KPMG LLP response to NIST privacy framework RFI
James Lai
Nicholas Schmidt
Daniel Beihoff

ORGANIZATIONAL CONSIDERATIONS	
1. The greatest challenges in improving organizations' privacy protections for individuals.	1. Culturally, organizations often fail to understand individuals' expectations when it comes to how their personal information are collected and used. Organizations also misunderstand the perceptions of consumers. Just because information is collected doesn't mean that it should be owned and used at the collector's discretion. In the consumer landscape we see this in the pervasive surveillance of online and real-world activities for the purposes of generating advertising that are both intrusive and of low value. For example, viewing websites that sell a product often lead to ads for the product that show up long after the consumer has already made their purchasing decision. Shopping for other people often results in seeing ads for products that aren't generally relevant to people's interests. These ads are low value because advertisers have no idea how long behavioral information are valid and lack context around the underlying reasons that people do things online so they promote products or services people have already bought or that they aren't usually interested in. The ads are intrusive because they make it clear that people's behaviors are being mined, profiled, and sold. Organizations also often fail to understand the value people place on their privacy. Behavior-based car insurance products are a good example. These products purport to let safe drivers save money on premiums by letting the insurer monitor their driving habits. These products have not seen wide adoption. In the world of HR privacy this disconnect manifests in similar ways, such as the increasing use of "wellness" programs that "encourage" people to use wearable devices that collect activity data and use it to generate fitness goals even though these programs often unintentionally discriminate against individuals

	with disabilities and make sensitive personal information available to third parties without regard for what they intend to do with that information. These examples demonstrate that individuals are not stakeholders in whatever processes businesses are using to make decisions that impact individuals' privacy expectations. Some legal frameworks like GDPR go so far as to make consultation with individuals a key part of the privacy risk assessment process. Regardless of whether a NIST privacy framework adopts that model or relies on privacy professionals working with organizations to stand in for individuals, organizations need to understand people's reasonable expectations around the processing of their personal information. 2. Even where organizations make strong statements relating to their commitments to understanding and respecting individuals' expectations around the collection and use of their personal information, many of them face challenges implementing and following their own commitments as evidenced by the sheer number of privacy breaches announced by otherwise sophisticated organizations. These incidents often arise because of poor information lifecycle management, lack of master data management and data quality capabilities, and insufficient application of metadata to information repositories that organizations could use to identify, classify, and keep track of personal information that they have collected. These metadata could be used to identify when data are no longer useful and thus subject to archiving / destruction pursuant to records management practices; track individual preferences around use of that data; enable exercise of individual "ARCO" and similar rights; and help detect patterns that might signal a data breach. 3. Even if organizations have mature practices around information lifecycle management and

	robust master data capabilities, many fail to address privacy risks in a timely fashion. As a result, privacy reviews often result in having to redo development work, which creates a bad experience for personnel and can lead to poor relationships between privacy resources and business contacts. Loss of trust in privacy practitioners within an organization can undermine their effectiveness and increase the risk of harm to the organization and to individuals if stakeholders try to avoid engaging with the privacy program. Too many privacy teams are asking "what did you do?" instead of "what are you planning to accomplish?" Organizations need to identify opportunities for earlier engagement so that understanding and managing privacy considerations become part of standard business planning practices. 4. Privacy works best as a multidisciplinary function that involves legal counsel, privacy program managers, privacy engineers, IT professionals, information security experts, and champions in key business functions like product management, marketing, HR, and customer care. When privacy roles are limited to a few business groups (often legal or IT for example) people miss things that result in data breaches. Privacy programs operate best when they focus on people, processes, and technology as well as on laws, regulations, and policies. Further, privacy program stakeholders with different roles to play should teach each other about their contributions to the overall functioning of the program so that they can help each other spot issues and improve the overall ability of the privacy program to deploy its limited resources in a flexible, efficient manner. Different groups within an organization have their own unique sets of concerns around privacy. For example, product managers and developers may have to design a solution that consumes user data and produces an intended result while legal and compliance personnel

