislation should also be national in scope so all Americans are equally protected. A state-by-state legislative framework for privacy creates friction and uncertainty for consumers who use services that don't stop at state borders.

II. Federal Legislation Should Include Key Principles Such as Consistency, Flexibility, and Choice

A core set of privacy principles should be reflected in federal privacy legislation. Verizon has publically shared these principles and is encouraging all stakeholders to work together to

[2] *Id.* at 48601.

achieve the common goal of strong privacy protections for users at the federal level.[3]

> **Consistency and Federal Framework. All entities, regardless of industry sector, that collect information about consumers should be subject to the same requirements. Because the Internet doesn't distinguish between state borders, there should be a federal framework governing privacy and not variable state-by-state rules. A single federal regulator—the Federal Trade Commission—is best positioned to enforce a Federal standard.**

Harmonizing the regulatory landscape across industries in the United States is critical to ensuring consumers' privacy is protected. NTIA rightfully notes that similar data practices in similar contexts should be treated the same rather than through a fragmented regulatory approach. In addition to harmonizing requirements across industries, it is also critical to have consistency across the country and not a state-by-state approach to privacy protection. In today's Internet economy it is impractical for state borders to serve as differentiators as to how products and services are offered. The Internet does not recognize state boundaries, and consumers should not have their privacy protections depend on their state. The RFC correctly notes it is harmful if Americans may not have equal privacy protections "depending on where the user lives."[4]

A single federal regulator of a single standard will serve to ensure consistent application both across industries and across the country.

---

[3] *See* *https://www.verizon.com/about/news/privacy-its-time-congress-do-right-consumers*.

[4] RFC at 48602.

<u>Flexibility</u>. Statutory requirements governing ever-evolving technology need to be flexible so that they don't become quickly outdated. The overall framework should be informed by the principle that the level of sensitivity of the personal information will dictate the corresponding protections. The FTC could have a role in providing guidance on statutory requirements, such as defining "personal information" and "sensitive personal information."

Verizon agrees with the RFC that flexibility is critical as it "allows for novel business models and technologies."[5] Flexibility will ensure that statutory requirements don't quickly become outdated as technology continues to advance. One important component of this flexibility is not dictating that all personal information should be treated the same. There must be built-in flexibility to tailor protections based on the sensitivity of the information. Such flexibility allows for incentivizing data de-identification or pseudonymization. Risk-based approaches also should be encouraged, as noted by NTIA. Risk-based analyses allow for the needed flexibility to assess potential privacy harms, where the sensitivity of the information is one of the inputs in modeling the level of risk in connection with data processing. Considering the importance of assessing the sensitivity of information in analyzing risk, the FTC could play a role in guiding industry as to what type of information is considered "sensitive." As the federal regulator with years of expertise in policy-making with respect to privacy and a long track record of privacy enforcement, the FTC is well-positioned to provide this input.

<u>Transparency</u>. Companies must provide clear and easy to understand information about their practices with respect to the collection, use, and sharing of personal information. As part of transparency, companies should have a mechanism that provides consumers with reasonable access to what information the company has about that consumer.

Individuals must be able to easily understand how organizations collect, store, use, and share their personal information. The RFC correctly acknowledges the importance of

[5] *Id.*

transparency and notes that transparency can be enabled through various means. Organizations should be encouraged to innovate in how information is communicated to individuals that use their products and services. While privacy policies describing companies' privacy practices are valuable, additional mechanisms, such as privacy dashboards and "just in time" notices can serve to well-inform customers and enable them to understand the practices being described and the choices they have at a more relevant time. To further increase transparency, users also should have reasonable access to their personal information.

> **Choice. Companies must provide consumers with the opportunity to opt in to the collection, use, and sharing of sensitive personal information and to opt out of the collection, use, and sharing of other personal information. Exceptions should be in place for the collection, use, and sharing of personal information for operational and other purposes (e.g., legal process).**

Individuals must be empowered to exercise reasonable control over their personal information, including collection, use, and sharing, as the RFC states. The type of choice, how it should be offered, and at what point in time it should be offered, will necessarily depend on context, taking into consideration certain factors such as user's expectations and the sensitivity of the information. Taking these factors into account will enable companies to provide users with more meaningful choices. For example, as a general matter, it is appropriate for consumers to be offered the choice, on an opt-in basis, for the use of their sensitive personal information, whereas opt-out choice will be appropriate when the information is not sensitive. Of course reasonable exceptions to offering choice must be in place (e.g., for operational purposes (such as to render or bill for service) or legal process), but it is important for organizations to recognize that from the consumer perspective, exerting greater control over their sensitive information is imperative.

<u>Data Security and Breach Notification</u>. Companies must put in place reasonable security measures to protect information and should notify consumers in appropriate circumstances when breaches occur.

