November 9, 2018

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Ave., NW
Washington, DC 20230

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

I. Introduction

The Computing Technology Industry Association (CompTIA) is a leading voice and advocate for the $1.5 trillion U.S. information technology ecosystem and the 11.5 million technology and business professionals who design, implement, manage, market, and safeguard the technology that powers the U.S. economy. Through education, training, certifications, advocacy, philanthropy, and market research, CompTIA is the hub for advancing the tech industry and its workforce.

CompTIA's member companies have long-understood the importance of protecting their users' privacy and securing the data they collect and store. Consumer trust equates to good business. But we also understand that despite the industry's best efforts, data breaches and identity theft are at an all-time high.[1] To curb this disturbing trend governments around the world have recently tried to meet this challenge through new privacy and data security laws. However, while these laws were often crafted with the best of intentions, they are more likely to result more in significant compliance costs and stifled innovation than improving consumer protection.

The outcomes-based approach proposed by NTIA in its Request for Comment[2] provides an outstanding framework for how the United States should look to regulate in the consumer privacy and data protection space. NTIA's model uses a similar risk-based approach to CompTIA's recently-crafted principles for federal privacy legislation. An outcomes-based approach provides flexibility for companies to decide how best to protect their users' privacy and the data in their possession instead of the top-down regulatory models used in other countries. Putting companies, not regulators, in charge of these decisions will improve privacy and security while reducing compliance costs. Instead of checking boxes to ensure compliance with the law, an outcomes-based approach will motivate companies to implement strong privacy and security practices that best fit their specific business models.

[1] Identity Theft Resource Center, 2017 Annual Breach Year-End Review at 3 (2018), https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf.
[2] National Telecommunications and Information Administration, Developing the Administration's Approach to Consumer Privacy, 83 FR 48600 (September 26, 2018) ("NTIA RFC").

It is thus time for Congress to pass a comprehensive law that strengthens consumer privacy and data security while preserving the regulatory environment that has allowed American innovation to thrive in recent years. CompTIA thanks NTIA and the Administration for the timely opportunity to comment on this pressing issue.

II. The Need for a U.S. Standard

Countries around the world, such as India,[3] are now looking to establish their own privacy laws and are drawing from the European General Data Protection Regulation (GDPR) as a model. The fact that the U.S. does not have a replicable alternative approach puts U.S. companies at a serious disadvantage. The adoption of GDPR or a similar approach as a global privacy standard will curb innovation. Our members' primary concern is that GDPR imposes so many specific obligations that it creates an immense compliance burden for companies without necessarily improving consumer protection. Large U.S. companies have spent billions of dollars to comply with GDPR,[4] while some smaller companies have chosen to cut off EU access to their services rather than spend the money necessary to comply.[5] Businesses should not have to choose between compliance and ceasing operations, particularly if they're already dedicating resources to protecting data and user privacy. NTIA's outcomes-based approach would ensure companies that take data security and user privacy seriously would not have to make such a choice. It should be the model for a U.S. consumer privacy law.

The U.S. is often criticized globally for its lack of a comprehensive privacy and data security regime. Instead of a singular law, the U.S. has a sector-specific privacy and security approach for industries such as banking and health care, while the FTC regulates most other industries under its Section 5 authority. This approach has drawbacks: it is not a replicable model for other countries, and the FTC's authority in this space is limited. As a result, California became the first state to pass a data privacy law when it passed the California Consumer Privacy Act[6] ("CCPA") in June, and other states may soon follow suit. Without Congressional action, companies may soon be facing a patchwork of state privacy laws along with the developing international patchwork. The time is right for Congress to act and pass a preemptive national law that ensures the FTC has the tools necessary to be the primary privacy and data security regulator.

CompTIA agrees with NTIA's statement in its Request for Comment, "the FTC is the appropriate federal agency to enforce consumer privacy."[7] The FTC has been the chief federal regulator in the privacy and data security sector since the passage of the Fair Credit Reporting

---

[3] *See* India's Draft Personal Data Protection Act (2018), available at http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdf.

[4] Oliver Smith, *The GDPR Racket: Who's Making Money From This $9bn Business Shakedown*, Forbes, May 2, 2018, *available* at https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/#6c03c1e234a2.

[5] Nate Lanxon, *Blocking 500 Million Users Is Easier Than Complying With Europe's New Rules*, Forbes, May 25, 2018, *available at* https://www.bloomberg.com/news/articles/2018-05-25/blocking-500-million-users-is-easier-than-complying-with-gdpr.

[6] Ca. Assembly Bill No. 375 (2018).

