Summary Analysis of the Responses to the NIST Privacy Framework Request for Information

Introduction

The National Institute of Standards and Technology (NIST) is developing a voluntary privacy framework, in collaboration with private and public sector stakeholders, to help organizations: better identify, assess, manage, and communicate privacy risks; foster the development of innovative approaches to protecting individuals' privacy; and increase trust in products and services.[1]

On November 14, 2018, NIST issued a Request for Information (RFI) seeking information from stakeholders on the development of the NIST Privacy Framework: An Enterprise Risk Management Tool ("Framework").[2] NIST requested feedback to better understand current organizational considerations for privacy risk management, how NIST should structure the Framework, and specific privacy practices that NIST should include in the Framework. As of the date of this publication, NIST has received nearly 80 responses from a range of stakeholders, including individuals and a variety of organizations representing industry, government, and public interest.[3] All of the responses were supportive of NIST's effort to develop the Framework.

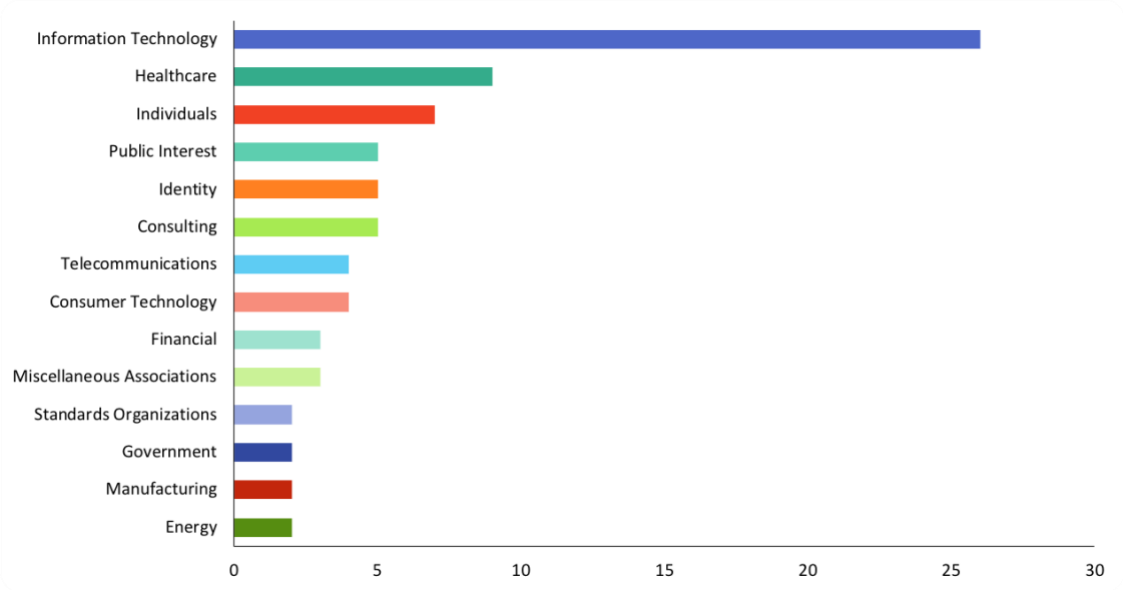

Figure 1 RFI Respondents by Sector

[1] For more information on the development process, see https://www.nist.gov/privacy-framework.
[2] Federal Register Notice 83 FR 56824, Developing a Privacy Framework, https://www.federalregister.gov/documents/2018/11/14/2018-24714 /developing-a-privacy-framework; Notice of Extension: Federal Register Notice 83 FR 64531, Developing a Privacy Framework, https://www.federalregister.gov/documents/2018/12/17/2018-27248/developing-a-privacy-framework.
[3] The responses are posted at: https://www.nist.gov/privacy-framework/request-information. As stated in the RFI, responses that contained "profanity, vulgarity, threats, or other inappropriate language or content" were not posted or considered.

This report represents a high-level analysis of the RFI responses to inform the development of the Framework. The following sections explain the methodology NIST used to perform the analysis of the RFI responses and describe major themes that emerged.

Analysis Methodology and Scope

Multiple NIST personnel reviewed each RFI response. For each review, NIST:

- Determined basic information about respondents to assess coverage of responses across sector and organization type;
- Mapped sections of text from RFI responses to topics based on the RFI; and
- Created associated keywords to facilitate identifying main points, commonalities, and recurring concepts across all responses. These commonalities contributed to the summary statements for each theme.

For this summary analysis, NIST has focused on the RFI responses that provided information relevant to the development of the Framework. While some responses included information on other topics—such as the development of federal privacy legislation—those topics are not included in this report.

Major Themes from the RFI Analysis

This section describes the major themes that NIST extracted from the RFI responses to advance the development of the Framework. The themes are organized in accordance with the topic sections of the RFI: organizational considerations, structural considerations, and specific privacy practices. Each theme includes a summary statement highlighting respondents' viewpoints. NIST has included excerpts from various RFI responses to illustrate these viewpoints. These excerpts are representative only; they are not intended to be exhaustive of all the responses received on the theme.[4]

Overview of the Themes

Organizational Considerations

Theme: Regulatory Compatibility

Theme: Interoperability with Global Standards

Theme: Benefits of Framework Attributes

Theme: Privacy Risk Management and Associated Terms

Theme: Transparency and Accountability

Theme: Workforce

Structural Considerations

Theme: Cybersecurity Framework Alignment

Theme: Principles, Information Lifecycle, and Goals/Objectives

Theme: Request for Guidance

[4] RFI response examples are not edited for spelling, grammar, or other typographical errors.

Specific Privacy Practices

Theme: De-identification

Theme: Informing Users and Enabling Preferences

Theme: Control and Data Management

Theme: Data Minimization

Theme: Encryption

Theme: Emerging Technologies

Organizational Considerations

ORGANIZATIONAL CONSIDERATIONS

Theme: Regulatory Compatibility

Summary Statement: Many respondents expressed that the Framework should support organizations' ability to comply with a range of legal responsibilities, including U.S. state and federal sector-specific laws and regulations and international regimes such as the APEC Cross-Border Privacy Rules, the European Union's General Data Protection Regulation, and Brazil's General Data Protection Law.

RFI Response Examples:

- The privacy framework must be rationalized with existing sector-specific US privacy laws. This process should help companies understand and smooth out their responses to our existing patchwork of laws…It is essential that any framework be compatible with other privacy approaches around the globe, including GDPR, CCPA, privacy laws in Australia, Brazil, and China, as well as the other industry-specific privacy laws in the US, including COPPA, FERPA, and HIPAA.[1]
- …NIST's Privacy Framework should align with and help advance key international privacy constructs, including the Asia- Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) System and the EU-U.S. Privacy Shield.[2]
- The financial services sector already complies with a range of domestic and international privacy and data protection laws, and the Framework process should not directly, or indirectly, create a new, overlapping, or duplicative process.[3]
- While the Privacy Framework should not mirror the GDPR, its controls must be developed with an awareness of the GDPR and the standards therein that are increasingly being adopted worldwide.[4]
- Our members are already required to follow the HIPAA Privacy Rule, and so must follow a set of prescriptive privacy requirements that are based on the Fair Information Practice Principles. We encourage NIST to ensure that the Proposed Framework harmonizes with the prescriptive obligations of HIPAA and other existing privacy frameworks…[5]
- …companies around the world are struggling to bring existing data processing practices based on legitimate business objectives into compliance with laws like the GDPR. The problem is especially difficult for international companies subject to a variety of conflicting data privacy laws in various jurisdictions. As a result, organizations seek industry recognized frameworks to synergistically guide corporate governance, compliance, information security, and enterprise risk management functions.[6]
- The insurance industry has been subject to the Gramm-Leach-Bliley Act (GLBA) and implementing privacy regulations for over two decades. Increasingly, states are considering, and adopting, privacy laws that have general applicability to all industries, including insurers. This complex patchwork of federal and state laws creates a difficult compliance environment that could negatively impact consumers rather than help them. The challenge only increase for companies operating globally as the international patchwork of laws continues to emerge as well. Hence, the compatibility attribute of the Privacy Framework is critical.[7]
- CMS is subject to many laws and regulations, including those listed above, and continues to be very attentive to NIST policies and guidance mandated by the e-Government Act, most notably NIST's Special Publication 800-53…CMS's first priority remains implementing risk management and compliance activities that comply with existing requirements.[8]

ORGANIZATIONAL CONSIDERATIONS

Theme: Interoperability with Global Standards

Summary Statement: A number of respondents stated support for interoperability of the Framework with global standards.[5]

RFI Response Examples:

- We strongly support the adoption and use of voluntary consensus standards accredited in an accepted framework such as that of the American National Standards Institute (ANSI), or meeting the same essential requirements.[9]
- NIST has long recognized that "[t]he development of international standards [] promotes U.S. interests by facilitating interoperability, security, usability, and resiliency, improving trust in online and offline transactions, promoting innovation and competitiveness, and helping U.S. products and services compete in global markets." Although that statement was made in the cybersecurity context, the same is true of privacy. Just as NIST recommended that "[f]ederal agencies should use relevant international standards for cybersecurity, where effective and appropriate," NIST should do the same for privacy. Doing so also would align with NIST's recommendation to use relevant international standards to achieve mission and policy objectives.[10]
- In light of the need for privacy protections, it is critical to have standards that provide interoperability, as well as have the ability to be innovated upon to align with practices of organizations implementing them. This can help minimize any extra burden caused by additional requirements. IEEE is developing standards and best practices in this field, including a growing set of projects on general privacy processes as well as more specific ones, including: ▪ IEEE P7002, Standard for Data Privacy Process ▪ IEEE P7006, Standard for Personal Data AI Agent ▪ IEEE P7012, Standard for Machine Readable Personal Privacy Terms ▪ IEEE P7004, Standard for Child and Student Data Governance ▪ IEEE P7005, Standard for Transparent Employer Data Governance[11]
- Risk-based approach: In order to align with ISO/IEC 27001 and the NIST CSF, the NIST Privacy Framework should be risk-based to allow for flexible, cost-effective approaches to privacy protections. Many risk management frameworks base business decisions on objective analysis of corporate risk vectors to facilitate an evolving response to threats based on changes in the legal or technological landscape. In the short term, this allows for more cost-effective solutions as residual risks are operationalized; in the long term, ongoing risk management methods take on a consistent, objective approach that stabilizes over time.[12]
- Mapping the framework to existing standards and requirements would greatly benefit organizations that base their practices on those standards and requirements. A privacy framework that is easily integrated with what organizations already do today is inherently useful and more likely to be accepted and adopted. Moreover, leveraging existing standards and requirements furthers the goal of global interoperability of the framework. A standard that aims for global interoperability is becoming increasingly important, particularly in light of the evolving global privacy regulatory landscape.[13]
- ...we encourage the consideration of the [Identity Ecosystem Framework] privacy framework as contained in the appendices be included in the Privacy Framework development process.[14]

[5] For a list of the standards and guidance cited by respondents, see https://www.nist.gov/privacy-framework.

