Internet Association

The unified voice of the internet economy / www.internetassociation.org / @internetassn

Internet Association's Response to NIST's Request for Information: Developing a Privacy Framework Docket No. 181101997-8997-01

Introduction

Internet Association ("IA") welcomes the opportunity to comment on the National Institute of Standards and Technology's ("NIST") Request for Information: Developing a Privacy Framework ("RFI"). IA's mission is to foster innovation, promote economic growth, and empower individuals through the free and open internet. IA is the only trade association that exclusively represents leading global internet companies on matters of public policy.

IA commends NIST's efforts to enhance the privacy protections provided to individuals' personal data through the development of the NIST Privacy Framework: An Enterprise Risk Management Tool ("Privacy Framework" or "Framework"). The Privacy Framework has the potential to be a valuable guide to organizations of all types and sizes as they account for privacy risks as part of their overall risk management strategy.

IA recently released its own framework for protecting privacy, "IA Privacy Principles For A Modern National Regulatory Framework" ("IA Principles"), with a focus on providing guidance for federal privacy and security legislation. IA believes that there is an urgent need for a national standard for personal data protection to provide individuals an appropriate level of privacy regardless of where they may live and with whom they share their data. The IA Principles recognize the importance of providing meaningful privacy protections while maintaining the flexibility needed to allow innovation to flourish. IA appreciates that NIST is committed to the same goals of enhanced personal data protection and maintaining an environment that fosters innovation.

IA has chosen to focus its comments on the proposed minimum set of attributes for the Privacy Framework in response to Question 8 posed by the RFI, as IA believes the minimum attributes can provide guiding principles to help NIST achieve the goals of the Framework.

Minimum Set of Attributes for the Privacy Framework

NIST has proposed establishing "minimum attributes" for the Privacy Framework to guide the process and remain focused on the stated objective of "a prioritized, flexible, risk-based, outcome-based, and cost-effective approach that can be compatible with existing legal and regulatory regimes in order to be the most useful to organizations and enable widespread adoption." 83 F.R. 56824 at 56825. IA agrees that the proposed minimum attributes are a beneficial starting point for developing the NIST Privacy Framework. We would like to emphasize certain elements of the minimum attributes as critical to the success of NIST's efforts.

Minimum Attribute: Compatibility with other Privacy Approaches (#6)

It is important that the NIST Privacy Framework supports compliance with privacy laws, and therefore, the Framework must be compatible with existing, and future, U.S. and international privacy regimes. The current patchwork of state, federal, and international laws on data privacy and security imposes significant regulatory burdens on companies without necessarily resulting in better protections for individuals. As new privacy laws proliferate, so do official guidance documents, opinions, recommendations, and checklists. In addition, there are currently a number of self-regulatory measures that companies have voluntarily undertaken to promote sound privacy practices and to build consumer trust such as the Network Advertising Initiative's Code of Conduct. Codes of conduct and certifications are likely to become more popular as they become accepted methods to show regulatory compliance, for example under Section 5 of the EU's General Data Protection Regulation. Comprehensive federal privacy and security legislation can provide consistency in standards and obligations across the U.S. and ease compliance burdens for many companies. Internationally there is unlikely to be a single privacy standard, as countries develop approaches that are appropriate to their unique needs, cultural values, and legal systems.

NIST should be mindful that companies, particularly online services, are increasingly global in scope and will need to meet obligations of laws outside the U.S. IA agrees with the National

Telecommunications and Information Administration's ("NTIA") naming interoperability as a High-Level Goal for Federal Action on privacy, noting the importance of harmonization in the comments IA submitted in response to the NTIA Request for Comments on Developing the Administration's Approach to Consumer Privacy. If NIST is able to establish and maintain a Framework that aligns global privacy requirements, the Framework will be able to serve its intended function as an internal tool to assist in assessing and managing privacy risks, including legal risks. Without proper alignment, the Framework is unlikely to realize its full potential as a tool for assessing global privacy obligations.

Minimum Attribute: Adaptable (#3)

NIST has articulated a number of critical concepts within its minimum attribute on adaptability, including seeking a Framework that applies across sectors, size and scale of companies, and geography. IA agrees that to achieve benefits for individuals and companies the Framework must provide the same protections for personal data across most sectors, regardless of whether it is gathered offline or online, except for those sectors, such as financial services and healthcare, where there are existing federal laws that cover how personal information must be treated. While federal legislation is critical to creating this baseline standard and harmonizing approaches, NIST's Framework can best support or anticipate such a baseline standard by building in a cross-sector approach, inclusive of online and offline data processing activities, that is scalable to organizations of all sizes. IA also agrees on the importance of the Framework being "technology-agnostic" in order for the Framework to remain a relevant tool as innovation continues, new privacy-enhancing technologies are developed, and disruptive new business models emerge.