[7] NTIA RFC at 48602.

Act in 1970[8] and has immense institutional knowledge. But the FTC's consumer protection authority is currently limited to "unfair or deceptive acts or practices,"[9] which may not cover the full breadth of potential issues that could arise when companies collect and use personal information. To ensure that the FTC can implement the outcomes-based regulatory model proposed by NTIA, legislation is needed to clarify and possibly expand the FTC's role as a privacy and data security regulator.

For example, the FTC penalizes companies for failure to adhere to their own privacy and security commitments and terms of service,[10] but no law requires companies to make those commitments in the first place. National Privacy legislation should follow NTIA's model to provide the FTC with the proper regulatory toolbox. It should lay out desired privacy outcomes and allow the FTC to punish companies when they fail to achieve them. This new federal privacy law should not interfere with any of the sector-specific laws such as HIPAA or Graham-Leach-Bliley, and should only be confined to empowering the FTC to serve a greater role as privacy regulator.

III. NTIA's Framework and CompTIA's Privacy Principles

CompTIA recently compiled a set of principles for federal privacy legislation. Our principles advocate for a risk-based approach that would require companies to implement common-sense protections for the data they collect. Both the NTIA and CompTIA's approaches focus on preventing consumer harm, and both give companies the flexibility to determine how best to prevent that harm.

Any conversation about privacy legislation should start with the desired outcomes and then determine how best to achieve them. But this common-sense approach hasn't necessarily been the universal model. Unfortunately, some other approaches seem to focus on punishing companies first and protecting consumers second. NTIA's approach appreciates that protecting innovation must also be a consideration in any discussion of privacy regulations.

NTIA lays its purpose out clearly stating "the desired outcome is 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."[11] It further breaks the desired outcomes into transparency, control, reasonable minimization, security, access and correction, risk management, and accountability.[12] It would be difficult to argue that these seven outcomes do not reflect a comprehensive picture of desired outcomes for protecting consumer privacy.

CompTIA's principles for federal privacy legislation fit seamlessly alongside NTIA's framework. Our principles draw upon input from member companies and from existing privacy

[8] Federal Trade Commission, Protecting Consumer Privacy and Security, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy-security.
[9] 15 USC § 45 (a)(1).
[10] Federal Trade Commission, Privacy and Security Enforcement, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement.
[11] NTIA RFC at 48601.
[12] *Id.* at 48601-48602.

frameworks, most notably the Asian-Pacific Economic Cooperation (APEC) Privacy Framework.[13] Our overarching theme is that the goal of any federal privacy law should be to prevent personal information from being misused in ways that could harm individuals. To accomplish this goal, federal legislation should require companies that collect and use personal information to:

- Adopt appropriate safeguards to secure that information;
- Build privacy and security protections into their products and services at the development stage ("Privacy and Security-by-design");
- Provide easily accessible and understandable information to their customers about what data they are collecting, how that information is being used, and what choices individuals have about information collection and use;
- Absent explicit user consent, limit data collection and usage of personal information to the uses conveyed to the customer, and, when necessary to provide a service requested by customer;
- When practicable, provide users with the ability to choose how their data is collected and used.

Additionally, we note that not all information collected should be treated equally under the law. Instead the greater the risk that the information could be used in a harmful manner, the stronger the protections should be regarding the data. Similarly, some uses of information provide greater risk of harm to consumers than others and should be regulated as such.

A federal privacy law should apply equally to all companies under the jurisdiction of the FTC, and should not impose different rules on different business models, nor should it require the use of any specific technologies. Companies should have flexibility in how they choose to comply with the regulations.

We see significant overlap between CompTIA's principles and NTIA's approach. Transparency, control, data minimization, security, risk management and accountability all appear in some form in CompTIA's principles. Also, we strongly support users' ability to access and correct personal data they have provided to a company. CompTIA's principles dovetail with several of NTIA's "High-Level Goals for Federal Action."[14] NTIA has done an exceptional job identifying and defining a comprehensive list of outcomes and goals which will preserve innovation while improving data protection and privacy nationwide.

IV. Conclusion

Since the internet's inception American companies have been the world's preeminent innovators, due at least in part to a regulatory regime that promoted a balance between innovation and consumer protection. While that regulatory regime now needs an update to better-protect consumers, it's possible to preserve that balance through legislation anchored in a risk and

[13] Asia-Pacific Economic Cooperation, APEC Privacy Framework (2015), *available at* https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015).
[14] NTIA RFC at 48602.

outcomes-based approach like NTIA has put forward. The U.S. needs to show the world that there's another, better way to protect consumers' data.