	could provide feedback on the risks associated with the privacy of the information involved so that developers could understand what kind of safeguards they need to design into the solution. It would also give stakeholders in the solution a chance to really evaluate the importance of consuming the information in the first place.
2. The greatest challenges in developing a cross-sector standards-based framework for privacy.	1. Selecting the right principles. Privacy frameworks function best when they are focused on generally accepted principles. This helps organizations design solutions that incorporate privacy safeguards from the outset. These principles should form the basis of desired privacy outcomes. The FIPPs, first developed in the 1970's, are a strong foundation for any framework, but it is likely that they need to be supplemented to deal with advances in technology. For example, the FIPP's don't adequately address topics like big data and pervasive surveillance. A NIST framework may need additional principles like ethics and accountability to enable organizations using it to understand and control personal data processing. 2. Targeting the right domains. A privacy framework needs to develop and maintain a variety of different functions to adequately identify and manage risks. Examples include having a governance model, staffing a privacy function with the right people, and targeting necessary business functions like incident response, privacy risk assessment and mitigation, etc. 3. Developing a maturity model. Different types of organizations have different risks and therefore need different safeguards. Not every privacy program domain needs the same level of maturity, and not every organization needs to have the same maturity levels as other organizations of a comparable size. Rather, even small organizations may need high levels of maturity in some cases depending on what they are doing with personal information. Any framework needs a maturity model that

	describes how a particular domain's safeguards work so that organizations can determine their privacy programs' maturity properly.
3. How organizations define and assess risk generally, and privacy risk specifically.	1. Organizations need to "start with why." Before getting into the mechanics of privacy risk assessment, privacy professionals working with organizations need to understand the business goals that application of a privacy framework is supposed to enable. On the other side of the coin, organizations should start the risk assessment process by defining for themselves why they are taking on the risk of collecting and using personal information in the first place. Mature risk assessment practices help organizations identify and close potential risks by presenting risks and benefits in context of business priorities. Organizations who use strong risk assessments may decide that some business activities do not provide the value they thought they would if it turns out that the risks are too challenging to mitigate and the rewards are not great enough to make the effort worthwhile.
4. The extent to which privacy risk is incorporated into different organizations' overarching enterprise risk management.	1. Privacy risk management can learn from other domains that identify and mitigate risks from external sources. For example, intellectual property risk management seeks to maximize enterprise-wide freedom of action by identifying external interests that may restrict organizations' ability to pursue certain business activities. In cases where these other risk management activities are more mature, organizations can help improve their privacy management practices by learning from existing risk management activities from other domains and incorporating privacy into them as another source of risk.
5. Current policies and procedures for managing privacy risk.	1. Developing policies and procedures starts with the application of a privacy management framework that is designed to identify and incorporate requirements defined by applicable laws, regulations, industry codes, organizational values, and key contracts that govern the handling of personal information.

	2. Policies document the applicable controls that give effect to various privacy program domains. They define an organization's approach to complying with the requirements of the applicable privacy management framework. Relevant policies for a mature privacy program include an enterprise-wide privacy policy that sets out organizations' commitments in the realm of privacy compliance and set out the core principles that the privacy program will attempt to meet; an HR related policy that provides necessary information on how employers will handle personal information of permanent and temporary workers; a recruiting policy that applies to job applicants; a third party risk management policy that defines requirements for any external service providers or vendors who will handle personal information on the organization's behalf; an incident response policy that documents how the organization investigates and deals with breaches of information security and that provides rules for complying with data breach reporting requirements under an inconsistent patchwork of applicable laws; and data classification and records management policies that define how business records containing personal information must be treated, retained, and destroyed; and finally, where appropriate, one or more external privacy policies that identify to individuals outside the organization like job applicants, customers, business contacts, and end users of products and services. 3. Procedures provide guidance that help stakeholders integrate privacy requirements documented by policies into covered business processes. Procedures bridge the gap between specific business practices and policies that identify enterprise requirements and expectations. For example, an HR privacy procedure document would apply the principles and requirements stated in an organization's enterprise-wide policy to key practices of the HR organization such as conducting investigations,