NTIA correctly notes that reasonable security measures should be employed by companies to safeguard personal information from loss, and unauthorized access, destruction, use, modification, and disclosure. Certain relevant factors, such as the nature and scope of a company's activities, the sensitivity of the data, the size of the organization and technical feasibility, will inform the specific measures that an organization puts in place. NTIA's emphasis on risk management is particularly important with regard to data security—where resources must be deployed in a manner best designed to mitigate the risk to users. Appropriate notification to users when breaches occur is also critical. Currently, there is no comprehensive federal legislative framework that addresses breach notification. All 50 states—and four U.S. territories—have their own laws governing breach notification, each with its own specific set of requirements, such as timing of notification, what triggers notification, and what must be included in the notification.[6] A comprehensive legislative federal approach to consumer privacy should include a breach notification regime to replace the current state-by-state standards, however, it may also be appropriate to address federal breach notification in a distinct legislative vehicle. A federal notification standard should require organizations to notify users of appropriate breaches that could cause material harm to users, such as the risk of identity theft. Limiting notification in this way helps limit the number and frequency of notifications which can actually be harmful to users. Inundating users with notifications when there is no real threat only serves to de-sensitive users to the notifications that are of real importance. The main purpose in

[6] In addition to the 50 states, the following also have breach notification laws: District of Columbia, Puerto Rico, Guam and the U.S. Virgin Islands.

notifying users is to put them on alert so they can take steps to minimize the impact of a breach. Accordingly it is important to limit notification to those circumstances so that users take appropriate action.

<u>Enforcement</u>. The enforcement regime for privacy should be two-fold: (a) FTC enforcement with civil penalties (subject to a cap); and (b) State attorneys general enforcement of Federal law.

As noted above, the FTC is the appropriate federal regulator to enforce a comprehensive federal privacy law. Because of the FTC's limited ability to seek civil penalties under its current legal authority, new comprehensive federal privacy legislation should enable the FTC to seek civil penalties for violations. Civil penalties—subject to a reasonable cap—will bestow deterrence capability on the FTC, while at the same time avoid arbitrariness and unreasonably punitive action. Without a cap, the disincentives for innovating may be too great thereby stifling the development of new products and services.

While a single set of privacy requirements under a new comprehensive federal law should be enforced by a single federal regulator—the FTC, it may be appropriate to allow state attorneys general to bring enforcement actions for federal law violations arising from actions impacting their state's residents.

<u>Safe Harbor Programs</u>. An entity will be deemed to be in compliance with the law if it participates in and is in compliance with a Safe Harbor program that meets or exceeds the requirements of the law.

Safe Harbor programs, with requirements that meet or exceed the requirements of a new federal law, will provide companies with a mechanism to demonstrate compliance. Safe Harbor programs benefit organizations by providing a detailed framework designed to be in compliance with the law, and it also benefits users by increasing accountability. To incentivize participation in these programs, companies should be deemed to be in compliance with the law if they are

following the program's requirements that must be designed to meet or exceed the law's requirements.

One of the privacy outcomes discussed in the RFC is "accountability" —that "organizations should be accountable externally and within their own processes for the use of personal information contained, maintained, and used in their systems."[7] Safe Harbor programs are a useful tool enabling companies to demonstrate their accountability in that in order to participate they map their privacy practices to the Safe Harbor program requirements.

III. Promoting Cross-Border Data Flows is Critical

Comprehensive federal privacy legislation in the United States may help reduce friction placed on data flows. As noted by NTIA, a regulatory landscape in the United States that is consistent with the international norms and frameworks developed in the multilateral forums in which the United States participates, will help in reducing barriers to seamless data flows. The privacy outcomes and high-level goals outlined in the RFC generally align with many of the privacy principles developed by the Organization for Economic Cooperation and Development and the Asia-Pacific Economic Cooperation forum.[8] Federal legislation that implements these outcomes and goals will further enhance Administration efforts both within international organizations, as well as through engagements with international stakeholders, to develop mechanisms to further enhance the free-flow of data.

* * * * *

[7] RFC at 48602.

[8] Organization for Economic Cooperation and Development, *OECD Privacy Framework* (2013), http://www.oecd.org/sti/ieconomy/privacy-guidelines.htm; and Asia Pacific Economic Cooperation forum, APEC Privacy Framework (2015), https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015).

While Congress should enact comprehensive federal privacy legislation, Verizon encourages NTIA, and other parts of the Administration, to continue its work to advance consumer privacy while protecting prosperity and innovation. As noted in the RFC, NTIA has worked in coordination with the International Trade Administration (ITA) to ensure consistency with international policy objectives. ITA's important work to facilitate cross-border data flows is critical for continued growth of the global economy. The RFC's privacy outcomes and goals can also serve as useful guideposts for the work being done within the National Institute of Standards and Technology—the development of a voluntary risk-based privacy framework. NTIA's commitment to growth and innovation is vital to the global marketplace and is critical to the United States through leadership on continued ways to grow the global economy.

Respectfully submitted,

/s/ Yael Weinman

Karen Zacharia
Of Counsel

Yael Weinman
Verizon
1300 I Street, NW, Suite 500E
Washington, DC 20005

November 8, 2018