Comments on NIST Developing a Privacy Framework

In the **SUMMARY:** it is stated that the framework is seen as being used to improve "organizations'' management of privacy risk for individuals arising from the collection, use and sharing of their information." While this is a well-founded statement, it might be more clearly stated as a means to manage the risk to ***both*** the individual and the organization (and its employees and supply chain) apart from the individual. The summary might also consider the extent to which individuals can be engaged to assess and manage risk in concert with the organization and the extent to which self-service is possible. Individuals can be enabled in a privacy forward workflow to participate early and with positive impacts in the information, and privacy risk management lifecycle. As structured, the challenge lies with the organization, when in fact in all cases there is a symbiotic relationship between an individual and organization(s). This is further complicated in the case of 3rd party services. Individual have different relationships that impact the services (and sub-services and micro-services) that use, or generate their personal information. While there is a later statement about how individuals interact with products and services, this might be brought further forward in the discussion and its importance in any privacy framework.

In **SUPPLEMENTAL INFORMATION: Genesis for the Privacy Framework's Development** it is stated that "It is a challenge to design, operation, or use technologies in ways that are mindful of diverse privacy needs in an increasingly connected and complex environment." While this is very true, there is a step that comes before this which is to gain an understanding of the nature of and the relationship of privacy risk, particularly in the United States where we have a fragmented regulatory and legal regime. The challenge in understanding the nature of the risks involved is also due to their interrelationship with other related business, security and cybersecurity risks. It is critical that a baseline understanding exists and that the risks can be profiled before engaging in the design, operation and use of technologies and more explicitly in the use of personal information. Further there is a need for this understanding to exist in development teams, and therefore the challenge exists not only in the design but also in the build and coding, prior to operation and use of privacy enhancing systems.

In **SUPPLEMENTAL INFORMATION Privacy Framework Development and Attributes** there is a statement that NIST "seeks to understand whether organizations would be better able to address the full scope of privacy risk with more tools to support better implementation of privacy protections." It is also clear that challenges exist with imbalance of power between individuals and organizations and the nature of the control over that information and the incentives from a strict business perspective apart from risk. At some point there needs to be a business incentive whereby there is ***value*** generated as a result of increased privacy protections and controls. A level set in this relationship may be as important as any tool set. A major component of this is transparency about the nature of relationship between individual and the organization as the controller of information and how that control is exercised. The requirements for innovation, as called for in the request for information (RFI) covers not only technology innovation but also innovation in business models, incentives and regulation. In this sense solutions need to not only be "compatible with existing legal and regulatory regimes in order to be most useful" but also to be able to support the evolution of these regimes that are currently underway around the world.

IDmachines' draft comments…

Regarding the minimum attributes of the Privacy Framework:

1. *Consensus-driven and developed and updated through an open and transparent process,* describes basing the development of the Privacy Framework on the approach used for the "Cybersecurity Framework" (CSF).

    Is it the intention of NIST to look to each of the agencies that oversee different sectors for their particular perspectives on privacy risk?

    For example, it would be interesting to know the difference across sectors in those cases where PII is gather based on consent versus legal basis or public safety and the requirements for notice and risk management. And it would be of interest to know not only the nature of gathering but also the sharing of information.

    This could also help in establishing priorities in addressing risk that may vary across sectors, use cases and contexts and add the important aspect of being able to measure risk as opposed to simply identification as currently depicted in the CSF.
2. *Common and accessible language.* While common and accessible language should always be a system design requirement throughout the risk and information lifecycle, it is suggested that this be expanded to a more general category of tools, technology and risk management techniques that are widely usable and that usability and user experience drive requirements during the design, build, operate, use and maintain stages of systems. This drives risk management more clearly into the operational domain where risk impacts and its mitigation take place.
3. *Adaptable to many different organizations and technologies, lifecycle phases, sectors and uses.* Since many risk management measures are driven by legal requirements perhaps a mention of the applicable law or use the term "jurisdictions" to complement the implication of the words "organizations" and "sectors".
4. *Risk-based, outcome-based, voluntary and non-prescriptive.* The term outcome-based seems to put the measurement of risk or benefit at the end of a process. While this is understandable it is important to understand the steps that take place to get to an outcome and that the earlier a risk can be addressed the lower the risk level and typically the level of effort and extent of the countermeasures needed to address it.
5. *Readily usable as part of any enterprise's broader risk management strategy and processes.*
6. *Compatible with or may be paired with other privacy approaches.* This is an interesting point to the extent that other frameworks, laws and codes of conduct exist, particular the later get to the specifics of use case and context.
7. *A living document.*

In **Goals of the Request for Information** there is a description of three goals, the 2nd of which is (ii) to gain a greater awareness about the extent to which organizations are identifying and communicating privacy risk and the 3rd of which is (iii) to specify high priority gaps. Another way to look at this is for the goal to be an ability to address high risk scenarios and communicating these risks and any gaps in knowledge or countermeasure in these cases as a high priority.