	benefits and compensation administration, and workplace health and safety reporting. Different business units would use tailored procedure documents to implement practices that are consistent with policies and that seek to avoid unreasonable disruption of existing ways of working.
6. How senior management communicates and oversees policies and procedures for managing privacy risk.	1. Senior management should nominate an executive sponsor for an organization's privacy program. Potential candidates for such a sponsor may include the General Counsel, Chief Privacy Officer (if the organization has one), Chief Information Officer (or similar roles), Chief Compliance Officer, Chief Risk Officer, and so on. The executive sponsor serves as an advocate for the privacy program. They ensure adequate funding and staffing and where necessary escalate issues to the senior leadership team. They also help give the privacy program access to an organization's board of directors for reporting purposes. 2. The executive sponsor reviews and approves the privacy management framework and the policies and procedures created to implement it. They also own allocation of funds to select and deploy tools designed to enable more effective execution of policy and procedure requirements. 3. Internal audit, external assessment, similar ongoing program governance resources report on their findings regarding the effective ongoing functioning and management of the privacy program to the executive sponsor. 4. Escalation of disagreements between the privacy program and other business units or third parties ultimately rolls up to the executive sponsor, who works with other executive stakeholders to find solutions. 5. Training and awareness effort run through the Executive Sponsor, who is responsible for approving such efforts when the privacy program

	wishes to do provide training content formally or not. 6. Senior management should also ensure adequate resourcing for a central repository for policies, procedures, and other privacy related resources.
7. Formal processes within organizations to address privacy risks that suddenly increase in severity.	1. Organizations should start by identifying the business processes that handle personal information. These may include but are not limited to HR, marketing, product management and development, customer care and warranty services, and IT. 2. Next, organizations should identify business functions that exercise a governance role over business practices that handle personal information. Some examples include legal, privacy office, records management, GRC, data loss prevention, and information security functions. 3. Organizations should develop privacy risk assessment processes that integrate governance functions into business processes including design of new business activities (development of products and services, etc.) and into change management activities (updating personal information inventories and maps) in order to identify when new or changed business activities lead to new or changed privacy risks. 4. Privacy risk assessments should be tailored to the needs of specific business processes. For example if an organization develops products and services using an agile software development model, a privacy risk assessment model that relies on a single privacy impact assessment for each product or service is unlikely to be as effective as a model that identifies risk at a high level at early phases of the development lifecycle and that drives ongoing engagement between product and privacy teams throughout the development process. On the other hand, a single privacy impact assessment may make more sense

	as part of vendor selection, contract negotiation, and onboarding of third parties who will handle personal information or in a traditional waterfall development model where a privacy impact assessment can occur as part of the "toll gates" that projects must pass through.
8. The minimum set of attributes desired for the Privacy Framework, as described in the Privacy Framework Development and Attributes section of this RFI, and whether any attributes should be added, removed or clarified.	A privacy management framework should contain at a minimum the following domains. 1. A governance and operating model that includes a description of the management of the privacy office. 2. Creation and ongoing maintenance of a personal information inventory. 3. Development of a risk and control matrix aligned to the domains of the privacy management framework and organizational risk tolerance and strategy. 4. Regulatory management practices including identifying and responding to regulatory change, engagement with regulators on relevant issues to the organization, responding to contact from regulators, and making required filings. 5. Information lifecycle management practices such as data minimization, information classification, records management and retention (including destruction), anonymization and pseudonymization, and transparency and control over the collection and use of personal information. 6. Privacy policies including internal master policies, public facing policies, and change management practices. 7. Processes, procedures, and technology supporting areas such as privacy by design and risk assessment as part of change management, managing international data transfers, receiving and responding to external inquiries and requests, corporate social responsibility reporting, and handling communication with