ORGANIZATIONAL CONSIDERATIONS

Theme: Benefits of Framework Attributes

Summary Statement: Respondents supported the Framework attributes described in the RFI, including common and accessible language, that it be adaptable, risk-based, outcome-based, technology-agnostic, non-prescriptive, and readily usable as part of an enterprise's broader risk management processes, and noted that these attributes would provide benefits including fostering innovation, creating a broader communication tool, and overcoming challenges for small and medium-sized businesses with more limited resources for privacy risk management.

RFI Response Examples:

- In addition to the process that created it, the Cybersecurity Framework's success is due to its attributes: As with the Cybersecurity Framework, NIST should not adopt a one-size-fits-all approach, nor should it promote a checklist mentality.[15]
- We fully support NIST's Privacy Framework initiative and we believe that a "forward-thinking" approach will support consumer protections, business innovations and alignment of policy, technological, and legal approaches to data collection, storage, use, and sharing.[16]
- We applaud NIST for its commitment to accessible language, which we have found lacking in other government processes. We encourage NIST to follow this through by ensuring that complicated concepts or documents on which the foundation is based are summarized or simplified for a general audience…[17]
- A risk-based, outcome-based, voluntary and non-prescriptive Framework allows companies to efficiently maximize human, financial and technical resources thereby meeting or exceeding consumer privacy expectations and fostering innovation.[18]
- It will further enhance privacy protections for individuals if the privacy requirements and the tools that support compliance are accessible and understandable to personnel within companies who are not lawyers, privacy professionals, or technologists. IA believes that any privacy framework should be sufficiently detailed and clear, so that the standards will be easily understood by individuals and straightforward for companies of all sizes to implement. IA applauds NIST's commitment to transparency in the process of creating the Privacy Framework and believes that the use of common and accessible language through the process will support public discourse on this important issue.[19]
- A NIST Privacy Framework should anticipate the constantly evolving nature of technology and be flexible enough to work for the data-intensive innovations of the future…The federal government should be mindful of current and future uses of data and embrace policies that promote U.S. progress and leadership in these emerging technologies.[20]
- Engine also appreciates NIST's goal of making the Privacy Framework "adaptable to many different organizations, technologies, lifecycle phases, sectors, and uses" and "platform- and technology-agnostic and customizable." Startups can traverse sectors, lifecycle phases, and business models, and no one-size-fits-all approach works for the thousands of small businesses that make up the U.S. startup ecosystem.[21]
- …the framework should…encourage the incorporation of privacy into existing enterprise risk management programs and processes.[22]
- Making the Privacy Framework applicable under these various contextual factors will be key to limiting its applicability to specific technologies, sectors, or business models. Avoiding a prescriptive approach is therefore paramount.[23]
- …the Framework should be scalable to organizations of all sizes and be platform- and technology-agnostic and customizable. The Framework should not create unnecessary or disproportionate burden on solo proprietors or small businesses. Many solo practitioners and small group practices must devote their limited resources to addressing immediate demands of clinical practice and clinical care and do not have the resources to hire an employee to focus on managing privacy risk.[24]
- The framework should provide broader approaches to implementing practices and procedures for smaller/resource-challenged agencies.[25]

ORGANIZATIONAL CONSIDERATIONS

Theme: Privacy Risk Management and Associated Terms

Summary Statement: NIST received a number of responses about privacy-related terms, but did not receive many responses on organizations' privacy risk management processes. Some respondents shared risk management practices focused on achieving data security objectives or referenced the use of privacy impact assessments or privacy by design principles. The lack of response may be due to the absence of a widely-accepted definition of privacy risk as noted by many respondents. A number of respondents indicated that privacy risk should be centered on individuals and potential harms while some cautioned NIST against providing a definition. Others encouraged NIST to account for beneficial and responsible data use in a privacy risk management approach. Respondents also differed between those who sought definitions for associated terms like "personal data" and those who encouraged NIST to refrain from doing so as many organizations use definitions already defined by laws and regulations.

RFI Response Examples:

- Workday achieves compliance with international privacy regulations by maintaining a comprehensive, written information-security program that contains technical and organizational safeguards designed to prevent unauthorized access to and use or disclosure of customer data…Workday also publishes a Service Organization Controls 2 (SOC 2) Type II report. The Workday SOC 2 report addresses all trust services principles and criteria (security, availability, confidentiality, processing integrity, and privacy).[26]
- Privacy risks are integral to our enterprise risk management framework, which incorporates both privacy and information security risk management. As we noted above, we maintain an organizational infrastructure to ensure broad-based privacy and security practices across our program.[27]
- 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.[28]
- At this point there are multiple privacy risk models, exhibiting various degrees of completeness, that can be used to identify privacy risk. These include, but are not limited to, FIPPs, Solove's taxonomy, Nissenbaum's contextual integrity and the one described in NISTIR 8062 (and in more detail in its initial draft). Ideally, any method for assessing privacy risk should be capable of using the privacy risk model of choice, as does, for example, System-Theoretic Process Analysis for privacy (STPA- Priv).[29]
- The NIST Privacy Framework should promote privacy risk assessment throughout the Service Development Life Cycle. We need to impress upon entrepreneurs that products and services (particularly IoT device manufacturers) must be built with "Privacy designed in", so we can compete with similar products and services originating from countries, in which "Privacy designed in" is already mandated, or in other countries where that sort of control might be strictly forbidden.[30]
- One challenge to date has been identifying what actual privacy risks are – specifically, outlining the kinds of harms that might occur based on the design choices made. Many compliance- focused models fail to anticipate broader issues that may arise.[31]
- Privacy Risk, which we would define to mean risk to the confidentiality, integrity and availability of the personal data of our own employees, our consumers and customers, and the personal data we may process through our corporate customers use of our products, is closely tied and integrated with the information security risks of our systems and the business risks associated with certain decisions.[32]
- 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…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.[33]
- …NIST should not define "privacy harm," which is an important policy decision. In NISTIR 8062, An Introduction to Privacy Engineering and Risk Management in Federal Systems, NIST explored the topic of defining "privacy problems" in federal systems. While that work can help to inform policymakers, it should not be incorporated into the Privacy Framework. Congress, NTIA and the FTC are all looking at privacy harms…In the RFI, NIST uses

the definition of personally identifiable information ("PII") from Office of Management and Budget Circular A–130, which defines PII as "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." CTIA urges NIST not to incorporate this definition, because the approach used by OMB for federal government entities should not be used in a regime-neutral and generally applicable Privacy Framework. There are different threshold definitions for covered data under different regimes—for example, "personal data" under The European Union's General Data Protection Regulation ("GDPR") is different from "personal information" under the California Consumer Privacy Act ("CCPA"), which is different from "customer proprietary network information" or "CPNI" under the Communications Act. NIST should not choose one, as these threshold definitions for covered data vary across regimes, and may change as federal policy evolves.[34]

- …there is no model we are currently aware of to assess individual privacy risks, either on average or specific to a person. Accordingly, more research is necessary in order to determine metrics for evaluating impact before this principle can be properly implemented. NIST should invest in and incentivize this research, which must be expansive and not limited to financial harms. Instead, it must also include emotional, psychological, physiological, human rights, and other impacts that individuals may face on account of a privacy event. It should also include a probe of possibilities for individual and collective remedies, including the options people may have to respond to or mitigate those impacts.[35]
- …current law generally only recognizes privacy risk when it materializes in actual damages. This economic loss doctrine fails to consider that privacy risk may not materialize in the moment, as identity theft is under no time restraint, and data once lost is not easily recovered. Subsequently, the NIST Privacy Framework should position privacy risk from the personal point of view, to help guarantee organizations continue to measure and mitigate privacy risk on an individual level.[36]
- How organizations define and assess risk generally, and privacy risk specifically are often considered in the context of economic tradeoff of risk versus reward, specifically around privacy risk and level of measures to practice and to implement such practices. They also include the utilization of risk management frameworks via risk and legal teams and business units to identify levels of acceptance as directed by market perception, company perception, subject matter expertise, and levels of return associated with investment. Organizations with enterprise risk management divisions may consider privacy risk relative to and in accordance with other risk elements, whereby the risk is weighed against the benefits and appropriate action is then taken that is in the best interest of the organization.[37]
- Large companies that rely on consumer data must be incentivized to think more seriously about "putting the customer first" when it comes to data collection.[38]
- To achieve better privacy outcomes for individuals, legal frameworks and the tools that support compliance with such frameworks should be built to recognize and assist in an analysis focused on the risk to the individual.[39]
- It rightly recognizes that harms occur not only from the unauthorized use of information, but equally from the authorized use of information in an unexpected or contextually different way. An operational system of responsibility is important, rather than placing the onus only on the individual to take steps to monitor information use in complex systems to protect individual privacy. These strengths, however, can be the source of harms if not constructed and implemented with care.[40]
- The RFI focuses extensively on privacy risk and does not refer explicitly to innovation and other benefits of data use.[41]
- A framework that does not take benefits into account would offer an incomplete picture of the considerations needed to identify, consider, and mitigate privacy risk associated with the next generation of data-driven technologies. This omission could lead users of the Privacy Framework to undervalue the benefits of data-driven innovations for consumers' convenience, health, and safety. Including in the Privacy Framework guidance to help organizations consider the benefits of responsible data collection and use while also taking steps to mitigate privacy risk would avoid this potential pitfall.[42]
- A Privacy Framework should facilitate beneficial and innovative uses of data that present low risk of harm to individuals. It should recognize companies' flexibility to best determine and mitigate their own risks.[43]

