Deloitte.

NIST Privacy Framework: Deloitte's RFI Response

Table of Contents

Deloitte.

1. Introduction

Deloitte[1] (or "we" or "our") appreciates the opportunity to respond to the National Institute of Standards and Technology ("NIST") Request for Information ("RFI") regarding the NIST Privacy Framework: An Enterprise Risk Management Tool ("Privacy Framework"). The following response is based on the collective experience of Deloitte's cyber risk professionals specializing in privacy and data protection.

Privacy is a growing concern of the general public, private and public organizations, and government agencies worldwide. Data breaches and other misuses of personal data are frequently reported in the media and, as a result, privacy laws are continuing to evolve and mature. Deloitte has provided cyber risk services across multiple industries to help organizations prepare for upcoming privacy legislation, identify and mitigate privacy risks, investigate data breaches, and develop and implement programs to mature an organization's privacy and data protection posture.

At its core, privacy rights and protections are intended to balance an individual's desire to control how their personal data is used by others and the need for organizations to collect, share, and process that personal data in the course of their business with realistic and predictable privacy controls in place. Identifying this balance is a challenge faced by many organizations and our observation is that these organizations will likely welcome the NIST Privacy Framework as a source of actionable guidance. However, while there is a temptation to produce a prescriptive set of privacy standards and requirements, recent history has shown that privacy evolves quickly and so the Privacy Framework should anticipate further advances in US and global privacy laws and standards.

Privacy is one of many concerns that today's organizations should manage and incorporate into their enterprise risk management strategies. Organizations without enterprise risk management programs face a significant challenge as there may not be a foundation on which to build a privacy program. Even organizations with established enterprise risk management programs may need to deal with international privacy requirements and determine how to resolve conflicts between laws in various jurisdictions.

To reduce variations in business and operating practices, some organizations rationalize global privacy requirements by distilling common requirements found in multiple sources and consolidating them into a set of unified privacy requirements. We anticipate the NIST Privacy Framework to be used in the following ways: A) as a standalone framework, B) along with the existing NIST Cybersecurity Framework, and C) as an input to rationalized global laws, industry leading practices, and other sources of privacy requirements.

With that in mind, we selected several of the topics raised in the NIST RFI to respond to and our responses to these questions are respectfully submitted below.

2. Organizational Considerations

A. How should a framework balance organizational maturity to protect individuals?

To some, a "privacy program" is the function within an organization that identifies, addresses, and is accountable for matters related to privacy. The lens through which they perform their duties, however, may be classified as compliance or regulatory in nature. As global privacy standards and laws have matured, particularly in the European Union with the introduction of the General Data Protection Regulation, we should also consider the human element of a privacy program. In other words,

[1] As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

organizations should look past the legal requirements, and seek to implement privacy practices to protect *people* from the potential misuse of their data. The NIST Privacy Framework should encourage this effort by promoting a focus on preventing harm to individuals.

One method that can be considered to reduce harm to individuals is to require "privacy by design" principles be embedded in business processes that involve the processing of personal data. Privacy by design (and by default) aim to reduce the frequency and magnitude of data misuse by proactively exploring where privacy considerations should be addressed in the development of new and changed systems and processes. This approach reduces the number of data misuses that "slip through the cracks" and lead to individual harm through data incidents and breaches. However, because privacy is about how data is *used*, and not just how it is secured and with whom it is shared, implementing privacy by design can be complex and challenging.

For the NIST Privacy Framework to reduce harm to individuals, it should strike a balance between mandating privacy by design and dictating how privacy should be implemented. In the former case, too much room for interpretation may lead to inconsistent practices that are difficult to benchmark, and—in the latter case—organizations may be tempted to satisfy the letter of the law rather than its spirit. Further complicating the situation is how legacy data and data shared with third parties should be handled. Retroactively implementing privacy by design to legacy systems may be impractical and monitoring third parties for compliance with contractual provisions may be similarly unlikely.

Controls perceived as impractical or inapplicable may lead organizations to discount the value of the Privacy Framework as a whole. Particularly challenging controls include—for example—legacy systems and data, inventorying and classifying unstructured data, and *enforcing* data privacy terms with third parties, etc. The Privacy Framework could assist in mitigating this challenge by providing alternative minimum requirements designed to reflect various levels of maturity. In addition, the Privacy Framework could assist organizations in more accurately assessing themselves while providing them with clear objectives for improvement. Likewise, organizations conducting privacy risk assessments on their vendors could have the option of accepting various levels of maturity based on their risk tolerances.

The minimum requirements should be sufficient to protect individuals from harm. By analogy, newcomers to the pharmaceutical market do not expect to have an easier time getting a drug to market than an established firm due to more lenient requirements for the newcomer.