	individuals and responses to requests relating to data subject rights (traditional ARCO rights, portability, deletion, etc.). 8. Integration with organizations' information security programs in order to prevent, detect, and respond to security incidents that may involve personal information. This includes designing safeguards to protect against misuse of authorized access to personal information. 9. Third party oversight including development of contract provisions, assessment of third parties' capabilities around the protection of personal information, and ongoing assurance. 10. Training, awareness, and public relations activities. 11. Monitoring and continuous improvement of the ongoing effectiveness of the privacy program such as controls monitoring, internal assessment, and independent assurance. 12. Incident management and response. Particular areas of focus in this framework domain should include identifying whether or not a security incident is also a reportable data breach that may trigger notification requirements.
9. What an outcome-based approach to privacy would look like.	Organizations taking an outcome-based approach to privacy should be able to: 1. Understand and document all personal information that they collect / generate, where it came from, who has access to it, how it's used, and how long it's retained before destruction. 2. Clearly and in plain language articulate to individuals how they collect and use personal information. 3. Provide mechanisms for individuals to express their wishes and enforce their rights regarding the collection and use of their personal

	information and to hold the organization accountable for living up to their commitments. 4. Be able to demonstrate that personnel representing individuals' rights and expectations are key stakeholders in decision-making processes that determine whether and how to collect and use personal information and that privacy risk assessment and management are integrated components of relevant business processes and procedures. 5. Show that they have processes in place for determining whether a security incident is also a personal information breach and if so managing applicable requirements. 6. Demonstrate effective training, awareness, PR, and government relations programs and procedures to ensure that personnel understand and appreciate organizational privacy commitments and that effective channels for engaging with external actors like regulators and NGO's exist. 7. Establish internal and independent assessment and validation mechanisms to ensure the ongoing effectiveness of the privacy program in the face of changing business priorities and threat landscapes and processes for making changes to policies, procedures, and safeguards based on any findings that may arise.
10. What standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles organizations are aware of or using to identify, assess, manage, and communicate privacy risk at the management, operational, and technical levels, and whether any of them currently meet the minimum attributes described above.	1. KPMG's privacy management framework and privacy maturity model provide a method for developing an effective privacy program that is tailored to an organization's specific needs with respect to privacy risk assessment and management. 2. The framework and maturity model can also be used to assess a privacy program against a known set of principles to identify an organization's ability to produce desired privacy outcomes, identify opportunities for improvement, and

	develop new or improved safeguards to appropriately manage risk. 3. Other frameworks such as ISO 27001 can also be effective components of a privacy program where they apply. For example ISO standards for information security management systems can help demonstrate that personal information assets have appropriate levels of protection in place. Other privacy seal programs can also help demonstrate that an organization is meeting a set of defined requirements.
11. How current regulatory or regulatory reporting requirements (e.g., local, state, national, international) relate to the use of standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles.	An increasing number of jurisdictions expect organizations to implement, maintain, and continuously improve principles based privacy safeguards that are technology agnostic and designed to provide reasonable and appropriate measures. Use of frameworks and independent reporting mechanisms like ISO, SOC 2, and the KPMG privacy management framework and maturity model enable organizations to show regulators and other external interested actors the steps they take to ensure that they understand and properly manage privacy risks.
12. Any mandates to use specific standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles or conflicts between requirements and desired practices.	1. Privacy by design, and a related set of practices known as “strategic” privacy by design should be a key component of any privacy framework. These practices focus on making privacy a core consideration in the development of new business activities and the management of changes. Privacy by design principles focus on establishing default states that understand and respect individuals’ expectations on how organizations will handle their personal information and giving organizations the right tools to do so. 2. A robust privacy by design program will include a suite of privacy enhancing technologies that are tailored to each organization’s particular risk model. Examples include: (a) deployment of encryption in transit and at rest to protect personal information assets from unauthorized access; (b) use of monitoring and data analytics to detect patterns of access that may indicate