IDmachines' draft comments…

Details About Responses to This Request for Information

Request for Information

Risk Management

In many risk management regimes there is a priority on identifying high-risk categories. NIST covers this in that it solicits information about how organizations assess risk it would be useful to have some mention or focus on what is considered high risk.

Once again, the risk assessment is driven from the perspective of the organization, while this is critical to any risk management framework it is suggested that this be expanded to understand the risk profile from the perspective of the individual or the inherent data (information risk) in connection with and apart from the organization and/or the individual and/or third-parties that might be involved.

NIST asks for information to help understand the use of frameworks, standards, guidelines and/or best practices related to legal or regulatory requirements. In terms of best practice there are numerous examples. Some different examples of best practice that exist include:

NIST should continue to leverage the effort of the research and development NIST funded at the Identity Ecosystem Steering Group (IDESG), which is now housed in the Kantara Initiative. The Identity Ecosystem Framework (IDEF) and the IDEF Registry have key requirements, supplemental information, and the identification of standards in addition to looking holistically at the risk picture including security as well as interoperability and usability.

Another area for consideration, and also part of the work developed in the Kantara Initiative is the Consent Receipt specification which is being adopted across multiple vendors as a way of achieving interoperability, extending the impact of access control countermeasures and achieving compliance across a wide range of trust frameworks, since it is the case that consent plays in some way in ***every*** known privacy framework currently in place in the work today as well as in existing international standards such as the International Standards Organisation (ISO) 29100 Information technology -- Security techniques -- Privacy framework.

Another area for examination includes efforts by the physical security industry to address secure communication channels between card readers and door controllers as they can often be a conduit for personal information in the form of identifiers and biometric information, as examples. This includes the Security Industry Association (SIA) Open Supervised Device Protocol (OSDP) with is not included in the International Electrotechnical Commission (IEC) standard as 60839-11-5. Since physical protection is critical to, among other things, the safeguarding of servers where personally identifiable information is processed and stored. A simple of set of six (6) risk management steps for physical security professional has also been developed by ASIS International, referred to as the ITSC6 that covers cybersecurity, supply chain and privacy risk management. In each of these cases there are particular audiences and risks that serve as an example of the challenge in providing a framework that reaches across sectors and the different professionals in those sectors.

IDmachines' draft comments…

Organizational Considerations

1. The greatest challenge in improving organizations' privacy protections for individuals.
    a. One focus needs to be improving the transparency about the extent and use of personal information and for this to be done in a way so that the individual is included from the very beginning of this process. One tool that is beginning to be leveraged is the idea of receipts that document this interaction. The receipts can cover notice, consent and or changes in status as examples. Many current implementations simply as for a user to "agree" without any particular, transparent or usable documentation about what actually took place as a result of the agreement.
    b. As mentioned earlier, there are significant benefits (improvements) to including individuals in the organizations' risk assessment and management effort. This can be extended to a "consent by design" approach and protocol, engaging the individual as earlier as possible, and if in fact this approach is followed, engaging at the beginning of the workflow in gathering sensitive information.
2. The greatest challenges in developing a cross-sector standards-based framework for privacy
    a. One challenge is that requirements and risk are very much based on the legal jurisdiction, this is true in the case of the state to state differences in the United States as well as the differences that occur internationally as well as the sectoral distinctions noted in the category heading.
    b. Another challenge is the lack of a common language to describe actors and attributes. This applies to existing standards and regulations. For example, data controllers, privacy controller and information controllers all refer to the same thing in different framework. The semantic interoperability challenge is beginning to be addressed by some parties such as the EU.
3. How organizations define and assess risk generally, and privacy risk specifically.
    a. In the case of privacy risk there are a number of characteristics that represent high risk. For example, large volumes of information, automated decision making, child information are all called out specifically in the General Data Protection Requirement (GDPR). This goes to an earlier comment about a need to call out high risk categories in a (privacy) risk framework.
4. The extent to which privacy risk is incorporated into different organizations' overarching enterprise risk management.
    a. As opposed to overarching approaches, unfortunately, there does seem to be more often fragmentation in terms of risk assessment in many organizations. This is due to the fact that there already exist risk silos in the organizations. For example, the physical security organization managing property and personnel risk, the CISO managing information risk, compliance teams managing that risk and legal teams managing business risk. The introduction of Business Information Security Officers (BISO) is one example of a partial step to look at this in a business overarching manner.
5. Current policies and procedures for managing privacy risk.
    a. Much of this is driven by jurisdiction, sector, purpose and justification so in effect driven by context.