- By its nature, risk management does not seek to eliminate all potential risk or prevent all possible harms, since such an objective is unattainable and heightens the likelihood of unnecessarily increasing costs, thwarting innovation, and harming consumer welfare. It is instead focused on identifying and prioritizing risks so that the organization can address them in a way that is proportionate with the potential harms to consumers. NIST's risk management model should assist organizations with appropriately calibrating the competing concerns at stake in connection with any particular data collection, use, or disclosure.[44]
- The common information security terms "threat" and "vulnerability" fail to adequately articulate the nature of privacy risks because many privacy risks arise from "authorized" behaviors...The NIST privacy engineering model uses the term "problematic data-action" rather than attempting to expand the "threat" risk factor to encompass pure privacy concerns. "Problematic data action means a data action that causes an adverse effect, or problem, for individuals." Maize believes that the Privacy Framework should adopt the concept of the "problematic data-action" as described in NISTIR 8062.[45]
- …industry policy and practice should be based upon a clear and broadly accepted definition of personally identifiable of information (PII) specified in NIST's intended Framework…[46]
- Developing a clear and operational definition of privacy risk is critical to the success of the Privacy Framework.[47]
- Similar to the process used in the CSF to create a "Glossary," the creation of a Framework must avoid using terms that are either too broad or conflict with terms used in existing laws and regulations. Standard terms and definitions in privacy requirements will need to be carefully analyzed, for example, terms including "consumer vs. customer," "personal information" or "personal data," "control," "access and correction" all have specific definitions for the financial services sector.[48]

ORGANIZATIONAL CONSIDERATIONS

Theme: Transparency and Accountability

Summary Statement: Many respondents emphasized the relationship between transparency and accountability with regard to organizational privacy policies and practices and improving consumer trust. These concepts also appear in other themes, including *"Informing Users and Enabling Preferences and Choice"* and "*Emerging Technologies"*.

RFI Response Examples:

- Privacy technology must be transparent and enable organizations to articulate how the technology arrived at its assessments or conclusions by providing human readable text descriptions and details showing what evidence was used to make decisions. Transparency will allow organizations utilizing technology to aid in privacy audits to demonstrate how the implementation of technology relates back to privacy engineering objectives and the FIPPs.[49]
- …we proactively educate our customers about how their data is being used and frequently receive feedback from our customers commending our outreach and transparency. We believe that the Privacy Framework, by providing further information and certainty to consumers, governments and business alike, will and should contribute to efforts to bolster public trust and confidence in personal data processing.[50]
- Adoption of elements of FAIR on Privacy will give consumers more control and a clearer understanding of their choices regarding the use of their personal data. It also clearly defines an entity's responsibilities so they can be held accountable by regulators, hereby ensuring companies use personal data responsibly and transparently.[51]
- Trust and accountability are founded on transparency. Without transparency, organizations cannot build and maintain trusted relationships. Accountability requires a trusted, transparent and documented organizational structure comprised of policies, processes, practices, controls and above all common values that guide strategic and business objectives. Transparency is critical. Accountability also requires transparency with consumers. Ensuring transparency through strong organizational policies around data and building capabilities, wherever possible, to set preferences or choices for data use, are crucial steps to fostering trust and confidence. Accountability means a system that places responsibility for protecting consumer data and privacy on organizations collecting or handling consumer data, particularly in an information society and ecosystem that is complex and continuously evolving. Organizational accountability embodies the following core elements: risk-assessment, policies and procedures (taking into consideration fairness and ethics), transparency, training and awareness, monitoring and verification, response and enforcement, and leadership and oversight. A privacy framework should incorporate these elements as the foundation to how an organization approaches privacy.[52]
- Trust is paramount to a cybersecurity company. To maintain our customers' trust, we try to be very transparent about our actions and our decisions. As part of 2 our commitment to accountability, we have posted our privacy policy on Github so our customers can see the changes we have made over the years. We know our customers are savvy, privacy conscious and security-minded, and we want to make sure they have the tools to hold us accountable. We also endeavor to be transparent in our communication about our own mistakes and failures.[53]

ORGANIZATIONAL CONSIDERATIONS

Theme: Workforce

Summary Statement: Responses reflected a range of viewpoints regarding the Framework and privacy workforce development. Some saw the Framework as a tool to improve development of a knowledgeable and skilled privacy workforce, while others requested the inclusion of workforce best practices and guidance in the Framework.

RFI Response Examples:

- FIA recommends that the Privacy Framework include best practices and encourage companies to not only address overall hiring and retention efforts, but also ways to include diverse voices at all levels — including attorneys specializing in privacy and data security, experts in data ethics and technologists.[54]
- A robust Privacy Framework can only positively support the recruitment of more informed individuals. An established Privacy Framework can be used to focus the workforce to view the people, process and technology surrounding privacy management in a more consistent and holistic way. Focusing on best practices will begin to do what the Cybersecurity Framework did: change the dialog from compliance to risk management. Being able to understand how to implement a successful and reasonably complete privacy program will go a long way towards meaningful organizational advances in improving privacy overall.[55]
- NIST should encourage organizations to foster diversity on the teams that work on privacy efforts. Successful privacy management requires the team to be able to understand and relate to and address situations that their users or customers are personally experiencing, which will likely represent a tremendously diverse set of problems and preferences…To make this guidance actionable, it might be helpful to include categories of expertise or general job titles in the documentation of the Framework, in support of NIST's goal to produce accessible information. Technical titles and specialties can be confusing and intimidating for some individuals, which can impact whether the right variety of experts are working on a given issue.[56]
- Including information regarding privacy engineering and its importance in implementing privacy by design should help advance recruitment of a knowledgeable and skilled workforce and ensure that more people, including but not limited to students who could pursue relevant education and company executives, are aware of this growing field and its utility.[57]
- A risk-based, outcome-focused Privacy Framework also will help create a privacy-focused workforce. Harmonizing privacy engineering practices and developing an interoperable framework will create common privacy operations in organizations globally and help to standardize and develop privacy workforce skills. Harmonization also creates a career-boosting skillset around the world, because skills learned in one country will be readily useful in another.[58]
- Curriculum, workshops, training, and codes of practice 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 developing organizations, subject matter experts, and users across use cases to develop a Privacy Framework that, in addition to enhancing data privacy, also supports workforce development.[59]
- Small businesses represent 99.7 percent of all U.S. firms, and they require heightened assistance and must play a more significant role in the development of privacy management strategies. It is important that NIST remain mindful of the fact that large companies often dedicate large budgets to create and maintain privacy control processes and have the ability to hire staff and consultants to mitigate privacy risks, while small enterprises very often do not. For many of our members, the role of chief privacy officer may be one of five hats worn by a single employee. The essential role of American small businesses, along with the unique resource constraints they face, make the NIST Privacy Framework even more important.[60]
- Cultural "Will to Protect": Leadership and culture is critical to an entity's privacy governance and execution. An entity must, by decision, choose and act as a prime business directive to protect private information and use the information in an ethical manner. Absent such strong leadership and culture, an entity will struggle to achieve effective privacy protection.[61]

Structural Considerations

STRUCTURAL CONSIDERATIONS

Theme: Cybersecurity Framework Alignment

Summary Statement: Many respondents expressed a preference for the Framework to align with or follow the structure of the Cybersecurity Framework, indicating that this could make the Framework easier to adopt. Some respondents suggested privacy-adapted functions and other elements. [6]

RFI Response Examples:

- …the Privacy Framework should be compatible with the Cybersecurity Framework ("CSF"). One place to start could be to identify privacy protective actions within the each of the CSF's five top-level elements of identify, protect, detect, respond, and recover. Given the success of the CSF, it would be useful to identify an analogous set of top-level elements for the Framework. For example, the privacy elements could be: identify, inform, steward, respond, redress.[62]
- The structures of the Privacy Framework and the Cybersecurity Framework should complement each other. As the Cybersecurity Framework provided steps for Identification, Detection, Protection, Response, and Recovery with regard to a data breach, so should the Privacy Framework map out an approximately linear path for safeguarding privacy.[63]
- Ideally, the Privacy Framework development will parallel the Cybersecurity Framework structure of functions, categories, and subcategories, allowing detail with clarity. Following the familiar format of the Cybersecurity Framework will leverage an organization's existing investment in the Cybersecurity Framework, particularly those in the healthcare industry.[64]
- …the Cybersecurity Framework should be the model for the Privacy Framework… For example, the Cybersecurity Framework helps organizations manage their cybersecurity risk by determining which security controls from NIST 800-53 they may utilize to achieve their security risk profile. Similarly, the Privacy Framework should help organizations manage their privacy risk by determining which privacy controls to utilize from the final version of NIST 800-53 Rev 5 or from other comparable standards.[65]
- Where practicable, utilizing the same control sets as categories and subcategories and same informative references for these categories, would also be helpful to limit duplication or misunderstandings for organizations using both frameworks. For example, many of the categories in the "Identify" function in the Cybersecurity Framework may very well prove to be equally applicable to the Privacy Framework.[66]
- …NIST should strive to achieve the greatest degree of interoperability with the CSF feasible. The power of the CSF framework stems from the manner in which it provided organizations a consistent way to: identify risks requiring management; select controls available to manage the risks; and assess their maturity at managing risks against a target state. It would be unnecessarily confusing to differ from that approach in the development of the forthcoming Privacy Framework without some significant justification.[67]
- The Framework should also include similar organizational constructs to those in the CSF as a means to help organizations understand how to manage privacy risks. Concepts like the "Core Functions" are easily adaptable to privacy.[68]
- What we are suggesting as a path forward would be to not try to force fit Privacy into the CSF directly but to use the structure of the CSF. The Functions, Categories, Subcategories, Informative References, Tiers, Profiles and Core are what makes the CSF easy to use and easy to communicate.[69]
- My main concern is that NIST should consider synchronization between NIST CSF and any upcoming privacy framework. Such as similar structure of functions, categories, sub-categories and informative references. The industry is well versed with CSF structure of implementation and informative references provides scope to consider different frameworks.[70]

[6] Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1., https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

STRUCTURAL CONSIDERATIONS

Theme: Principles, Information Lifecycle, and Goals/Objectives

Summary Statement: Many respondents expressed an interest in the Framework using various organizational constructs posed in the RFI, including privacy principles, the information lifecycle, and goals/objectives, with several respondents suggesting the combined use of multiple constructs with a CSF structure. A number of respondents expressed an interest in seeing existing sets of principles – including the Fair Information Practice Principles – and objectives such as NIST's Privacy Engineering Objectives of predictability, manageability, disassociability, reflected in the Framework.