	misuse of authorized credentials; and (3) anonymization and pseudonymization of personal information where doing so will retain utility of data while reducing its sensitivity. 3. With respect to anonymization in particular, common approaches to anonymization that rely on removing names and directly identifying information but keeping demographic and other data, is insufficient. It is vulnerable to an inference attack, where an actor who already has some information about a data subject can identify that subject's record within the "anonymized" database. Generally, most Americans can be uniquely identified using only three pieces of information that are often gathered and rarely redacted: zip code, birthdate, and sex. This information is often relevant to the purpose of a database, especially in medicine, and cannot always be removed without sacrificing some of the database's utility. Therefore, the use of differential privacy techniques should be encouraged if not mandated, especially for comprehensive or sensitive data sets where de-anonymization would present a serious benefit to an unscrupulous actor or a serious risk of harm to a data subject.
13. The role(s) national/international standards and organizations that develop national/international standards play or should play in providing confidence mechanisms for privacy standards, frameworks, models, methodologies, tools, guidelines, and principles.	1. While it would be ideal if all states and two-hundred-plus nations adopted the same privacy standards, it is unlikely to happen given different local and national challenges, incentives, and cultural values. Therefore, it would be very useful to the average consumer if a common international privacy vocabulary could be developed. Such a common vocabulary would ease translation between the legal languages and concepts of different countries and states, thus simplifying a consumer's ability to determine their rights and make informed decisions about providing and using their data. It would be ideal if the NIST framework furthered this by providing a privacy terminology dictionary which it encourages lawmakers and companies to use. Additionally, the GDPR's call for easily-

	understood symbols in Article 12(7) should be supported and endorsed. 2. A privacy framework that acknowledges the contributions of standards organizations and existing risk management frameworks can help organizations find common ground among national and international rules and make it easier for them to operate amidst different jurisdictions' rules governing the processing of personal information. GDPR and similar comprehensive regulatory frameworks confer broad extraterritorial jurisdiction on their enforcement authorities. A privacy framework consistent with broadly accepted good practices and standards can help organizations avoid a chilling effect on internet commerce arising from increased compliance costs of doing business in markets with inconsistent regulations.
14. The international implications of a Privacy Framework on global business or in policymaking in other countries.	A NIST privacy framework would provide American organizations with a resource they can use to identify appropriate practices and safeguards for the handling of personal information in a global economy. A successful framework will help organizations who use it demonstrate that they have implemented sufficiently mature practices to be trusted custodians of personal information and demonstrate to outside interests that they are making good-faith efforts to manage privacy risks throughout the enterprise. Ultimately, the amount of international impact will depend upon how closely the final framework tracks to principles articulated in prominent privacy regulations such as GDPR or the principles articulated by the Federal Trade Commission. A NIST privacy framework can also help point the way to better policy. The United States' current sectoral and state-by-state approach to privacy regulation can create confusion in edge cases about what data is covered and what rights individuals have, especially in organizations that may fall under multiple sets of rules with

	different standards. For example, an insurance company may fall under GLBA, HIPAA, FCRA, the California Consumer Privacy Act, and New York Financial Services Cybersecurity Regulations. A principles and outcomes based framework that empowers organizations to implement strong policies and practices can help navigate the complexities of the legal and regulatory landscape.
15. How the Privacy Framework could be developed to advance the recruitment, hiring, development, and retention of a knowledgeable and skilled workforce necessary to perform privacy functions within organizations.	A principles and outcomes based privacy framework can improve organizations' ability to recruit, develop, and retain skilled privacy professionals by providing a common language to evaluate people against and by enabling hiring managers and privacy program leaders to define roles that are tailored to different areas of expertise. It would also aid in identifying necessary employee growth areas and further refining training and privacy awareness courses; as well as privacy certifications, which are on average heavily biased to knowledge of the applicable statutes and regulations and less towards technical topics and implementation. Although the privacy profession is, and should be, multidisciplinary, identifying technical skills or knowledge every privacy professional should know will be of deep service to the development of the profession.
STRUCTURING THE PRIVACY FRAMEWORK	
16. Please describe how your organization currently manages privacy risk. For example, do you structure your program around the information life cycle (i.e., the different stages—from collection to disposal—through which PII is processed), around principles such as the fair information practice principles (FIPPs), or by some other construct?	When advising clients, KPMG uses a proprietary privacy risk model called the Privacy Management Framework, which was originally based on GAPP but has been significantly improved and revised to accommodate new developments. This framework is divided into twelve principle-based categories (for instance, inventory/data mapping and policies), with most categories having several lower-level subcategories. The categories/subcategories are then broken down into one of five "maturity levels," which span from no action on the subcategory to full integration into the business rules and controls of a company's technology and procedures. When assessing or advising a company on a category/subcategory, we assess