IDmachines' draft comments…

b. There are in fact a wide range of policies and procedures for managing privacy risk including existing privacy requirements as well as frameworks that cover security and consent management that are relevant to privacy risk. In many cases these are captured as best practice. In particular it is useful to understand best practice in the u

6. How senior management communicates and oversees policies and procedures for managing privacy risk.
    a. Unfortunately, the modus operandi seems to be reactive as opposed to pro-active. Another version of this is to focus on the management of privacy risk in the form of legal liability versus providing privacy ***rights*** as defined in a given jurisdiction. This is not a new set of patterns. The provision of privacy rights as a matter of policy needs to be a message from the top down and serves as an example of privacy by design as a means of addressing privacy risk.
7. Formal processes within organizations to address privacy risks that suddenly increase in severity
    a. There are a number of ways that result in a sudden increase in risk.
        i. Sudden increases in risk can result from a breach. In this case it is critical that that a plan be in place. Conducting breach "table top" exercises to test out actions can evaluate the effectiveness and operational reality of the formal process. The challenge is that a formal process for breach without test may be a process without the expected operational benefits.
        ii. Sudden increases in risk can also result from a change in the nature of the information risk that requires an update of the risk assessments and countermeasures. The process that needs to be in place is one that monitors risk conditions with an eye on changes with a particular emphasis on high risk. ***Some*** examples would include:
            1. Change in population, for example the inclusion of children and their related information.
            2. Change in the location of data processing or change in infrastructure or platforms used.
            3. Change in the processor role(s), particularly in the case of 3rd parties, and sub-processors.
            4. Change in the extent to which information is shared.
            5. Change in jurisdiction of the information controller.
            6. Change in the purpose and/or justification.
            7. Change in scale of data processed or data subject population.
            8. Change in automated decision-making algorithms.
            9. Change in privacy policy.
8. The minimum set of attributes 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.
    a. The IDEF Baseline principles provide a nice complement to this section. https://idesg.edufoundation.kantarainitiative.org/portals/0/documents/core/IDEF-Baseline-Requirements-v1.0-FINAL-10152015_MOD-4.pdf
    b. Also see comments above specifically about the *Privacy Framework Development and Attributes* section.

IDmachines' draft comments…

9. What an outcome-based approach to privacy would look like.
    a. Again, a challenge when addressing outcomes is to understand the entire supply chain. These include the organization, the data subjects, those that "touch" the information in between these in the information lifecycle, privacy and consent management solution and product providers, regulators, enforcement officials and even courts of law. Outcomes related to privacy risk and a framework needs to, at some point, touch all of these actors.
    b. An outreach to insurance companies that provide cybersecurity or liability insurance whereby adoption, and perhaps audit by third parties, of a privacy framework would reduce premiums can have a significant impact.
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.
    a. The need to work across layers (business, technical, legal is another way to represent these) is an important and often overlooked requirement in order to address and deliver usable outcomes.
    b. Clearly the NIST Cybersecurity Framework falls into this category and the related NIST Special Publications such as 800-37 and 800-53. There still exist challenges here for these to be living documents and for NIST to reach out even further with regard to attribute 1 for the process to be consensus-driven, again particularly when it comes to individuals'/data subject rights. On occasions the use of repositories such as Github have proven helpful in achieving minimum attribute 7 for these to be living documents. For example, the process with SP 800-63 update very effectively leveraged this approach.
    c. On attribute 2 of common and accessible language the work underway at the Worldwide Web Consortium (W3C) on semantic interoperability for privacy is germane https://www.w3.org/Privacy/permissions-ws-2018/papers/axel-polleres.pdf
    d. Clearly ISO has a number of efforts in this area, particularly ISO 29100 and the work in process for ISO 29184 Information technology -- Online privacy notices and consent. This work leverages the efforts underway in the Kantara Initiative which developed a Consent Receipt specification and has an active working group on Consent Management.
    e. Again, the IDESG, not Kantara, Identity Ecosystem Framework (IDEF) and the IDEF registry address a number of these attributes. In particular its inclusion of usability which is an important complement to attribute 2 of making things accessible.
    f. While voluntary approaches and a focus on outcome-based actions are critical, as called out in attribute 4 there needs to be complementary efforts to frame this in terms of business value versus risk reduction.
    g. Again, with respect to attribute 4, in reality most actions are driven by breaches, regulation and the reaction of the marketplace or the stock market. The impact relative to these negative outcomes can strong drivers. So it is important to frame the outcome discussion to take into account both positive and negative outcomes.