B. How may industry practices and existing compliance approaches affect organizations?

We engage with many organizations that are prepared to "do what it takes" to protect individual privacy. Yet often, doing what it takes means different things for different organizations. Developing and implementing useful, cross-sector frameworks is challenging due to the differing regulatory requirements and the purposes for which organizations are processing personal data.

Many heavily regulated organizations see themselves as well prepared to adapt to changing laws or regulations due to well-developed business development and compliance processes, yet even these processes often operate in a siloed manner. Even so, they are often more prepared as they maintain compliance and legal functions to interpret and implement applicable changes to mitigate emerging privacy risks. Less regulated companies are often building privacy compliance structures based on compliance with applicable law and regulation, yet addressing privacy concerns in reaction to emerging issues, breaches, and media coverage.

Besides the state of an organization's regulatory environment, another challenge to creating a universal framework is the purpose of processing for an organization. Organizations that use personal information incidentally (e.g., process payment card information) do not have the same purpose of processing as organizations that use personal information as the product (e.g., commercialization of personal data for targeted marketing). These organizations handle information differently because of the added operational risks to which they are exposing themselves—and their customers—through the processing of the customer's personal data.

Ultimately, developing a universal framework is not the toughest challenge. A tougher challenge is to create a framework that can lead to the practical implementation of practices that will protect an individual's privacy. Organizations that are heavily regulated have processes for incorporating these types of considerations into existing frameworks, yet even regulated industries may struggle to implement practices that span disparate functional domains such as privacy and procurement.

Privacy has become a new standard for organizations processing personal data, which perforce includes startup and smaller companies which will have a more difficult time implementing the Privacy Framework.

The challenge is not tailoring a framework for different industries, but helping entities operating at different levels of privacy compliance in implementing broad privacy protections through a framework.

C. How do organizations incorporate changes to privacy laws and risks?

Organizations handle new privacy laws or changes in privacy risks through a diverse range of approaches. Their approach may depend on multiple factors, including the size and scale of the organization, the types of and sensitivity levels for the data they process, the dedication of staff to data protection and privacy, and resources and tools they may have available to monitor changes in risk. It can also vary depending on the specific application of a new law to a specific industry or type of business (e.g., new health privacy law and impact on health providers).

From our experience, we have found that the following steps can be taken by organizations to address new and emerging privacy risks:

(1) Build awareness of new regulations or risks and determine applicability
(2) Gauge the impact of risk through assessments and Privacy or Data Protection Impact Assessments
(3) Monitor organization and change management processes to recognize activities that could change the impact of risk

1: Organizations may be alerted to new regulations or changes to privacy and data risk through multiple methods. Large organizations typically leverage law firms and/or professional services firms that provide periodic newsletters and email notifications when there are potentially impactful changes in privacy law. Smaller organizations typically discover new regulations at a later interval and monitor changes in laws, regulations, and guidance through publications by trade associations.

It is important that organizations watch the legislative and judicial process to determine when regulations are in their final form and become a requirement or legal directive. This determines when requirements are applicable to that organization's business as there may be months or even years when draft versions of laws are circulating, but not yet legally binding.

2: Once the new laws or regulations have been finalized, the organization determines the potential impact that it may have upon them. Many organizations use processes such as Privacy Impact Assessments (PIA) or Data Protection Impact Assessments (DPIA) to evaluate changes impacting different areas of their business. Organizations also conduct periodic privacy program assessments of their privacy program, or components thereof, to evaluate the health and maturity needs of their program. The periods of time between program assessments will depend on the speed of change in regulations and the marketplace. Finally, internal privacy audits can be used to periodically evaluate the organization's changes in privacy risk posture, identify gaps in the program that need improvement, and ascertain how well privacy controls are operating.

3: One of the more difficult steps to establish in large, decentralized organizations is to locate and establish change management related processes in which to embed triggers to commence Privacy by Design principles and assessments. This is vital for the strength of privacy compliance and risk management because an evaluation process of changes within an organization that may impact risk is only as strong as the ability to identify those changes as they occur. Therefore, organizations should

identify newly established processes throughout its business, such as in IT and technology requests, Procurement, and Change Management, to notice change that may impact personal data and privacy risk. By establishing triggers in processes, and not depending solely upon employees to notify about changes to risk, privacy programs may gain greater maturity and become more resilient to change over time.

D. How may small privacy programs benefit from greater integration with the organization?

Effective privacy risk management requires coordination and communication across the organization, and a broad viewpoint of risks to the organization. Some privacy organizations, likely due to their newness and recent emergence as a standalone group, focus on specific privacy issues instead of looking at risk holistically. This is as expected. However, it may not be as impactful to the root of the data risk issue for an organization. Many non-privacy professionals have been tempted to measure the achievements of privacy programs by seeing if risk for a specific metric was reduced rather than seeing the value in maturing privacy controls more broadly, resulting in programs that are overly focused on only a few privacy-related risks (e.g., the breach of sensitive data rather than the misuse of non-sensitive data).