	their current maturity level and the maturity level we would expect to see based upon their business and the data they're handling. This system is useful because it allows a company to identify both its current status and a roadmap for improvement.
17. Whether any aspects of the Cybersecurity Framework could be a model for this Privacy Framework, and what is the relationship between the two frameworks.	The NIST Cybersecurity Framework can form a critical component of any privacy program. Regulators around the world expect organizations who handle personal information to implement reasonable and appropriate administrative, physical, and technical safeguards designed to ensure the confidentiality, integrity, and availability of information assets. These safeguards are a crucial building block of responsible privacy management. That said, while mature information security practices are necessary to a successful privacy program, they are not sufficient by themselves. While the NIST Cybersecurity Framework is a good model for limiting access to any kind of information asset to those with a legitimate purpose for its use, a privacy framework further exists to ensure that those who have authorized access to personal information are making appropriate uses of that access.
18. Please describe your preferred organizational construct for the Privacy Framework. For example, would you like to see a Privacy Framework that is structured around: a. The information life cycle; b. Principles such as FIPPs; c. The NIST privacy engineering objectives of predictability, manageability, and disassociability or other objectives; d. Use cases or design patterns; e. A construct similar to the Cybersecurity Framework functions, categories, and subcategories; or f. Other organizing constructs? Please elaborate on the benefits or challenges of your preferred approach with respect to	A privacy management framework should focus on operational domains that provide options for addressing common privacy requirements such as maintaining an inventory of personal information processing activities, data breach response, privacy by design, and enabling individuals to exercise legal or contractual rights around the control of their personal information. This approach allows organizations to customize their privacy programs according to their own individuals risk landscape. Principles such as FIPP or GAPP can be useful to help develop outcomes that operational domains will attempt to achieve.

integration with organizational processes for managing enterprise risk and developing products or services. If you provided information about topic 10 above, please identify any supporting examples of standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles.	Privacy engineering objectives are critical tools in the successful integration of privacy by design efforts into existing business planning, development, and change management practices. For example, the KPMG privacy management framework focuses on operational aspects of a privacy program such as a governance and operating model, privacy impact assessment, data inventory, third party risk management, security for privacy, data subject rights handling, and incident response. The KPMG maturity model describes controls that manage risks on a continuum from ad hoc to optimized deployment of administrative, physical, and technical safeguards.

SPECIFIC PRIVACY PRACTICES
 	
In addition to the approaches above, NIST is interested in identifying core privacy practices that are broadly applicable across sectors and organizations. NIST is interested in information on the degree of adoption of the following practices regarding products and services:
 	
• De-identification;
• Enabling users to have a reliable understanding about how information is being collected, stored, used, and shared;
• Enabling user preferences;
• Setting default privacy configurations;
• Use of cryptographic technology to achieve privacy outcomes—for example, the disassociability privacy engineering objective;
• Data management, including:
  • Tracking permissions or other types of data tracking tools,
  • Metadata,
  • Machine readability,
  • Data correction and deletion; and
  • Usable design or requirements.
	KPMG prioritizes an understanding of data flows, especially the data life cycle and how it is used and stored. A data inventory and a completed and updated list of held personally identifiable information are vital to successfully achieving the desired outcomes NIST has identified here.
	
	An accurate inventory enables organizations to be transparent to individuals regarding the collection, storage, use, and transfer of personal information in a formal privacy policy and supplemental resources like short form notices, “nutrition label” style disclosures, and layered privacy policies.
	
	The inventory is also critical to enable people to express their preferences. A good set of transparency tools gives individuals information they need to make informed decisions. A mature master data management program that includes data classification and policy enforcement systems can enable tracking of personal preferences by tagging personal information assets with metadata that describes its permitted and prohibited uses and identifies the organizational roles that have permission to access the data in the first place.

