Comments on NIST's *Developing a Privacy Framework*
83 FR 56824

Comments submitted by:

Andrew Neal

Preface

These comments are submitted as commentary and advisory notes to identify challenges encountered when implementing privacy principals and controls, either framework based or ad hoc, into private sector production environments. These are based on the observations of an information security and compliance professional with several decades of consulting experience and exposure to a wide variety of organizations, industries, frameworks and regulatory regimes.

I did not attempt to reply to each item. I limited my responses to areas where I feel I have some practical knowledge.

Comments

At a high level….

Many organizations have been reactive regarding data-centric regulations, client demands and industry standards, assigning resources as each new requirement draws attention. Inputs include security required by regulation or contract, multiple privacy regulations and related client/consumer demands, IP protection, data collections and analysis as part of business operations, and litigation and regulatory data obligations. As these individual requirements proliferate budgets are being stretched. There is a growing recognition that security, privacy and other governance issues cannot be addressed one regulation or purpose at a time, but must be part of a comprehensive data governance program that incorporates:

- An understanding of the organization's business processes and data flows
- The tools to more precisely target data collection, usage, opportunities, risks and destruction.
- A process or framework with which the complete data management and protection footprint (e.g. security, privacy, regulatory obligation, litigation response, etc.) can be defined, applied and measured.
- Ultimately, the ability to achieve multiple stakeholder wins with a single budget.

Whether this is recognized as an ESRM process or not, it must be part of the organization's business process for it to be effective.

1. **The greatest challenges in improving organizations' privacy protections for individuals;**
   The first challenge we see organizations struggling against is identifying all the data assets produced or utilized by their organization. High level process flow diagrams rarely reflect actual day-to-day activities. There is no standard way to define or communicate these assets and the related processes. Silos within the organization, often driven by budgeting

processes, can impact the ability to attain a comprehensive view of the organization's data resources.

Data content can often be undefined or ambiguous. Attorney's often receive unlabeled foreign language documents as part of a case or project. They cannot tell if it contains privacy sensitive data until AFTER it has been translated by a third party. Civil litigation often includes very large, undefined collections of unstructured data. It is impossible to determine the privacy implications of that data without detailed analysis, which nobody has a desire or budget to do.

2. **The greatest challenges in developing a cross-sector standards-based framework for privacy;**
   A common lexicon and method to define privacy related concepts. Just within a handful of privacy regulations you can find a wide range of meanings for 'personal information'. A cross-sector framework would have to include a way to harmonize terminology.

   As an example, one of my engagements is the words largest translation company. They translate materials for banks, government agencies, pharmaceutical companies, hospitals, and the hospitality industry (to name a few). Each of these are subject to broad and geographically specific government privacy and security regulations (GDPR, CCPA, etc.), industry specific regulations (HIPAA, NYDFS, etc.), and client contractual obligations. The workflows required to be compliant in any given situation are a very complex overlay of multiple obligations. Communicating and documenting each situation, across thousands of permutations, is very difficult.

12. **Any mandates to use specific standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles or conflicts between requirements and desired practices;**
    As mentioned in number 2 above, it is unrealistic to assume a given organization will be limited to mandated use of a single or limited number of standards or frameworks. The organization in the example is audited via every imaginable security framework, and very many home-grown privacy frameworks. A common framework with broad applicability would be helpful, especially if it lends itself well to mapping against other frameworks..

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;**
    There has yet to be a universally adopted standard or framework for cybersecurity, and I doubt privacy will be any different. Every in-the-wild use of the NIST cybersecurity framework I have seen has been customized by the organization using it, creating a lot of variants. International standards have value as they provide some common measurement tools, but only within the community of those who adopt them.

18. **Please describe your preferred organizational construct for the Privacy Framework. For example, would you like to see a Privacy Framework that is structured around**

Option 'a', the information lifecycle, comes closest. My practice has lead me to believe it is a combination of the information lifecycle and the business process cycle. Misunderstandings about, or changes to, data lifecycle and business processes are responsible for a large percentage of non-compliance related to security or privacy objectives.

20. **Whether, in addition to the practices noted above, there are other practices that should be considered for inclusion in the Privacy Framework;**
    Other practices:
    - Data content identification (this is not always clear in some environments)
    - Alternate workflows (in some environments, the additional precautions or restrictions applied to privacy-sensitive data create additional cost or delays, so privacy/no-privacy alternatives are important).
    - Data lifecycle enforcement

22. **Which of these practices you see as being the most critical for protecting individuals' privacy;**
    No magic bullets. Applying the appropriate practice for the specific situation is the most critical action.

23. **Whether some of these practices are inapplicable for particular sectors or environments;**
    Some may be inapplicable or impractical, based on each situation. There is no one-size-fits-all.

24. **Which of these practices pose the most significant implementation challenge, and whether the challenges vary by technology or other factors such as size or workforce capability of the organization**
    The main challenge is when one of these practices is 'bolted on' to a long standing business process. Ideally, the business process should be re-engineered with privacy objectives included. Built in will be much stronger and more efficient than bolt-on.

25. **Whether these practices are relevant for new technologies like the Internet of Things and artificial intelligence;**
    An appropriate practice properly applied will be effective across new technologies. The examination of the business/data process considering business objectives and privacy/security objectives is what will yield effectiveness and relevancy.

--- end of comments