Privacy programs, based upon their limited size and reach, may benefit from not remaining siloed from other parts of the business. Many other parts of an organization process personal data daily, including legal, information security, information technology, HR, security, training, communications, marketing, and sales. This expansive reach of privacy concerns and risks within an organization necessarily implies that privacy programs, with their limited staff numbers and inability to be everywhere at once, may need to team with these other areas of the business to carry forward the message from the privacy program. However, that does not mean that the business alone should be making privacy decisions. The privacy program will still need to monitor and advise on specific legal and privacy issues as they emerge.

Privacy practices have historically focused on providing legal guidance and support to the business to comply with privacy laws and regulations. This approach works well for rules-based regulations, yet the principles-based regulations that continue to emerge require greater operational input. Privacy is often not centrally managed within an organization. The privacy office may own the policies, but they limit their role to advising and guiding the business, and then may guide the business to determine how to implement processes to meet the policies. The privacy office may need to take a more active role in leading the implementation of policies within the business, particularly for new and more demanding privacy requirements.

3. Structuring the Privacy Framework

A. How may the Cybersecurity Framework be leveraged to develop and maintain the Privacy Framework?

The Cybersecurity Framework—particularly the security objectives of confidentiality, integrity and availability—should inform the Privacy Framework and provide guidance in addressing privacy risks that result from unauthorized access to information. Additionally, the Cybersecurity Framework should be aligned with the Privacy Framework so that organizations' security activities do not lead to privacy risks and/or hinder achievement of privacy outcomes laid out in the Privacy Framework.

B. How may the Privacy Framework be structured?

The Privacy Framework can be more useful to organizations if structured around specific requirements and controls that support the privacy goals of organizations. Therefore, we support the idea of incorporating the NIST privacy engineering objectives of predictability, manageability, and disassociability into the Privacy Framework and using these objectives to translate existent privacy

principles and practices into controls, to the extent possible. While this may be a burdensome task for some, the outcome should benefit organizations by helping them operationalize and implement privacy principles and practices. There is also an opportunity to leverage components of the Cybersecurity Framework to help organizations create target goals and prioritize activities with considerations for context and organizational needs.

4. Specific Privacy Practices

A. Why may the ethical use of data be one of the more important and more challenging aspects of privacy practices?

NIST lists several privacy-enhancing practices (e.g., de-identification, transparency, preferences, encryption) and solicits input on whether these practices are in use at organizations and whether there are other practices that should be included in the Privacy Framework. Two sometimes overlooked aspects of privacy frameworks are: 1) their ability to predict future misuses of personal data and the practices needed to prevent those misuses, and 2) their treatment of ethical considerations that overlap with privacy.

1: Constant political and technological changes make future information misuse unpredictable. History has shown that seemingly innocent information, such as political party affiliation, can be misused. In the 1930s, many Americans vehemently opposed to fascism joined socialist groups to demonstrate their opposition to fascism. This affiliation was later used in the 1950s to deny employment, among other misuses. Crucially, at the time people joined these groups, it was not expected that these relationships would be used decades later in such a manner. Will the same fate befall genetic data currently processed to explore people's ancestry, medical risk factors, and other reasons? If the aim is to protect people from harm, organizations should work to look decades into the future while simultaneously not stifling innovation.

2: Ethical concerns related to privacy present themselves in both obvious and latent forms. Tracking someone's browsing habits is commonplace today, but using this data to modify the news stories they see poses unforeseen risks. Similarly, profiling and targeting users may alter their behavior thus impacting free choice. This concern is not hypothetical. There is evidence that demonstrates that people will limit their searches for sensitive health conditions if they believe their searches are not private thus potentially depriving them of appropriate medical care.

To return to the questions raised by NIST, yes, many organizations use the practices listed in the RFI; however, these practices alone may not prepare organizations for the privacy issues they will likely face in the future. The Privacy Framework should be developed such that it encourages its users to conduct (and periodically reconduct) further privacy analysis, for example a privacy impact assessment, so that the latest known privacy issues can be identified.

B. What are the implementation challenges of maintaining Notice?

The practice of providing a current and transparent notice to data subjects poses a significant implementation challenge to many organizations, and in particular for technology startup companies. Providing a transparent and current notice is one of the fundamental privacy practices upon which consumers and regulators alike depend, as the legally binding provisions articulate the details of the types of data processed, the purpose behind its collection and processing, what the organization is doing with the data, with whom it is shared, and the measures taken to secure the data in relation to its sensitivity. Given the legal ramifications of the notice, it becomes even more important to regularly review and update it for changes in an organization's business and data processing activities.