11. How current are regulatory or regulatory reporting requirements (e.g. local, state, national, international) related to the use of standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles.
    a. Following on from the previous comment, adding a stick to any carrots will impact and typically increase use and adoption of frameworks. Examples in the life safety domain include requirements for fire alarms, fire doors and fire extinguishers that are implemented at state and local levels. Providing a framework that can be used to make it easy to drive requirements to these levels can have a significant impact. This is particularly important to avoid a balkanization of regulations and requirements such as currently exists in the US with hundreds of privacy related regulations and laws, a number that is increasing by the day.
12. Any mandates to use specific standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles or conflicts between requirements and desired practices.
    a. So as pointed out there are more that 200 laws in the US and a raft of international laws currently as well as many forthcoming. Some of the more significant one's are related to the information for children and also healthcare related directives.
    b. With regards to the security industry and surveillance systems there do exist surveillance codes of conduct such as those put forward by the UK Surveillance Commissioner for a range of video and machine vision applications such as Surveillance Camera Code of Practice and more recently In the picture: A data protection code of practice for surveillance cameras and personal information https://ico.org.uk/media/1542/cctv-code-of-practice.pdf including license plate reading, body worn cameras, unmanned aerial vehicles and other systems.
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.
    a. An important role is the development of codes of conduct in industry such as the reference to surveillance standards in the UK. There has been a mixed bag in the United States on industry-based codes of conduct. Efforts such as those in the utility and finance sectors (NERC/CIP and PCI) have had some benefits in terms of getting service provides and their responsibilities as identity and service providers to come together and try to manage risk as an industry but in general they do not adequately if at all address privacy risk. A template for an industry code of conduct practice and assessor program for privacy does not exist. The International Association of Privacy Professional (IAPP) does provide a certification. Though it looks primarily at the legal layer and as mentioned it is strongly suggested that framework consideration there must be a balance privacy framework that looks across legal as well as business and technical layers and desired outcomes. Again, the IDEF and IDEF Registry provides a self-assertion of service providers, it has 3rd party assessment under consideration at this time.. Other identity assurance programs such as the Kantara Identity Assurance Framework (IAF), have the 3rd party assessment components in place but not, currently, coverage from a privacy framework perspective.

All of these provide added confidences to the extent that they gather best practice, engage subject matters experts and provide an objective assessment of risk and its management throughout the information, actor and relationship lifecycles.

14. The international implications of a Privacy Framework on global business or in policymaking in other countries.
    a. A Privacy Framework should ideally work across global contexts only introducing unique requirements as a last resort or in pursuit of a specific profile or use case. To the extent that companies interact globally once a framework is adopted it will have a global impact as users, and organizations that interchange data interoperate with individuals and organizations across jurisdictions and sectors throughout the information and their service lifecycles. In particular, many organizations look to NIST as a source of best practices to help them address the challenge of operating globally so the Privacy Framework needs to be sensitive to this. NIST often provides a mapping across other frameworks in its publications, such as in the CSF, 800-53 and 800-63. That would be a useful appendix for the Privacy Framework.
15. How the Privacy Framework could be developed to advance the recruitment, hiring, development, and retention of a knowledgeable and skilled workforce necessary to perform privacy functions within organizations.
    a. Curriculum, workshops, training, and the afore mentions codes of practices and certifications all can build and be part of the development of a Privacy Framework. NIST should look to leverage industry, trade organizations, other standards development organizations, subject matter experts and users across use cases to create a community that works together to achieve this objective.