RFI Response Examples:

- …NIST should prioritize pursuing a structure and construct similar to the Cybersecurity Framework, while perhaps integrating concepts or terminology from some of the other constructs within this structure as appropriate. For example, principles such as the FIPPs continue to have enduring vitality in a variety of contexts, including informing ITI's FAIR on Privacy, NTIA's contemplated privacy framework, and various other sets of principles and legislative efforts globally. The FIPPs also provide familiar terminology to many stakeholders, so incorporating references to the FIPPS may facilitate achieving a Privacy Framework that can serve as a common language accessible to multiple stakeholders across multiple technologies, use cases, and contexts.[71]
- Because of the key considerations in development of systems that collect data, use of that data and the retention and destruction of any data, HITRUST recommends that NIST strongly consider the information life cycle as defined by NIST or based on existing representations in structuring the NIST Privacy Framework. This ensures that the variables found at each stage in the life cycle can be appropriately considered and analyzed. Additionally, as different personnel will often be more involved at various points in the life cycle, it is a useful structure to aid one's implementation of the Framework.[72]
- EHNAC stresses PHI Flow, Level of Data Handling and the full information life cycle as the initial component of its criteria. This is preferred and scales well to organizations of various shapes and sizes.[73]
- Consumer Reports supports some combination of (a) the information life cycle, (b), principles such as the Fair Information Privacy Practices (FIPPs), and (d) uses cases or design patterns. Information life cycle focuses on moments of collection, retention, sharing, and deletion. Principles like the FIPPs are essential to frame privacy practices as they go beyond risk. And use cases/patterns are useful to show good and bad practices (e.g., the Federal Trade Commission's Dot Com Disclosures).[74]
- There are some existing structures in place that could be used as a starting point to develop specific outcomes. For example, the Fair Information Practice Principles (FIPPs) are internationally recognized principles that have informed existing Privacy regimes such as the GDPR in the EU. The principles of Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, Accountability and Auditing could be used in a similar role as Categories in the CSF, with specific outcomes being derived from each principle.[75]
- …the RFI offers sound starting points for the industry to consider, including objectives of predictability, manageability and disassociability.[76]
- Maize believes that general principles stated in HIPAA regulations, the fair information practice principles (FIPPs), and the three privacy engineering objectives of predictability, manageability, and disassociability provide excellent guidance on how the Privacy Framework can enable privacy professionals to assess emerging technologies.[77]
- 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.[78]
- Like the NIST CSF model, organizations would likely use the Privacy Framework model to establish privacy objectives and a roadmap of initiatives with timelines to ultimately achieve those objectives. To align with Instead of labeling Functional components as 'Categories' and 'Subcategories,' please use terms such as

privacy "Principles" or functional "Objectives," which will a) Acknowledge ongoing organizational efforts to respect and honor Privacy, b) Align with the EU philosophy on Privacy that underlies GDPR, and c) Speaks directly to 'business' decision makers, who are ultimately accountable for implementation and ongoing execution of operational practices that honor privacy.[79]

- Similarly, we would suggest for consideration NIST specifically using the OECD principles as the organizational structure around which to build the voluntary framework. Doctrinally, the FIPPS provided the basis for the OECD principles. In additional, however, the OECD principles have the benefit of a global footprint which would suggest, if used as the basis of the privacy tool, a heightened level of potential synchronicity with global digital privacy protection efforts.[80]
- Privacy frameworks such as the FIPPs, the APEC Privacy Framework, and the OECD Privacy Principles are the foundational documents on which most privacy laws, regulations, and practices are based. HITRUST recommends that the NIST Privacy Framework development process should include a review of these frameworks to understand these key principles and how they could inform a modern, risk-based approach to privacy. [81]
- 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.[82]

STRUCTURAL CONSIDERATIONS

Theme: Request for Guidance

Summary Statement: Some respondents requested that NIST provide various forms of guidance, including informative references, guidance regarding specific privacy practices, a roadmap, use cases, and mappings to laws and standards.

RFI Response Examples:

- …NIST should start work on a Privacy Framework with the baseline assumption that the core functions—i.e., identify, protect, detect, respond, recover—are equally applicable as they were to the CSF. Wherever feasible, the method used to identify and apply relevant controls should be similar. If that turns out to be true, NIST's efforts to build a Privacy Framework will…focus future standards development efforts on gaps identified through the process of assembling a privacy-specific set of "informative references.[83]
- We suggest including Asia-Pacific Economic Cooperation (APEC), Cross-Border Privacy Rules (CBPR), HIPAA Privacy Rule, GDPR, ISO27001, and ISO27018 in an Informative Reference Section.[84]
- Other aspects listed above, like information life cycle, engineering objectives, use cases and design patterns, etc. should be covered in guidance associated with the framework.[85]
- The NIST privacy engineering objectives of predictability, manageability, and disassociability or other objectives – No. We believe this should be a second layer of privacy framework documentation, after defining the framework core, tiers and profiles…We recommend NIST provide additional clarification and guidance for various use cases, such as HIPAA de-identification.[86]
- …FIA recommends that the Privacy Framework address guidelines on communicating and developing privacy protections across an entity's supply chain. The guidelines should also address practices in dealing with an organization's existing suppliers, contractors as well as professionals seeking to do business with the organization.[87]
- Just as NIST published a Roadmap in conjunction with the Cybersecurity Framework, NIST should plan to publish a Roadmap in conjunction with the Privacy Framework that highlights key areas where additional work to develop and build consensus around privacy standards and best practices is necessary. Indeed, a more robust Roadmap will likely be necessary to map Privacy Framework development areas given the relative dearth of well-established consensus privacy risk management standards and best practices, as compared to the significant number of established cybersecurity standards available when the Cybersecurity Framework was created.[88]
- If NIST could map how their privacy framework would help address compliance with privacy regulations around the world, it would give these companies meaningful analysis and advice on how to structure their practices to meet all of their competing obligations.[89]
- 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.[90]
- The Cybersecurity Framework points organizations to substantive and technical cybersecurity guidance and best practices in informative references. This provides users a menu of options from which to choose, and not a fixed list of requirements. The Privacy Framework should take the same approach….To the extent NIST relies on or highlights NISTIR 8062 in the Privacy Framework, it should do so only as an informative reference and with a clear explanation of its federal government focus.[91]

Specific Privacy Practices

SPECIFIC PRIVACY PRACTICES

Theme: De-identification

Summary Statement: Many respondents agreed that de-identification is an important privacy practice to include in the Framework, with some discussing specific concepts like anonymization and pseudonymization.

RFI Response Examples:

- De-identification is a key feature in national and international laws and frameworks, and its importance in privacy risk reduction is seen in the many laws that exempt de-identified data from certain requirements. HITRUST strongly believes that de-identification – both full anonymization and pseudonymization as appropriate – is one of the key best practices in data use and analysis. NIST must ensure that any controls or processes relating to de-identification require the use of proper and appropriate expertise. As we have seen throughout the internet era, re-identification of data someone deemed de-identified can be extremely easy. We must ensure a full risk analysis is considered during the de-identification process before data is used or released.[92]
- The Framework should recognize the privacy benefits of new technologies, such as de-identification techniques, homomorphic encryption, and secure multiparty computation. In doing so, the Framework should seek to help organizations determine when to use new privacy-promoting technologies, based on their risk profile and assessment.[93]
- Many cryptographic techniques that exist today or are currently being researched could be mapped to disassociability. Adopting disassociability as an objective could raise awareness of the benefits of these techniques and increase demand for more advances. A further consideration is whether a taxonomy could be constructed of existing identity-related classifications, including anonymity, de-identification, unlinkability, unobservability, pseudonymity or others. Such a taxonomy could potentially support more precise control mapping and risk mitigation.[94]
- The framework should identify how companies can implement standard “privacy-by-design” principles including data and access minimization, encryption, anonymization and pseudonymization, and others.[95]
- Data de-identification reduces privacy risks, and in combination with aggregation, the amount of personal data that is available is also significantly reduced.[96]
- As the HIPAA de-identification methodologies are widely used both within and outside of the healthcare industry, we recommend that NIST recognize these methodologies as acceptable for protecting consumer privacy under the Proposed Framework.[97]
- Consumer Reports supports the inclusion of deidentification in this list of specific privacy practices. However, NIST should expand on what deidentification means in order to require higher levels of transparency as to deidentification practices and better protections for making de-identified data public. In order for a company to assert that any such data is deidentified they should be required to document the deidentification methods used to provide for meaningful external accountability.[98]
- Here, we encourage NIST to exercise care in nuance. While information may be de-identified, in that it can be divorced from a specific direct identifier, databases with even a small number of data points are often at risk of re-identification with trivial ease. …NIST’s inquiry should look beyond simply de-identification to include anonymization and aggregation techniques that will better protect data as artificial intelligence tools continue to advance.[99]

SPECIFIC PRIVACY PRACTICES

Theme: Informing Users and Enabling Preferences

Summary Statement: Many respondents expressed strong support for practices that inform individuals about data processing practices and enable individuals to make choices and convey preferences about data processing, while recognizing shortcomings related to notice and consent.