Technology startups are characterized by their rapid innovation and accelerated product development lifecycle. Further, startups may also experiment with their business models in their attempt to grow and become viable in the marketplace. Both of these factors contribute to the challenge of developing and keeping current a transparent privacy notice. These companies are presented with the following options:

1) Update the privacy notice when data is to be processed differently, such as when new features are added or removed
2) Draft the privacy notice in a manner such that it does not require constant updates, but is less valuable to individuals

Option 1 is undesirable because it could be costly, difficult to track, result in update fatigue, and would risk being inaccurate. Option 2 is similarly undesirable as an overly vague notice fails to perform the single function it is designed to do, namely to provide *notice* of the data processing activities. As mentioned previously, startups and other companies employing this methodology should not be given a free pass to use personal data as they please, but consideration should be given to how notice requirements are drafted to account for these use cases.

C. Are the listed privacy practices relevant for new technologies like the Internet of Things?

Internet of Things (IoT) constitute interconnected cyber physical systems equipped with sensors and processing powers that enable the collection, processing, and transmission of large quantities of data. Not unlike online services, IoT-enabled devices raise privacy questions regarding control, data ownership, retention and storage, disclosure to governments, and others. Similarly, they raise concerns about individual and societal harms resulting from loss of privacy due to unauthorized and authorized uses of information. With a few exceptions, the prevailing number of well-established privacy and security practices that have guided technology companies, banks, and online retailers can also help reduce privacy risks of IoT.

IoT sensors, for example, are vulnerable to a host of risks including data exfiltration, identity spoofing, modification of device components, and others. The practices laid out in the NIST Cybersecurity Framework and other security guidelines can help organizations provide the security that is required to avoid loss of privacy from such malicious practices. The privacy practices listed in the RFI such as de-identification and use of cryptographic technology can also improve the privacy conditions of users by increasing anonymity and reducing identification in undesirable contexts.

However, some of the listed practices that have been foundational in privacy frameworks such as enabling user preferences through notice and choice are challenged in the IoT environment. The real-world interfacing IoT sensors can and do collect information from those not aware (e.g., the ambient data collection by Internet Protocol cameras or smart toys) without granting them the opportunity to consent, customize available privacy controls, or exercise individual rights. Further, the collection and sharing of meta-data is also a growing concern.

Therefore, the privacy framework should emphasize default privacy configurations—even without user action—such as de-identification, tokenization, limitations on data collection and sharing, end-to-end security, etc. It is also essential that it emphasize assessment of the potential risks for stakeholders and setting of responsibilities for the players in an IoT ecosystem. Additionally, as discussed in a preceding section on ethical uses of information, risk assessments should also aim at continuously identifying and preventing (or reducing) information activities that are not inherently harmful or unauthorized but could lead to a host of harmful consequences.

5. Additional consideration for the type and cause of individual harm

Throughout this comment, we have explored techniques that could reduce the harm to individuals impacted by privacy violations. It is also worthwhile, however, to consider what is meant by "harm" and whether the current regulatory environment and existing privacy frameworks are sufficient to distinguish between different types of harm. Consider the following two scenarios and decide which

results in greater harm: Scenario A) the mild misuse of personal data, or Scenario B) the loss of personal data with the potential for more extensive misuse.

In Scenario A, such as when individuals receive unsolicited emails or text messages after providing contact information for another purpose and do not explicitly consent to that type of messaging, there is an actual harm to individuals. They shared personal data and it was misused (e.g., an email address was provided to a bank to only receive electronic statements and now unrelated marketing materials are received). Contrast this with Scenario B, such as after a database containing credit card numbers has been breached, when the majority of individuals whose data was stolen suffer no immediate harm. Not everyone's credit card number will be fraudulently used, for those numbers that are misused individuals are generally not financially responsible, receiving a new credit card number is only a minor inconvenience, and the percentage of people who then have their identity stolen is only a fraction of the people whose data was breached.

Scenario B type stories dominate the news despite them only *potentially* harming many of the people involved and Scenario A type stories are essentially ignored by the public. The Privacy Framework is an opportunity to call out this discrepancy and shift the balance and reduce actual harm to individuals.

6. Conclusion

Privacy is both simple and complex. People may be passionate or indifferent about their personal privacy, but they have an intrinsic sense of what privacy means to them and through that lens privacy is simple. Simultaneously, privacy is complex in that it directly impacts legal requirements, technology, security, as well as ethical considerations. We applaud NIST's efforts to develop a Privacy Framework that contemplates addressing this paradox of simplicity and complexity.

Deloitte appreciates the opportunity to share our observations and analysis derived from our extensive experience advising clients with respect to their challenges in developing effective, risk-based privacy programs. We look forward to continuing to share our insights in workshops and other forums NIST makes available. Once completed, the Privacy Framework will be utilized by countless organizations to carry out NIST's objective of improving organizations' management of privacy risks. We share this objective and thank NIST for considering our thoughts and perspectives.

Contact

For further information, please contact

Dan Frank
Advisory Principal | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
