Developing a Privacy Framework

“Request for Information on Developing a Privacy Framework” Submitted by Nuix
Docket No. 181101997-8997-01

The following comments are in response to specific questions in the RFI but not necessarily on covering all aspects of all questions. The suggestions come from our observations of practitioners in the privacy discipline using specific technologies to identify, organize and respond to privacy imperatives.

About Nuix
Nuix (www.nuix.com) understands the DNA of data at enormous scale. Our software pinpoints the critical information organizations need to anticipate, detect, and act on risk, compliance, and security threats.

Our intuitive platform identifies hidden connections between people, objects, locations, and events—providing real-time clarity, control, and efficiency to uncover the key facts and their context.

Organizational Considerations

1. *The greatest challenges in improving organizations' privacy protections for individuals;*

One of the biggest knowledge gaps that organizations have when establishing a privacy framework is having a clear idea of what information they have and where it resides. Building an effective data inventory and map involves several aspects:

A. What types of data are managed – privacy data elements can be related to location, health, physical characteristics, finances, or several other categories. To be able to appropriately track and protect this data, it helps to know what categories of data you capture.
B. In what platforms and formats does it reside. Familiarization with data platforms will help design an appropriate technology and schedule for maintaining a data inventory
C. Where is it physically located? Location impacts jurisdiction
D. Understanding who is responsible for capture, management, and protection

Without this knowledge, organizations may be missing large collections of private data. A privacy framework should provide guidance on how to ensure a comprehensive definition and inventory.

2. *The greatest challenges in developing a cross-sector standards-based framework for privacy;*

When creating a cross-sector framework, it seems logical to take the requirements and scopes of as many identified and existing regulations as practical to build an overall framework. As a result, compliance with the framework will increase the likelihood of compliance with a greater number of external regulations. All regulations have some varying degree of some standard activities from a functional perspective. These functions often span internal organizational structures to the overlap is not always visible. At each level, specific standards could be employed to identify appropriate levels of rigor for that function given the industry or sector. As a preliminary list of functions that can be found in many regulations and standards, the following items are organized around three stages:

Plan – Steps to develop an internal program for privacy compliance

A. Identify PII types and associated risk – How does one's particular organization capture and manage personal data related to identity, location, health, and finance? This can be done through interviews of key data stewards and by indexing existing content systems to identify data element types
B. Build a Data Map – Document the location and platform where each to the above data types are located. This map can serve to prioritize activities around content collections for index, audit, retention, protection and search
C. Plan access, security and incident response – When mandates for time sensitive responses are required by regulation, an Incident Response Plan, identifying responsibilities, activities and technologies, should already be in place.

Implement – Making changes to the way information is governed so that greater and more responsive compliance is possible. Specific implementation activities suggested or required by numerous regulations include:

A. Information Governance enhancements including transfer to ECM, relocation and migration of content to different storage or segments, or tagging and labeling content to make search, disaster recovery, retention, and production easier
B. Security enhancements including new perimeter technologies, network security groups, and endpoint activity monitoring so that personal data is more secure.
C. Activity enhancements including report and log management, database meta-modeling, process mapping, consent gathering
D. Responsibilities and personnel including Data Protection Officer designation, records and security liaisons, incident response responsibilities
E. Mitigate dangerous or unnecessary content through data minimization activities including retention management and purging, encryption in place, anonymization
F. Manage records to ensure they are kept long enough but not kept too long

Response - Often constrained with deadlines and can be initiated by data subjects, regulators, litigants or other actors. Response activities prescribed by numerous regulations include:

A. Gather consent – Organizations gather documented evidence of opt-in or opt-out preferences
B. Report activities
C. Subject or Information Access Request – So that an individual or entity can see what data is being used
D. Right To Be Forgotten – So that an individual can opt out of their data being used
E. Monitoring activities around managing data
F. Filtering – To prevent responsive data from being moved inappropriately
G. Breach Investigation

6. How senior management communicates and oversees policies and procedures for managing privacy risk;

A policy compliance framework in an organization should include:

- Consistent, accessible and understandable policies
- Technology to both support and measure compliance
- Communication and training followed up with auditing
- Process and activities with subsequent continual improvement

8. The minimum set of attributes desired for the Privacy Framework, as described in the Privacy Framework Development and Attributes section of this RFI, and whether any attributes should be added, removed or clarified;

Determining attributes should be focused on identifying attributes that are minimally sufficient for someone to be able to:

- Create a false identity
- Steal
- Find you if you do not want to be found
- But don't add a lot of noise

One specific attribute that could be clarified is that custom numbering systems, used for employee IDs, account numbers, and so forth, should be made to be more easily identified in content. For example, a 9-digit (otherwise random) number is very difficult to distinguish from other numbers like a social security number; making it into a pattern will also make it easier to locate and protect.

10. What standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles organizations are aware of or using to identify, assess, manage, and communicate privacy risk at the management, operational, and technical levels, and whether any of them currently meet the minimum attributes described above.

Index and classification management tools can index corporate data across many platforms, languages and geographies. These tools:

- Index – Extract text, data, metadata, attributes, coordinates, colors, and other elements of all digital objects in a corporate environment
- Identify number and word patterns for privacy attributes
- Classify according to content
- Reduce false positives
- Remediate risky content so that network security, encryption, and relocation can all be used to better protect personal data.

13. The role(s) national/international standards and organizations that develop national/international standards play or should play in providing confidence mechanisms for privacy standards, frameworks, models, methodologies, tools, guidelines, and principles;

Using a specific tool should not be a requirement or else people will adhere to the minimum compliance level and no further.

Specific Privacy Practices

In addition to the approaches above, NIST is interested in identifying core privacy practices that are broadly applicable across sectors and organizations. NIST is interested in information on the degree of adoption of the following practices regarding products and services:

- De-identification is a valuable process for information that taken out of its native environment to be shared between organization or function. It cannot be easily de-identified and still be useful for its original purpose.
- Enabling users to have a reliable understanding about how information is being collected, stored, used, and shared. The difficulty in the GDPR requirement that allows for a data subject to see their content in native format is that often that will expose others' personal content to that first data subject. For example, a spreadsheet that lists former employees' travel credit cards cannot be easily shown to a former employee when requested. Allowing for transformation, rendition, redaction is important for this process.

20. Whether, in addition to the practices noted above, there are other practices that should be considered for inclusion in the Privacy Framework;

Guidelines around the employee termination and transfer process to eliminate PII from corporate systems when no longer needed.