Structuring the Privacy Framework

16. Please describe how your organization currently manages privacy risk. For example, do you structure your program around the information lifecycle (i.e., the different stages – from collection to disposal – through which PII is processed), around principles such as the fair information practice principles (FIPPs), or by some other construct?
    a. At OpenConsent we have developed a framework that has been leveraged to develop codes of conduct, workflows and a lifecycle for organizations and service providers to profile their privacy, and security risks. It takes 5 steps beginning with a definition of jurisdiction, identifying the relevant information and in particular an high-risk categories, then a preliminary profile with a public transparency baseline and a means to make that profile public, and maintain it, from there we focus on requirement or stipulations specific to the organization or service, including the need for dedicated resource such as a data protection officer and review and reporting on a data privacy impact assessment and finally the risk and controls and countermeasures. This is brought together at a single location to make it easy for organizations as well as individuals to see the “state” of privacy. We suggest that transparency be an important design principle in the framework, at OpenConsent it is a key component to consent by design. Further we believe that the extent to which explicit consent can be included in the Privacy Framework it will help to achieve global outcomes as we have found consent to be a part of all existing prior privacy frameworks we have cataloged.

IDmachines’ draft comments…

17. Whether any aspects of the Cybersecurity Framework (CSF) could be a model for this Privacy Framework, and what is the relationship between the two frameworks.
    a. The CSF is a complement and, in the sense, that it is also a framework from NIST is would be efficient for the Privacy Framework to share common views, components, and resources as best it can. It may be the case that a Privacy Framework puts in place new components of the information workflow and lifecycle. For example, the consideration of sensitive information as part of the registration process and its measurement and management may require more steps than simply "harvesting or importing" information as is often the case in identity and credentialing workflows.
18. Please describe your preferred organization construct for the Privacy Framework. For example, would you like to se a Privacy Framework that is structured around:
    a. The information life cycle
        i. There are multiple information lifecycles depending on whether this is look at from a user managed perspective or from a relying party perspective. Clarity around this and the precursors to establish context are important when setting the information lifecycle for consideration.
    b. Principles such as the FIPPs
        i. The FIPPs are a critical component and the Privacy Framework need to make clear how it relates to, leverages, builds on or replaces the FIPPs. The Privacy Framework should cast a broad umbrella in looking for a basis for structure in addition to the FIPPs.
    c. The NIST privacy engineering objectives or predictability, manageability, and disassociability or other objectives.
        i. These objects should be leveraged and examined for their applicability across existing frameworks as well as their incorporation int the Privacy Framework.
    d. Use cases or design patterns
        i. Critical, these need to be in clear language and should be at different levels of complexity for different primary actors. NIST should look to industry to develop and present these. NIST should develop a government use case that interacts with individuals as an example and to help contribute to the conversation about the best means and techniques in use case presentation. The can include modeling and programming languages but should not do this to the exclusion of clear and simply written use cases.
    e. A construct similar to the Cybersecurity Framework functions, categories, or subcategories, or
        i. Yes, a similar construct will be a likely outcome but should not constrain or overly influence the categorizations.
    f. Other organization's constructs
        i. Yes, particularly that that have existing privacy and usability frameworks early on in the process. Also engage with those that have constructed these frameworks to see the extent to which they have lessons learned.

Specific Privacy Practices

19. Whether the practices listed above (see document) are widely used by organizations
    a. Beside this query as importantly, compare and contrast these particularly in like organizations and use cases to understand the differences.
20. Whether, in addition to the practices noted above, there are other practices that should be considered for inclusion in the Privacy Framework
    a. To echo a previous point, the user experience and expectations should play an early and primary role in establishing the Privacy Framework in keeping considerate of all stakeholder risk perspectives. The framework should be considerate of as many actors as possible.
21. How the practices listed above or other proposed practices relate to the existing international standards and best practices.
    a. The Privacy Frameworks needs to work in concert, build off, address gaps and provide a coordinated and comprehensive vision that takes these into account.
    b. The evolving work in relationship management and understanding what is required to managed complicated, shared, layered privacy and other risks.
22. Which of these practices you see as being critical for protecting individuals' privacy?
    a. The establishment of codes of practice that are actionable and relevant in particular high-risk use cases.
23. Whether some of these practices are inapplicable for particular sectors or environments
    a. No and there needs to be a rigorous skepticism if it is thought otherwise.
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's capability of the organization.
    a. There are many, scale, interoperability, granularity of control to address multitude of context. This should challenge the Privacy Framework to address the need for innovation and to the point of this being a living document, push hard for better options.
25. Whether these practices are relevant for new technologies like the Internet of Things and artificial intelligence
    a. Trick question? Without saying and present another extensive and existential topic.
26. How standards or guidelines are used by organizations in implementing these practices?
    a. Specifically, to AI and IoT there are a wide range of standards efforts (surprise…). Much of the work is academic though there are some trade associations that have been in place for robotics and automation for some time that provide examples. In a connected world the challenge for a Privacy Framework lies more in working across standards and the device, network, communications, operating system and programming layers.