



American Insurance Association

555 12th Street, NW
Suite 550
Washington, DC 20037
202-828-7100
Fax 202-293-1219
www.aiadc.org

November 9, 2018

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Room 4725
Washington, D.C. 20230

VIA Electronic Mail: privacyrfc2018@ntia.doc.gov

RE: Docket No. 180821780-8780-01: Developing the Administration's Approach to Consumer Privacy

To Whom It May Concern:

The American Insurance Association (AIA) appreciates the opportunity to respond to the National Telecommunications and Information Administration's (NTIA) Request for Comment (RFC) on ways to advance consumer privacy while protecting prosperity and innovation. Consumer privacy and data security are priority issues for the insurance industry, and as such, we strive to maintain the balance between protecting consumer privacy and trust while meeting consumer expectations. In addition, our industry has been subject to the Gramm-Leach-Bliley Act (GLBA) and implementing regulations for over two decades. It is from this background that we provide the following feedback.

The RFC outlines a set of user-centric privacy outcomes and high-level goals to foster Federal privacy protections. AIA believes these outcomes and high-level goals are reasonable and support their continued development. In particular, we identify the following goals as fundamental to developing effective Federal action on privacy: Regulatory Harmonization; Risk and Outcome Based Approach; Interoperability; and Incentivizing Privacy Research.

Regulatory Harmonization

The need to "avoid duplicative and contradictory privacy-related obligations placed on an organization" cannot be overstated. As mentioned earlier the insurance industry is subject to the GLBA and implementing state insurance department privacy laws and regulations. Increasingly, states are considering, and adopting, privacy laws that have general applicability to all industries, including insurers. This complex patchwork of federal and state laws creates a difficult compliance environment that could negatively impact consumers rather than help them.

A Risk and Outcome Based Approach

It is important to focus on the sensitivity of different types of personal information when evaluating actual risk and the controls to put in place. Formally documenting the application of privacy principles in appropriately defined circumstances would help ensure that organizations are striking an appropriate balance between risk based due diligence and consumer protection.

Incentivize Privacy Research

The federal government should seek to facilitate and promote research into practical privacy enhancing technologies that will make it easier for businesses to implement privacy controls and lead to better consumer protection. In addition, privacy research, more generally, will foster regulation that actually meets consumer expectations and benefits them rather than establishing excessive regulatory requirements that only create burdensome implementation and execution with no appreciable benefit for consumers.

The RFC provides a distinction between organizations that control data and third party vendors that process it. With increasing migration of data to cloud storage hosted by a handful of providers, consumers and regulators should expect more responsibility and liability of these providers. Perhaps, as part of a privacy research initiative, the NTIA could explore ways cloud providers could educate consumers about shared responsibility, help consumers mitigate privacy risks, and explore ways the providers themselves could further mitigate their cyber risk.

Interoperability

For global organizations implementing technology solutions in multiple jurisdictions, harmonizing national legislation will serve to foster innovation and speed to market, as it will reduce the time spent analyzing and applying multiple privacy regulations. It could also foster international cooperation. For example, if the U.S. was deemed to offer an adequate level of privacy protection, it would establish a robust legal basis to transfer European data to the U.S. without the need for additional measures such as cross-border data transfer contracts for each transfer from Europe to a third party in the U.S.

The risk and outcome-based approach that NTIA identifies as a goal is a well-balanced approach consistent with U.S. privacy expectations and innovation, which we support. As such, it would be helpful to understand, specifically, how such an approach would be interoperable with a regime like the European Union's General Data Protection Regulation. In considering this, it is important to keep in mind developing an approach that would avoid implementing interoperable requirements at the cost of unwieldy procedures into federal regulations.

Some additional areas that NTIA may want to consider are as follows:

Clear Definitions

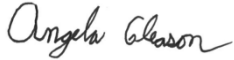
A goal of Federal regulation should be to promote consistent and appropriately focused definitions for fundamental terms. For instance, what does NTIA envision "personal information" to mean? We would recommend that it would be a robust, yet narrowly, defined definition that can be consistently applied in a manner that promotes regulatory harmonization. Additionally, consumer harm is often referenced in the RFC. The focus with respect to consumer harm should be on the use of personal information to the detriment of the consumer. Harm may be more than tangible economic harm, but it should not be speculative or theoretical. Finally, what does transparency mean to NTIA? While consumers should have the right to transparency with respect to their data, there should be limits that can be assessed through increased privacy research and by asking questions like, to what extent does a consumer need transparency? For example, do consumers need to know the details of how an organization stores their data or is it sufficient that they broadly know the organization has a security program in place to protect the consumer's data.

Importance of Data

Data is critical to innovation and developing products that meet consumer demands and expectations. Data is critical to the development of new technologies such as, artificial intelligence and autonomous vehicles. Also, gathering data to serve the greater good is an objective of many technologies such as, the Internet of Things and Drones. NTIA could emphasize these benefits in greater detail, so that the concept does not get lost in policy development.

Again, we thank the NTIA for their thoughtful approach to balanced privacy perspectives. We welcome the opportunity to answer any question you may have or to be of further assistance

Respectfully submitted,



Angela Gleason
Senior Counsel