

**Before the
FEDERAL TRADE COMMISSION**

Hearings on Competition and Consumer Protection)
in the 21st Century:) FTC 2018-0098
)
Consumer Privacy)

COMMENTS OF VERIZON

In advance of the Federal Trade Commission’s (FTC) scheduled February 12-13, 2019 privacy hearings, Verizon appreciates this opportunity to provide comments on federal privacy legislation – an area identified in the FTC’s Background and Questions for Comment relating to these hearings (“Questions for Comment”).¹

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, 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.

¹ See *FTC Hearing on Competition and Consumer Protection in the 21st Century – February 2019, Background and Questions for Comment*, <https://www.ftc.gov/news-events/events-calendar/ftc-hearing-competition-consumer-protection-21st-century-february-2019>.

I. Comprehensive Privacy Legislation is Necessary

It is critical for the United States to establish a comprehensive federal consumer privacy law. 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.

In the Questions for Comment, the FTC specifically asks about existing sectoral privacy laws, such as those in the communications sector. Privacy protections relating to communications should be consistent with those imposed on the rest of the Internet ecosystem. Today, the same types of data are subject to different privacy frameworks depending upon who the service provider happens to be. This leads to consumers not understanding how their data is being protected. To address this problem, the privacy requirements specific to the communications sector² should be replaced by a comprehensive federal privacy law. And that law should confer jurisdiction as it relates to privacy and data security over all communications providers (including common carriers) to the FTC and remove any related authority from the Federal Communications Commission.³

² *E.g.*, 47 U.S.C. §§ 222 and 551 and any implementing regulations.

³ In addition, the specific statute covering video viewing, the Video Privacy Protection Act (VPPA), is similarly unnecessary and should be eliminated because a federal comprehensive privacy law would address the activity covered in the VPPA. 18 U.S.C. § 2710.

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 achieve the common goal of strong privacy protections for users at the federal level.⁴

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. 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.

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

Flexibility. 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."

⁴ See <https://www.verizon.com/about/news/privacy-its-time-congress-do-right-consumers>.

Flexibility is necessary to account for different types of business models and technologies and to allow for innovation in both. 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—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.

Transparency. 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. Transparency can be achieved through a variety of means, and organizations should be encouraged to innovate in how information is communicated to individuals that use their products and services. While published 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. The type of choice, how it should be offered, and at what point in time it should be offered, will necessarily depend on context. Factors such as the user's expectations and the sensitivity of the information should be taken into account. By considering these factors, companies can 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.

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

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. Managing risk is at the core of an organization's security

practices—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.⁵ A comprehensive legislative federal approach to consumer privacy should include a breach notification regime to replace the current state-by-state standards. 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-sensitize users to the notifications that are of real importance. The main purpose in 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.

Enforcement. 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

⁵ 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.

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.

Safe Harbor Programs. 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 encourage 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.

III. Hearings

The need for comprehensive federal privacy legislation should be one of the specific topics discussed at the February hearings. Specifically, the hearings should include robust discussion of what principles should be reflected in comprehensive privacy legislation as well as

which sectoral laws would no longer be necessary if a comprehensive federal privacy regime were put in place. Verizon looks forward to continuing to engage with the FTC as well as other stakeholders on these important issues.

Respectfully submitted,

Karen Zacharia
Of Counsel

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

December 21, 2018