RFI Response Examples:

- In the end, no matter what steps a data processing entity may take to mitigate risk, it is the individual who is best placed to understand the extent of a risk and make a decision based on their own context and risk threshold. This is not to say that notification is enough. Notice and choice, as experts have noted at length, is a failed model for protecting privacy. Users must have rights to effectively control the processing of their data. There must be an obligation on entities to adequately protect that data, including to meaningfully limit when and to what extent data can be processed. However, where entities are making choices regarding risk thresholds, informing individuals of the factors behind those choices and allowing them to weigh the risk for their own lives empowers people to make more informed, reasonable decisions for themselves.[100]
- The best way for companies to provide choices and a reliable understanding of what is being collected without overwhelming the consumer is to accord data collection, in the first instance, with consumer expectations. Furthermore, in order to strike the balance of effective consumer information without overwhelming the user, companies should avoid the use of user interfaces that deceive or manipulate users into acting in a way that benefits the company and not the individual. These dark patterns of design can nudge users away from choosing the privacy-protective choices made available to them.[101]
- The reality is that the risks to individuals, as well as their ability to assess and make informed decisions regarding such risks, vary considerably depending on the context of their relationship with the entity collecting their data and the context in which they provide their data. One-size fits all mandates have resulted in consumers being inundated by long, dense, legal documents that are designed to provide "notice," but frequently fail to adequately educate individuals about how their data will be used and what choices they may have related to those uses.[102]
- Enhance Transparency. FAIR on Privacy recommends that individuals should be informed of the collection and use of their personal data in a way that is meaningful, clear, obvious, and useful so they have a better understanding of what they are (or are not) consenting to with respect to their personal data. This includes being informed of the categories of companies (including third parties) who collect their personal data and how they use it. We believe our expression of this outcome in FAIR on Privacy builds on the position outlined by NTIA in its RFC but further elaborates the specific commitments that companies should be required to make to enhance transparency and create "informed consumers." NIST's Privacy Framework can play an important role in identifying, organizing, and communicating privacy risk management standards and best practices to help organizations implement enhanced transparency.[103]
- At the same time, IoT devices without screens or other direct user interfaces create significant practical challenges for privacy regimes premised on notice and consent. The notice and consent model was built on the premise that users can be given comprehensive information about an organizations privacy practices at a point in time before data is collected, as well as an opportunity to consent to those practices. That model does not translate well to IoT devices that have a limited ability to display traditional notices or collect traditional consents. The Privacy Framework should accordingly recognize that important outcomes like an informed user may be achieved in other ways.[104]
- Grounds for Processing Beyond Consent. The Framework should recognize that traditional concepts of notice and consent may not be the best method of informing and empowering users of their privacy choices, particularly for new technologies. Too often, notice and choice has resulted in long, legal, regulator-focused privacy notices and check boxes that do not effectively advance the privacy of most individuals. Indeed, regulators, advocates, academics, and consumers around the world increasingly are skeptical of notice and choice and believe that the shortcomings associated with consent in this framework are enabling companies to do what they want with personal data without sufficiently protecting privacy. The Framework can instead focus on enabling the protection of consumer privacy through tools that

empower individuals to control how their personal data is used, as well as through continuous risk-based analyses designed to ensure the protection of individuals' information. The Framework also should recognize that consumers reasonably expect companies to engage in certain types of data processing in the context of their relationship and activity, and that consent may not be needed when the collection or use of data is either obvious from the context of the transaction or sufficiently accepted or necessary for public policy reasons.[105]

- The status quo—largely comprised of click-wrap consent agreements—does not alleviate this information asymmetry. And the status quo also leaves consumers vulnerable to another consequence of commercialized data collection—data breaches.[106]
- The Coalition also urges NIST to encourage organizations to move beyond traditional notice and consent regimes when broaching the subject of how to address data privacy and security together.[107]

SPECIFIC PRIVACY PRACTICES

Theme: Control and Data Management

Summary Statement: Several respondents reflected on practices related to control – in some cases meaning users having control over or access to their data, and in other cases, organizations controlling and managing data, including data deletion, data segmentation, use of metadata, and data portability. Responses included support for certain practices, as well as cautionary points.

RFI Response Examples:

- Protecting an individuals' privacy starts with being able to control what happens to, or who has access to the data an organization has collected about the individual.[108]
- Access. Companies should recognize that data belongs to users, and it should be easy for users to get a copy of, correct, and delete their personal information.[109]
- I urge a paradigm shift that recognizes consumers' valuable property interest in their data, and requires adequate procedural safeguards to protect meaningful control over and consent to sharing consumer data, by consumers. Consumers should have more control over their data; NIST should take this opportunity to help shift the current paradigm and empower consumers.[110]
- The Framework should support managing privacy risk in a way that respects people and communities. This includes acknowledging that, in many cases, there is no single best answer to a privacy question. For example, some people prefer to see tailored ads and content while others prefer to minimize personalization of their experience. Neither of these views is inherently problematic for privacy. Organizations should plan to account for diversity in privacy preferences while building their systems, thus providing users with intuitive choices to control their data and experience.[111]
- NIST's Privacy Framework must recommend that organizations control, monitor, and audit privileged access to prevent attacks from insiders with valid access, insiders with improperly escalated access, and bad actors inside or outside the organization that have stolen privileged access credentials.[112]
- 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…[113]
- …some specific outcomes may be: Can a company quickly locate all data for an individual, especially without well-defined IDs? Can it delete all the information for an individual without undue hardship? Is it able to follow up with all the partners to whom they sent personal data for an individual and able to understand the provenance of any specific piece of data that it has about an individual?[114]
- Specifically, the framework should consider how individuals may differ in how they regulate and control information they consider private and confidential. If a physician is not aware of, or does not contemplate, a patient's desires regarding privacy expectations, the medical encounter can be counterproductive for patients and physicians alike.[115]
- …data portability is not addressed in this Privacy Framework. Consumers need the ability to not only see what data companies have about them but also the right to take their consumer data elsewhere.[116]
- …requiring the documentation of the flow of data, at use, at rest and in transit, when encrypted and the level of information handled would align with other current standards, frameworks and models.[117]
- …we note that specific challenges frequently observed include: controlling the flow of individual data; the ability to ensure individual data secured through specific source transactions remains secured and within the confines and context of the specific engagement; managing the retained data and associated data management risk in retention of the volume of data sets; and the number of connected devices increasing the challenges of ensuring sustained privacy.[118]

SPECIFIC PRIVACY PRACTICES

Theme: Data Minimization

Summary Statement: A number of respondents raised the topic of data minimization, although the responses reflected a degree of ambiguity, alternately framing it as an important principle (see the "*Principles, Information Lifecycle, and Goals/Objectives*" theme) and as a privacy practice that can be implemented. Respondents also described practices that support data minimization, including default privacy-friendly settings and data management practices like deletion (see the "*Control and Data Management*" theme).

RFI Response Examples:

- Data Collection/Use Limits: Enterprises and government must limit the collection of PII and minimize its retention by, for example, only acquiring and retaining data essential to provide service to active clients. Minimization: Private and government sector actors must be required to mitigate the risk of PII breaches by minimizing the identifiability of data created, collected, and retained regardless of how minimal or briefly held that data is. Individuals also should be informed that, in many cases, it may not be essential to provide PII simply because it's requested.[119]
- Privacy settings should be set to minimize the amount of data collected about the user by default. Data minimization, done correctly, would redistribute the onus of good data practices onto the company and off of the consumer. Consumers are already overwhelmed with the number of decisions they are asked to make. Consumers should be empowered to use products without fear that the service or product will mine and collect more data than the consumer would reasonably expect. Ever-present pop-up dialogs and byzantine user controls do not serve users well; instead, consumers should be entitled to expect that data collection and sharing will be limited to the context of their interactions with any given company.[120]
- The most challenging practice to put in place for many entities is setting strong default privacy settings. As we have seen through responses to breaches from large technology companies, many existing products and services were not designed to allow granular consent or collect personal data in a way that labels it with the use for which it was collected. Without combating this challenge and growing the field of privacy by design, we will not see the substantial growth needed in privacy risk reduction worldwide.[121]
- 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.[122]
- The adoption of mechanisms that limit data collection and enforce the notion of data lifecycle and data aging are vital for a future privacy framework. The ubiquitous nature of IoT devices supports a mandate requiring organizations to adopt policies focusing on a clear identification of the data gathered by organizations, its domain, and the associated lifecycle, which includes its eventual deletion." [123]
- We map the data through its lifecycle and -- except the data we are legally obligated to keep -- delete personal data according to the principles of data minimization and the right of a data subject to object to processing.[124]
- 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:…E. Mitigate dangerous or unnecessary content through data minimization activities including retention management and purging, encryption in place, anonymization…[125]
- Data minimization, user controls, and strong enforcement should be central to any approach to consumer privacy.[126]
- …Payfone has identified five important building blocks for identity privacy, these are: 1. Data Minimization to reduce overall privacy attack surface…[127]

SPECIFIC PRIVACY PRACTICES

Theme: Encryption

Summary Statement: Many respondents expressed support for including encryption as a privacy practice in the Framework, while some noted the need to have flexibility for various contexts, particularly in the healthcare sector, where data may need to be associated with specific individuals.

