Date: February 14, 2019

Comment from the Internet Society on the
National Institute of Standards and Technology's
Request for Information on Developing a Privacy Framework

Docket No: 181101997-8997-01

The Internet Society is pleased to submit these comments in response to the National Institute of Standards and Technology's (NIST) Request for Information (RFI) on Developing a Privacy Framework.[1]

The Internet Society is a global not-for profit organization committed to the development, evolution and use of an open, globally-connected, secure and trustworthy Internet for the benefit of all people throughout the world. We work in partnership with our global community, consisting of 50,000 members, 136 chapters and special interest groups, and 149 organizational members. The Internet Society is also the organizational home of the Internet Engineering Task Force (IETF)[2] and the Online Trust Alliance (OTA) initiative[3].

Privacy is an important right and an essential enabler of autonomy, dignity, and freedom of expression for individuals. The ability for individuals to interact online without sacrificing their privacy is key to reinforcing user trust on the Internet. When privacy is undermined, it exposes users to actual and potential harm, undermining user trust and thereby diminishing the value of the Internet.

The Internet Society applauds NIST's action to develop The *NIST Privacy Framework: An Enterprise Risk Management Tool* ("the Framework"), and the agency's plan to develop the Framework in a "consensus-driven, open, and collaborative process." Just as the *NIST Framework for Improving Critical Infrastructure Cybersecurity* did in the security domain,[4] the Privacy Framework presents an opportunity to provide a powerful toolset for assessment and improvement of an organization's privacy management strategy, policy, and practice, with the end goal being better organizational privacy practices.

Open, transparent, consensus-driven process

We welcome the clear statement of an open, transparent and consensus-driven approach to defining and developing the Framework (bullet #1 of the Development and Attributes section of the RFI). In this approach it is important to ensure that all stakeholders are adequately represented in the process. "Adequate representation" must mean representation that compensates for any built-in power imbalances between stakeholders. If a powerful stakeholder is dominant in the process, careful consideration should be given as to what safeguards could be put in place to ensure that less powerful or audible stakeholders are represented in a way that gives adequate weight to their legitimate interests.

[1] https://www.federalregister.gov/documents/2018/11/14/2018-24714/developing-a-privacy-framework
[2] https://www.ietf.org/
[3] https://otalliance.org/
[4] https://www.nist.gov/cyberframework

A Risk-Management Approach to Privacy

The RFI specifies that a goal of the Framework is to “help organizations better identify, assess, manage, and communicate privacy risks.” While risk management can support a successful approach to privacy for organizations, it is critical that such an approach also mitigates risk to individuals and third parties (whose personal data may be explicitly or incidentally collected), rather than solely the risk faced by the organization. Risk management approaches often aim to minimize risk to the organization handling the data, not to the individuals whose personal data they hold. For some organizations, the risk that poor security or privacy creates may not extend to them. Instead, it may seem riskier to spend resources on data security and privacy than to use them elsewhere in the business.[5]

The success of the other goals of the Framework, to “foster the development of innovative approaches to protecting individuals' privacy” and to “increase trust in products and services,” relies heavily on ensuring that the risk management approach takes individuals and third parties into consideration. If the privacy risks of individuals are not deemed a risk to an organization, they will not be encouraged to develop innovative approaches to protect the privacy of individuals. It will be crucial to ensure that the Framework carefully links individual privacy risk, its effect on an organization, and how to manage the privacy risk of individuals and third parties within an organizational privacy risk-management approach. We recommend that any risk-based approach to privacy management be carefully assessed to ensure that it adequately represents the interests of individuals (data subjects), thus avoiding a disproportionate focus on enterprise risk to the exclusion of other legitimate interests.

Bullet #4 of the Development and Attributes section of the RFI mentions the idea of a flexible voluntary ‘catalogue’ of approaches, which is sensible, but it is likely to require careful monitoring of the resulting outcomes to ensure that organizations do not simply "cherry-pick" a subset of catalogue items that allows poor practice to continue essentially unchanged (while claiming compliance with the Framework).

Assessing Privacy Risk: Selected Current Approaches

Past experience suggests that one of the most difficult aspects of the Framework will be identifying and assessing privacy risk. Identifying and assessing privacy risk for organizations, individuals, and third parties may be a daunting task. In recent years, the number and sophistication of privacy risk assessment tools has increased. Many focus on discrete areas – like the privacy of a device, a website, or data at rest. In our view, these narrowly-focused risk assessments are a necessary but insufficient part of a more comprehensive, organizational approach that considers the full range of privacy risks and applicable mitigations. In some instances, best practice in one tightly-focused domain is also applicable in other areas of organizational risk management, and a broad-based approach will help the organization ensure that best practice is propagated across functional silos and use cases.

[5] https://www.internetsociety.org/blog/2017/10/current-approach-data-handling-isnt-working-equifax-breach-illustrates/

Two examples of broader-based approaches:

The Online Trust Alliance Trust Audit ("the Trust Audit") provides a "comprehensive evaluation of a site's best practices in brand and consumer protection, security, and privacy." Since its inception in 2009, the Trust Audit has continued to refine its methodology for analysing the privacy and data protection practices of an organization's website.[6] Importantly, this methodology not only assesses a site's management of privacy risk for individuals, it also assesses how a site communicates its practices to its users.

Each year, the Audit analyses over 12,000 consumer-facing websites, including top retailers, banks, consumer service sites, government agencies, news and media companies, Internet Service Providers, mobile carriers, email providers, web hosts, and in 2018 healthcare related websites including genetic testing sites.

These sites are then awarded points for their implementation of security and privacy standards, and penalized for vulnerabilities, breaches, and regulatory settlements across the following categories: Domain, Brand, and Consumer Protection; Site, Server, and Infrastructure Security; Privacy, Transparency, and Disclosures. All sites that score above 80% and receive 60 points in each category (out of 300 total points across all categories) are included in the Honor Roll.

The audit measures a range of issues regarding privacy and security best practices; from how best to inform users on unsubscribing form email lists, to the use of encryption when transmitting data, to useful privacy policies.

Included in this wide range of measurements is an assessment of each sites' consumer facing privacy policy. Each privacy policy is graded on over 20 variables. These include: informing users that their data may be shared with third parties, what specific data may be shared, and what choices users' have to control their data. The audit covers many other aspects of each company's privacy policy, but the goal is to quantify how well top companies and websites are communicating with their users about privacy issues.

Mozilla's "Privacy Not Included" provides privacy assessments for consumer Internet of Things (IoT) devices to create a buying guide for gifts over the holiday season.[7] Privacy Not Included measures the implementation of security and privacy best practices in IoT devices, particularly focusing on their effects on their users.[8] Like the Trust Audit, Privacy Not Included also looks at specific privacy practices, such as policies on data retention and sharing of user data with third parties, and the clear communication of these practices to their customers.

Conclusion

As NIST formulates the privacy risk assessment methodologies for its Framework, the Internet Society would welcome the opportunity to consider and provide input on the potential technical

[6] https://otalliance.org/2018-online-trust-audit-methodology
[7] https://foundation.mozilla.org/en/privacynotincluded/
[8] https://foundation.mozilla.org/en/privacynotincluded/about/

implications (if any) of those methodologies. Further, through our global community, we have the opportunity to bring a global and cross-jurisdictional perspective on privacy to this work.

The Internet Society welcomes this opportunity to share its views with NIST through the Request for Information on Developing a Privacy Framework. We are encouraged by NISTs commitment to pursuing an open, multi-stakeholder process in developing the Framework, and look forward to continued engagement in this process.