Minimum Attribute: Risk-based, Outcome-based, Voluntary, and Non-Prescriptive (#4)

IA applauds NIST for its focus on achieving meaningful outcomes for individuals, and for seeking to maximize data privacy and security through a flexible approach focused on addressing the risks that are presented in specific data processing scenarios. Too much of today's privacy regulations and frameworks assume that the risks to individuals are the same across a range of transactions if, for example, the data at issue is of the same type. The reality is that the risks to individuals, as well as their ability to assess and make informed decisions regarding such risks, vary considerably depending on the context of their relationship with the entity collecting their data and the context in which they provide their data. One-size fits all mandates have resulted in consumers being inundated by long, dense, legal documents that are designed to provide "notice," but frequently fail to adequately educate individuals about how their data will be used and what choices they may have related to those uses. To achieve better privacy outcomes for individuals, legal frameworks and the tools that support compliance with such frameworks should be built to recognize and assist in an analysis focused on the risk to the individual. These frameworks and tools should encourage adoption of measures to mitigate the risks in a manner flexible enough to allow for new and better approaches to be developed to achieve the desired privacy outcomes.

IA also agrees that the NIST Framework should be voluntary. NIST has set ambitious goals for the Privacy Framework, and balancing the need to align and support legal compliance on a global basis and having a living document with a transparent and open process for establishing and evolving the Framework may be challenging. It is critical that organizations that are subject to privacy laws are able to prioritize compliance with legal requirements over their adoption of specific risk-management tools.

Minimum Attribute: Common and Accessible Language (#2)

Common and accessible language is a critical component of transparency, which IA believes is a core principle for a national privacy framework. For example, IA's Principles specifically state that "a national framework should give individuals the ability to know whether and how personal information they provide to companies is used and shared with other entities, and if personal information is shared, the categories of entities with whom it is shared, and the purposes for which it is shared." To achieve better privacy outcomes for individuals, privacy standards need to be more consistent, should focus on reasonable consumer expectations in the context of the nature of their interactions, and be communicated in a way that consumers can understand. It will further enhance privacy protections for individuals if the privacy requirements and the tools that support compliance are accessible and understandable to personnel within companies who are not lawyers, privacy professionals, or technologists. IA believes that any privacy framework should be sufficiently detailed and clear, so that the standards will be easily understood by individuals and straightforward for companies of all sizes to implement. IA applauds NIST's commitment to transparency in the process of creating the Privacy Framework and believes that the use of common and accessible language through the process will support public discourse on this important issue.

Minimum Attribute: Useable as Part of Broader Risk Management Strategy (#5)

NIST's Privacy Framework should make it easier for organizations to understand how measures implemented for the protection of individual personal data may intersect with and impact other risk management strategies. In certain instances, cybersecurity best practices may enhance personal data protection through technical measures, such as encryption. In other instances, organizational decisions to protect personal data (e.g. minimizing the collection or retention of personal data) may result in a diminished ability to protect the systems where such data may be processed from other threats to company systems (e.g. investigating fraud or other security risks) which could have far-reaching adverse effects. Data minimization could also adversely impact the ability to assess and correct discriminatory impacts of decision-making processes. It will be helpful if NIST's Privacy Framework can guide organizations through a holistic consideration of privacy protection measures and organizational impacts.

Additional Considerations for Minimum Attributes

As noted above with regard to the minimum attribute for usability in the broader risk management context, NIST's Privacy Framework can play an important role in helping organizations understand the trade-offs that may exist for implementing certain data protection techniques. Another important area where the Privacy Framework may be helpful could be guidance on assessing the impact of the exercise of individual data rights — such as access, correction, portability, and deletion — on other individuals' rights and freedoms. IA recognized the importance of individual rights to control personal data in the IA Principles by including access, correction, deletion, and portability as key elements of a national privacy framework. IA likewise recognized that these rights must be carefully balanced against the privacy and security interests of other individuals' in their own personal data as well as their interests in the exercise of their other rights, including freedom of expression. NIST's Framework could help organizations identify potential conflicts and suggest practices that might reduce risks, such as developing procedures to validate individuals' identities prior to responding to data access requests.

Conclusion

IA appreciates NIST's commitment to an open and collaborative process for developing the Privacy Framework and looks forward to further opportunities to provide input as the effort progresses.