RFI Response Examples:

- Encryption and/or Tokenization should be applied to private data to render it useless if stolen which reduces the risk to the individual.[128]
- Formal processes should be implemented to protect personal data and address privacy risks. While these may currently be built into incident response plans, it may be of benefit to widen their reach, giving greater attention toward prevention as well (i.e., investments in encryption; centralized key systems, etc.). The requirements for these formal processes should be like the requirements of GDPR as well as the consequences. An exceptional Privacy Framework would benefit greatly from a comprehensive and complementary Federal data protection act that enforces the protection of personal data.[129]
- If these practices are not currently employed in most organizations, they should be considered. One of these items stood out from the rest: Use of cryptographic technology to achieve privacy outcomes—for example, the disassociability privacy engineering objective. Encryption and centralized key management is the key (so to speak) to achieving compliance with Article 25 over Data Subjects' Rights, even though Privacy by Design to achieve Privacy by Default has occurred. Meaning, the Article 25 objective is to apply privacy principles and perform a risk assessment, utilize available technology, and prevent a breach of data subjects' rights. A way to assure that, in today's breach-prone environment, is to implement a centralized key management solution over encrypted data…All these practices are critical to the protection of individuals' privacy, with centralized encryption key management and encryption or tokenization efforts being among the most critical.[130]
- …a worthwhile privacy framework necessarily requires appropriate security controls. Safeguards such as encryption, pseudonymization, enforceable codes of conduct, and security protections enable data use for socially beneficial purposes, while reducing risk of misuse or harm to individuals.[131]
- We would also urge NIST to take up research on the ways technical measures like encryption benefit user privacy. We rely on encryption to build our cybersecurity products and keep our customers' data secure, and we believe that it is key to privacy on the internet.[132]
- The AMA urges caution around disassociability in certain contexts in health care. Disassociability focuses on enabling a data system to process personal information or events without association to individuals or devices beyond the system's operational requirements. This decoupling "blinds" an individual's identity or activities from undue exposure, thus actively protecting that individual from privacy risk. In the practice of medicine, data systems may need to associate personal information to a patient or a patient's device. Otherwise, care may be negatively impacted. Thus, the disassociability privacy engineering objective as a use of cryptographic technology may not be appropriate in the health care industry.[133]
- Data Security: Actors in all data ecosystems must take affirmative steps (e.g., using strong encryption) to safeguard PII to prevent its inappropriate access and use.[134]
- Perhaps the most promising avenue for social graph portability would be for social network providers to allow the export of encrypted versions of your and your contacts' unique user IDs to obscure those IDs while also providing authentication, such that your relationships could only be automatically replicated on another service by your actual contacts, and only with consent from both you and them. However, offering such a privacy-protective social graph portability feature would require a major collaborative technical effort that could raise unanticipated privacy and security challenges as well as legal compliance questions, which is why companies and policymakers—including the FTC—need to start discussing and developing such approaches now.[135]

SPECIFIC PRIVACY PRACTICES

Theme: Emerging Technologies

Summary Statement: Respondents generally considered that the Framework should be inclusive of emerging technologies, including the internet of things and artificial intelligence.

RFI Response Examples:

- Algorithmic decision tools and predictive analytics are being used to make decisions about consumers without sufficient transparency, testing, or accountability. While there is great potential in these emerging technologies, consumers need greater protections for the use of these tools. Therefore, we urge a federal entity like the Federal Trade Commission or NIST to give guidance directing companies and organizations that use algorithms to do regular assessments of the accuracy of the algorithmic decisions, and to inspect the source code in order to root out any inherent or sample-bias that has been embedded in the algorithm….NIST should craft guidelines for the use of algorithms to help determine whether a particular algorithm produces decisions that are fair, accurate and representative.[136]
- The AMA believes privacy practices are relevant for new technologies like the Internet of Things, artificial intelligence, and genomic sequencing. Specifically, proper data management and enabling users to have a reliable understanding about how information is being collected, stored, used, and shared should be adopted. While the types of data items are not new, these technologies provide greater potential access of those data items to other individuals or entities.[137]
- Regarding whether these practices are relevant for new technologies like the Internet of Things (IoT) and Artificial Intelligence (AI), IoT systems address the interaction of computing resources with physical entities through sensors and actuators, and an IoT environment is an environment of connected components that can be combined to form IoT systems. Communication is fundamental to IoT, and communication systems must be interconnectable, inter-workable, and interoperable, bringing potential privacy threats that could exploit vulnerabilities. IEEE P2413, Standard for An Architectural Framework for the Internet of Things (IoT), addresses the common concern of assurance in how to convince stakeholders that obligations for being safe, reliable, resilient, secure, and meeting privacy expectations are met.[138]
- The need for interoperability and strong management practices are particularly acute for new technologies such as the Internet of Things ("IoT") and Artificial Intelligence ("AI"). Voluntary, consensus-based standards provide a basis for facilitating these objectives. The Privacy Framework should not only be interoperable with other frameworks and standards, but also ensure that IoT and AI systems developed in consultation with the Privacy Framework will be able to interoperate with other devices and systems. Several other countries have national strategies expressing support for standards that facilitate this type of globally-connected IoT devices, including the U.K. and South Korea…The Privacy Framework should help organizations use and build upon upcoming new technologies including AI and IoT and reflect the use of data in the development of those technologies. U.S. leadership is critical for protecting U.S. consumers, institutions, and industry competiveness and innovation in the era of digital transformation.[139]
- A Privacy Framework that is inclusive of such immersive technologies and takes into consideration how organizations developing and deploying such technologies and devices, be it for enterprise or consumer use, and individuals using such technologies is paramount as we anticipate increased use of AR and other immersive technologies in the near future. These technologies hold tremendous promise to improve enterprise efficiencies, but also holds the potential to introduce new or additional privacy vulnerabilities and concerns, and may compromise in particular the enterprise in regard to compliance issues, financial loss and reputation and brand.[140]

[1] Erica Fox, Cloudflare at 4-5.
https://www.nist.gov/sites/default/files/documents/2018/12/21/20181221_cloudflare_erica_fox_comments_for_nist_re_consumer_privacy_508.pdf
[2] Brian Scarpelli, ACT The App Association at 5.
https://www.nist.gov/sites/default/files/documents/2019/02/04/act_brian_scarpelli_508.pdf
[3] The Bank Policy Institute, American Bankers Association and the Securities Industry and Financial Markets Association at 2.
https://www.nist.gov/sites/default/files/documents/2019/02/04/bpi-aba-sifma_bpi-aba-sifma_508.pdf
[4] Carl A. Anderson, HITRUST at 3.
https://www.nist.gov/sites/default/files/documents/2019/02/04/hitrust_carl_anderson_calvin_beebe_508.pdf
[5] Tina Grande, Confidentiality Coalition at 2.
https://www.nist.gov/sites/default/files/documents/2019/02/04/confidentialitycoalition_tina_grande_508.pdf
[6] Alan Calder, IT Governance USA at 1.
https://www.nist.gov/sites/default/files/documents/2018/12/21/20181221_it_governance_alan_calder_nist_privacy_framework_comments_508.pdf
[7] Angela Gleason, American Property Casualty Insurance Association at 1.
https://www.nist.gov/sites/default/files/documents/2019/02/04/apcia_angela_gleason_508.pdf
[8] Michael Pagels, Centers for Medicare & Medicaid Services at 2.
https://www.nist.gov/sites/default/files/documents/2019/02/04/cms_michael_pagels_508.pdf
[9] Jamie Ferguson and Lori Potter, Kaiser Permanente at 6.
https://www.nist.gov/sites/default/files/documents/2019/02/04/kp_jamie_ferguson_lori_potter_508.pdf
[10] Jason P. Matusow, Microsoft Corporation at 4.
https://www.nist.gov/sites/default/files/documents/2019/02/04/microsoft_jason_matusow_508.pdf
[11] Konstantinos Karachalios and Karen McCabe, IEEE at 4-5.
https://www.nist.gov/sites/default/files/documents/2019/02/04/ieee_konstantinos_karachalios_karen_mccabe_508.pdf
[12] Alan Calder, IT Governance USA at 2.
https://www.nist.gov/sites/default/files/documents/2018/12/21/20181221_it_governance_alan_calder_nist_privacy_framework_comments_508.pdf
[13] Katie Ignaszewski, IBM at 4-5.
https://www.nist.gov/sites/default/files/documents/2019/02/04/ibm_katie_ignaszewski_508.pdf
[14] The Federated Identity Resilient Ecosystem at 4.
https://www.nist.gov/sites/default/files/documents/2019/02/04/fire_the_federated_identity_resilient_ecosystem_subgroup_508.pdf
[15] Thomas C. Power and Melanie K. Tiano, CTIA at 9.
https://www.nist.gov/sites/default/files/documents/2019/02/04/ctia_thomas_power_melanie_tiano_508.pdf
[16] Marilyn Zigmund Luke, America's Health Insurance Plans at 1.
https://www.nist.gov/sites/default/files/documents/2019/02/04/ahip_marilyn_zigmund_luke_508.pdf
[17] Amie Stepanovich, Estelle Massé and Nathan White, Access Now at 4.
https://www.nist.gov/sites/default/files/documents/2018/12/12/nist_privacy_engineering_comments_from_access_now.pdf
[18] Angela Gleason, American Property Casualty Insurance Association at 1.
https://www.nist.gov/sites/default/files/documents/2019/02/04/apcia_angela_gleason_508.pdf
[19] Internet Association at 5.
https://www.nist.gov/sites/default/files/documents/2019/02/04/internetassociation_internetassociation_508.pdf
[20] Stephanie Hall, National Association of Manufacturers at 2.
https://www.nist.gov/sites/default/files/documents/2019/02/04/nam_stephanie_hall_508.pdf
[21] Engine at 2.
https://www.nist.gov/sites/default/files/documents/2019/02/04/engine_engine_508.pdf
[22] Katie Ignaszewski, IBM at 4.
https://www.nist.gov/sites/default/files/documents/2019/02/04/ibm_katie_ignaszewski_508.pdf
[23] Shaundra Watson, BSA The Software Alliance at 3.
https://www.nist.gov/sites/default/files/documents/2019/02/04/bsa_shaundra_watson_508.pdf
[24] James Madara, American Medical Association at 3.
https://www.nist.gov/sites/default/files/documents/2018/12/21/20181220_ama_madera_nist_rfi_on_privacy_framework_508.pdf
[25] Anthony Johnson, Bureau of Engraving and Printing at 1.