	Additional tools such as deidentification, privacy engineering objectives, and cryptography help ensure that organizations provide the right level of access to personal information assets to the right people.
19. Whether the practices listed above are widely used by organizations.	Practices like those listed above help KPMG clients reach the desired level of maturity in their privacy safeguards. Not every organization needs to employ all of them. Organizations need to assess their personal information inventory in the context of their business strategies to determine how mature their safeguards should be for each privacy program domain. The desired maturity level will then inform the use of such practices.
20. Whether, in addition to the practices noted above, there are other practices that should be considered for inclusion in the Privacy Framework.	We would recommend an incorporation of PR, training, and awareness dimensions to privacy and the regular review of Corporate Social Responsibility. Additionally, we would recommend requirements for regular, independent validation of important privacy practices (such as right to deletion, notice and consents, anonymization, and media destruction). Lastly, as mentioned in 12, we would recommend a wider adoption of differential privacy and other privacy engineering techniques as part of robust privacy by design practices.
21. How the practices listed above or other proposed practices relate to existing international standards and best practices.	Many of the practices suggested above are useful in efforts to comply with international privacy laws like the GDPR. KPMG's privacy management framework domains map to the substantive requirements of the GDPR and enable organizations to understand the kinds of safeguards and privacy enabling practices (including those described above) that will improve their compliance efforts.
22. Which of these practices you see as being the most critical for protecting individuals' privacy.	1. Having a personal information inventory provides the foundation that the rest of the privacy program depends on. Organizations must have an accurate inventory to understand what they are doing and plan for the privacy outcomes they want to have. Master data management, identity and access management, and change management are supporting practices that help

	ensure the inventory stays up to date as business practices evolve. 2. Transparency and choice / data subject rights mechanisms based on the information gleaned from the personal information inventory and processes and systems for receiving, tracking, and implementing individuals' choices help organizations meet people's expectations around the processing of personal information. 3. Privacy risk assessment, privacy engineering, and privacy by design practices embedded into business processes that involve personal information help organizations identify and respond to potential threats early. 4. Training and awareness activities help build an informed workforce. 5. Routine independent assessments enable organizations to monitor the health of their privacy programs and continuously improve on their practices. Independent assessments help organizations avoid insider bias in the review of their practices, which could lead to the gradual erosion of privacy protections and greater regulatory exposure.
23. Whether some of these practices are inapplicable for particular sectors or environment.	Some specific tools / techniques are special purpose solutions to problems that don't always appear in every organization's risk landscape. For example differential privacy is a tool that organizations can use to improve the anonymity of deidentified data sets while maintaining data quality. Organizations that do not rely on the use of anonymized data sets would have no call to implement differential privacy techniques. Most of the other practices identified are technology agnostic and describe outcomes that can be adapted to a wide variety of sectors.
24. Which of these practices pose the most significant implementation challenge, and whether the challenges vary by technology or other factors such as size or workforce capability of the organization.	1. Keeping and maintaining accurate personal information inventories are difficult and often time-and-labor intensive to produce and maintain for large organizations.

	2. Records management / master data management are frequently challenging because many organizations do not have mature information lifecycle management practices, which results in excessive retention of information long past the end of its utility and challenges enforcing individuals' rights and choices on systems. 3. Privacy by design can look like a nebulous concept that is hard to implement properly, especially in agile shops where things move quickly and a heavy privacy impact assessment is impracticable in some cases.
25. Whether these practices are relevant for new technologies like the Internet of Things and artificial intelligence.	The outcomes, practices, and principles identified in a NIST privacy framework should be technology agnostic. These concepts can apply to emerging technologies just as easily as they can apply to more established ones. The data inventory and personally identifiable information lists are very relevant to the Internet of Things, AI, and other new technologies. The internet of things especially will make the practice of keeping a compiled list of personally identifiable information
26. How standards or guidelines are utilized by organizations in implementing these practices.	Standards and guidelines can help form a consensus among different stakeholders like consumer protection groups, privacy advocates, government agencies, and businesses around what good privacy outcomes should look like and how to measure the effectiveness of practices designed to achieve them. They can also come with independent assessment frameworks to provide additional accountability.