https://www.nist.gov/sites/default/files/documents/2018/12/18/20181214_bep_anthony_johnson_privacy_framework_comments_508.pdf
[26] Workday at 2.
https://www.nist.gov/sites/default/files/documents/2019/02/04/workday_workday.pdf
[27] Jamie Ferguson and Lori Potter, Kaiser Permanente at 3.
https://www.nist.gov/sites/default/files/documents/2019/02/04/kp_jamie_ferguson_lori_potter_508.pdf
[28] Dan Frank, Deloitte at 4.
https://www.nist.gov/sites/default/files/documents/2019/02/04/deloitte_dan_frank_508.pdf
[29] Stuart Shapiro and Julie Snyder, The MITRE Corporation at 2.
https://www.nist.gov/sites/default/files/documents/2019/02/04/mitre_stuart_shapiro_julie_snyder_508.pdf
[30] Andrew L Soodek, Secure Compliance Solutions LLC at 5.
https://www.nist.gov/sites/default/files/documents/2019/02/04/scs_andrew_soodek.pdf
[31] The Better Identity Coalition at 4.
https://www.nist.gov/sites/default/files/documents/2019/02/04/bic_jeremy_grant_508.pdf
[32] McAfee at 6.
https://www.nist.gov/sites/default/files/documents/2019/02/04/mcafee_kent_landfield_508.pdf
[33] Internet Society at 2.
https://www.nist.gov/sites/default/files/documents/2019/02/15/tis_the_internet_society_508.pdf
[34] Thomas C. Power and Melanie K. Tiano, CTIA at 8-9.
https://www.nist.gov/sites/default/files/documents/2019/02/04/ctia_thomas_power_melanie_tiano_508.pdf
[35] Amie Stepanovich, Estelle Massé and Nathan White, Access Now at 2.
https://www.nist.gov/sites/default/files/documents/2018/12/12/nist_privacy_engineering_comments_from_access_now.pdf
[36] Alan Calder, IT Governance USA at 2-3.
https://www.nist.gov/sites/default/files/documents/2018/12/21/20181221_it_governance_alan_calder_nist_privacy_framework_comments_508.pdf
[37] Konstantinos Karachalios and Karen McCabe, IEEE at 2.
https://www.nist.gov/sites/default/files/documents/2019/02/04/ieee_konstantinos_karachalios_karen_mccabe_508.pdf
[38] Mark Brnovich, Attorney General of Arizona at 1.
https://www.nist.gov/sites/default/files/documents/2019/02/04/ag_az_mark_brnovich_508.pdf
[39] Internet Association at 4.
https://www.nist.gov/sites/default/files/documents/2019/02/04/internetassociation_internetassociation_508.pdf
[40] Janine Hiller at 1.
https://www.nist.gov/sites/default/files/documents/2019/02/04/vt_janine_hiller.pdf
[41] Shaundra Watson, BSA | The Software Alliance at 3.
https://www.nist.gov/sites/default/files/documents/2019/02/04/bsa_shaundra_watson_508.pdf
[42] Michael Petricone and Rachel S. Nemeth, Consumer Technology Association at 7.
https://www.nist.gov/sites/default/files/documents/2019/02/04/cta_michael_petricone_rachel_nemeth_508.pdf
[43] Tim Day, U.S. Chamber of Commerce Technology Engagement Center at 4.
https://www.nist.gov/sites/default/files/documents/2019/02/04/tec_tim_day.pdf
[44] Loretta Polk, Rick Chessen, NCTA – The Internet & Television Association at 5.
https://www.nist.gov/sites/default/files/documents/2019/02/04/ncta_loretta_polk_rick_chessen_508.pdf
[45] Daniel Fabbri, Maize Analytics at 2-3.
https://www.nist.gov/sites/default/files/documents/2019/02/04/maize_daniel_fabbri_508.pdf
[46] James Hendler, Association for Computing Machinery at 3.
https://www.nist.gov/sites/default/files/documents/2019/02/14/acm-james_hendler.pdf
[47] Lea Kissner, Google at 3.
https://www.nist.gov/sites/default/files/documents/2019/02/04/google_lea_kissner_508.pdf
[48] The Bank Policy Institute, American Bankers Association and the Securities Industry and Financial Markets Association at 7.
https://www.nist.gov/sites/default/files/documents/2019/02/04/bpi-aba-sifma_bpi-aba-sifma_508.pdf
[49] Daniel Fabrri, Maize Analytics at 4.
https://www.nist.gov/sites/default/files/documents/2019/02/04/maize_daniel_fabbri_508.pdf
[50] Lindsey Finch, Salesforce at 2.
https://www.nist.gov/sites/default/files/documents/2019/02/04/salesforce_lindsey.pdf
[51] John Miller, Information Technology Industry Council at 2.
https://www.nist.gov/sites/default/files/documents/2019/02/04/iti_john_miller_508.pdf
[52] Katie Ignaszewski, IBM at 2.
https://www.nist.gov/sites/default/files/documents/2019/02/04/ibm_katie_ignaszewski_508.pdf
[53] Erica Fox, Cloudflare at 2-3.

https://www.nist.gov/sites/default/files/documents/2018/12/21/20181221_cloudflare_erica_fox_comments_for_nist_re_consumer_privacy_508.pdf
[54] Kenya N. Wiley, Fashion Innovation Alliance at 4.
https://www.nist.gov/sites/default/files/documents/2019/02/08/fia_kenya_wiley_rfi_response.pdf
[55] McAfee at 10.
https://www.nist.gov/sites/default/files/documents/2019/02/04/mcafee_kent_landfield_508.pdf
[56] Lea Kissner, Google at 4-5.
https://www.nist.gov/sites/default/files/documents/2019/02/04/google_lea_kissner_508.pdf
[57] Carl A. Anderson, HITRUST at 3.
https://www.nist.gov/sites/default/files/documents/2019/02/04/hitrust_carl_anderson_calvin_beebe_508.pdf
[58] Jason P. Matusow, Microsoft at 11.
https://www.nist.gov/sites/default/files/documents/2019/02/04/microsoft_jason_matusow_508.pdf
[59] Security Industry Association at 4.
https://www.nist.gov/sites/default/files/documents/2019/02/04/sia_sia.pdf
[60] Brian Scarpelli, ACT The App Association at 3.
https://www.nist.gov/sites/default/files/documents/2019/02/04/act_brian_scarpelli_508.pdf
[61] Brian Cummings, Tata Consultancy Services at 1.
https://www.nist.gov/sites/default/files/documents/2018/12/19/20181217_tcs_brian_cummings_nist_privacy_framework_508.pdf
[62] Dylan Gilbert, Public Knowledge at 4.
https://www.nist.gov/sites/default/files/documents/2019/02/05/public_knowledge_dylan_gilbert.pdf
[63] Threat Sketch at 5. https://www.nist.gov/sites/default/files/documents/2019/02/04/threatsketch_threatsketch.pdf
[64] Karen Greenhalgh, Cyber Tygr at 1.
https://www.nist.gov/sites/default/files/documents/2019/02/04/cybertygr_karen_greenhalgh_508.pdf
[65] Jason P. Matusow, Microsoft at 13.
https://www.nist.gov/sites/default/files/documents/2019/02/04/microsoft_jason_matusow_508.pdf
[66] Cybersecurity Coalition at 3.
https://www.nist.gov/sites/default/files/documents/2019/02/04/cybersecuritycoalition_cybersecuritycoalition_508.pdf
[67] Eric Wenger, Cisco at 2. https://www.nist.gov/sites/default/files/documents/2019/02/04/cisco_eric_wenger_508.pdf
[68] The Bank Policy Institute, American Bankers Association and the Securities Industry and Financial Markets Association at 3.
https://www.nist.gov/sites/default/files/documents/2019/02/04/bpi-aba-sifma_bpi-aba-sifma_508.pdf
[69] McAfee at 12.
https://www.nist.gov/sites/default/files/documents/2019/02/04/mcafee_kent_landfield_508.pdf
[70] Kuljeet Kaur, Opus Fund Services at 1.
https://www.nist.gov/sites/default/files/documents/2019/02/04/nist_rfi-opus_fund_services.pdf
[71] John Miller, Information Technology Industry Council at 12-13.
https://www.nist.gov/sites/default/files/documents/2019/02/04/iti_john_miller_508.pdf
[72] Carl Anderson, HITRUST at 3.
https://www.nist.gov/sites/default/files/documents/2019/02/04/hitrust_carl_anderson_calvin_beebe_508.pdf
[73] Lee Barrett, Electronic Healthcare Network Accreditation Commission at 6.
https://www.nist.gov/sites/default/files/documents/2019/02/04/ehnac_lee_barrett_508.pdf
[74] Katie McInnis, Consumer Reports at 5.
https://www.nist.gov/sites/default/files/documents/2019/02/04/con_rep_katie_mcinnis_508.pdf
[75] Jeff Greene, Symantec at 3. https://www.nist.gov/sites/default/files/documents/2019/02/04/symantec_jeff_greene.pdf
[76] Joshua Seidemann, NTCA-The Rural Broadband Association at 7-8.
https://www.nist.gov/sites/default/files/documents/2019/02/04/ntca_joshua_seidemann.pdf
[77] Daniel Fabbri, Maize Analytics at 1.
https://www.nist.gov/sites/default/files/documents/2019/02/04/maize_daniel_fabbri_508.pdf
[78] Dan Frank, Deloitte at 5-6. https://www.nist.gov/sites/default/files/documents/2019/02/04/deloitte_dan_frank_508.pdf
[79] Andrew Soodek, Secure Compliance Solutions at 7.
https://www.nist.gov/sites/default/files/documents/2019/02/04/scs_andrew_soodek.pdf
[80] Workday at 5.
https://www.nist.gov/sites/default/files/documents/2019/02/04/workday_workday.pdf
[81] Carl Anderson, HITRUST at 2.
https://www.nist.gov/sites/default/files/documents/2019/02/04/hitrust_carl_anderson_calvin_beebe_508.pdf
[82] Andrew Neal at 3.
https://www.nist.gov/sites/default/files/documents/2019/02/04/cit_andrew_neal_508.pdf
[83] Eric Wenger, Cisco at 2. https://www.nist.gov/sites/default/files/documents/2019/02/04/cisco_eric_wenger_508.pdf

[84] Jeff Greene, Symantec at 3. https://www.nist.gov/sites/default/files/documents/2019/02/04/symantec_jeff_greene.pdf
[85] James Crandall, American Petroleum Institute at 7.
https://www.nist.gov/sites/default/files/documents/2019/02/04/api_james_crandall_508.pdf
[86] Jamie Ferguson and Lori Potter, Kaiser Permanente at 7.
https://www.nist.gov/sites/default/files/documents/2019/02/04/kp_jamie_ferguson_lori_potter_508.pdf
[87] Kenya Wiley, Fashion Innovation Alliance at 3.
https://www.nist.gov/sites/default/files/documents/2019/02/08/fia_kenya_wiley_rfi_response.pdf
[88] John Miller, Information Technology Industry Council at 3.
https://www.nist.gov/sites/default/files/documents/2019/02/04/iti_john_miller_508.pdf
[89] Erica Fox, Cloudflare at 5.
https://www.nist.gov/sites/default/files/documents/2018/12/21/20181221_cloudflare_erica_fox_comments_for_nist_re_consumer_privacy_508.pdf
[90] IDmachines at 9.
https://www.nist.gov/sites/default/files/documents/2019/02/04/idmachines_idmachines_508.pdf
[91] Thomas C. Power and Melanie K. Tiano, CTIA at 12, 17.
https://www.nist.gov/sites/default/files/documents/2019/02/04/ctia_thomas_power_melanie_tiano_508.pdf
[92] Carl A. Anderson, HITRUST at 3-4.
https://www.nist.gov/sites/default/files/documents/2019/02/04/hitrust_carl_anderson_calvin_beebe_508.pdf
[93] Jason P. Matusow, Microsoft at 7.
https://www.nist.gov/sites/default/files/documents/2019/02/04/microsoft_jason_matusow_508.pdf
[94] Charles Jaffe, Health Level Seven International at 4.
https://www.nist.gov/sites/default/files/documents/2019/02/04/hl7_charles_jaffe_508.pdf
[95] Dr. Amol Deshpande, WireWheel at 2.
https://www.nist.gov/sites/default/files/documents/2019/02/04/wirewheel_amol_deshpande.pdf
[96] B. Lynn Follansbee, US Telecom – The Broadband Association at 4.
https://www.nist.gov/sites/default/files/documents/2019/02/04/ustelecom_b._lynn_follansbee.pdf
[97] Tina Grande, Confidentiality Coalition at 2.
https://www.nist.gov/sites/default/files/documents/2019/02/04/confidentialitycoalition_tina_grande_508.pdf
[98] Katie McInnis, Consumer Reports at 5-6.
https://www.nist.gov/sites/default/files/documents/2019/02/04/con_rep_katie_mcinnis_508.pdf
[99] Amie Stepanovich, Estelle Massé and Nathan White, Access Now at 5-6.
https://www.nist.gov/sites/default/files/documents/2018/12/12/nist_privacy_engineering_comments_from_access_now.pdf
[100] Id. at 4.
[101] Katie McInnis, Consumer Reports at 6-7.
https://www.nist.gov/sites/default/files/documents/2019/02/04/con_rep_katie_mcinnis_508.pdf
[102] Internet Association at 4.
https://www.nist.gov/sites/default/files/documents/2019/02/04/internetassociation_internetassociation_508.pdf
[103] John Miller, Information Technology Industry Council at 5.
https://www.nist.gov/sites/default/files/documents/2019/02/04/iti_john_miller_508.pdf
[104] Jason P. Matusow, Microsoft at 6.
https://www.nist.gov/sites/default/files/documents/2019/02/04/microsoft_jason_matusow_508.pdf
[105] Id. at 7.
[106] Mark Brnovich, Arizona Attorney General at 1.
https://www.nist.gov/sites/default/files/documents/2019/02/04/ag_az_mark_brnovich_508.pdf
[107] Cybersecurity Coalition at 4.
https://www.nist.gov/sites/default/files/documents/2019/02/04/cybersecuritycoalition_cybersecuritycoalition_508.pdf
[108] Jeff Greene, Symantec at 4.
https://www.nist.gov/sites/default/files/documents/2019/02/04/symantec_jeff_greene.pdf
[109] Apple at 2.
https://www.nist.gov/sites/default/files/documents/2019/02/04/apl_apple_508.pdf
[110] Mark Brnovich, Arizona Attorney General at 2.
https://www.nist.gov/sites/default/files/documents/2019/02/04/ag_az_mark_brnovich_508.pdf
[111] Lea Kissner, Google at 4. https://www.nist.gov/sites/default/files/documents/2019/02/04/google_lea_kissner_508.pdf
[112] One Identity at 2-3.
https://www.nist.gov/sites/default/files/documents/2019/02/04/oneidentity_one_identity.pdf
[113] Nuix at 2.
https://www.nist.gov/sites/default/files/documents/2019/02/04/nuix_nuix.pdf
[114] Dr. Amol Deshpande, WireWheel at 3.

https://www.nist.gov/sites/default/files/documents/2019/02/04/wirewheel_amol_deshpande.pdf
[115] James L. Madara, American Medical Association at 2.
https://www.nist.gov/sites/default/files/documents/2018/12/21/20181220_ama_madera_nist_rfi_on_privacy_framework_508.pdf
[116] Katie McInnis, Consumer Reports at 11.
https://www.nist.gov/sites/default/files/documents/2019/02/04/con_rep_katie_mcinnis_508.pdf
[117] Lee Barrett, Electronic Healthcare Network Accreditation Commission at 4.
https://www.nist.gov/sites/default/files/documents/2019/02/04/ehnac_lee_barrett_508.pdf
[118] Konstantinos Karachalios, IEEE at 1.
https://www.nist.gov/sites/default/files/documents/2019/02/04/ieee_konstantinos_karachalios_karen_mccabe_508.pdf
[119] James Hendler, Association for Computing Machinery at 5.
https://www.nist.gov/sites/default/files/documents/2019/02/14/acm-james_hendler.pdf
[120] Katie McInnis, Consumer Reports at 8.
https://www.nist.gov/sites/default/files/documents/2019/02/04/con_rep_katie_mcinnis_508.pdf
[121] Carl Anderson, HITRUST at 4.
https://www.nist.gov/sites/default/files/documents/2019/02/04/hitrust_carl_anderson_calvin_beebe_508.pdf
[122] Dan Frank, Deloitte at 7. https://www.nist.gov/sites/default/files/documents/2019/02/04/deloitte_dan_frank_508.pdf
[123] Working Group for IEEE Project 1912 at 6.
https://www.nist.gov/sites/default/files/documents/2019/02/04/ieee_1912_the_working_group_for_ieee_project_1912_508.pdf
[124] Erica Fox, Cloudflare at 6.
https://www.nist.gov/sites/default/files/documents/2018/12/21/20181221_cloudflare_erica_fox_comments_for_nist_re_consumer_privacy_508.pdf
[125] Nuix at 2.
https://www.nist.gov/sites/default/files/documents/2019/02/04/nuix_nuix.pdf
[126] Eric Null, New America's Open Technology Institute at 1.
https://www.nist.gov/sites/default/files/documents/2019/02/04/oti_eric_null.pdf
[127] Aidan Herbert, Payfone at 1.
https://www.nist.gov/sites/default/files/documents/2019/02/04/payfone_aidan_herbert.pdf
[128] Jeff Greene, Symantec at 5.
https://www.nist.gov/sites/default/files/documents/2019/02/04/symantec_jeff_greene.pdf
[129] ISACA at 3.
https://www.nist.gov/sites/default/files/documents/2019/02/04/isaca_isaca_508.pdf
[130] Id. at 6-7.
[131] B. Lynn Follansbee, US Telecom – The Broadband Association at 4.
https://www.nist.gov/sites/default/files/documents/2019/02/04/ustelecom_b._lynn_follansbee.pdf
[132] Erica Fox, Cloudflare at 3.
https://www.nist.gov/sites/default/files/documents/2018/12/21/20181221_cloudflare_erica_fox_comments_for_nist_re_consumer_privacy_508.pdf
[133] James L. Madara, American Medical Association at 4.
https://www.nist.gov/sites/default/files/documents/2018/12/21/20181220_ama_madera_nist_rfi_on_privacy_framework_508.pdf
[134] James Hendler, Association for Computing Machinery at 5.
https://www.nist.gov/sites/default/files/documents/2019/02/14/acm-james_hendler.pdf
[135] Eric Null, New America's Open Technology Institute at 6-7.
https://www.nist.gov/sites/default/files/documents/2019/02/04/oti_eric_null.pdf
[136] Katie McInnis, Consumer Reports at 13.
https://www.nist.gov/sites/default/files/documents/2019/02/04/con_rep_katie_mcinnis_508.pdf
[137] James L. Madara, American Medical Association, at 5.
https://www.nist.gov/sites/default/files/documents/2018/12/21/20181220_ama_madera_nist_rfi_on_privacy_framework_508.pdf
[138] Konstantinos Karachalios and Karen McCabe, IEEE at 5.
https://www.nist.gov/sites/default/files/documents/2019/02/04/ieee_konstantinos_karachalios_karen_mccabe_508.pdf
[139] Jason P. Matusow, Microsoft Corporation at 4,6.
https://www.nist.gov/sites/default/files/documents/2019/02/04/microsoft_jason_matusow_508.pdf
[140] Rob LaBelle, Brainwave, LLC at 2.
https://www.nist.gov/sites/default/files/documents/2019/02/04/brainwaive_rob_labelle_508.pdf