McAfee
Together is power.

January 14, 2019

VIA EMAIL: privacyframework@nist.gov

Attn: Katie MacFarland
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Re: McAfee's comments in response to NIST's Request for Information (RFI) on *"Developing a Privacy Framework"*, Docket No. 181101997–8997–01

McAfee LLC appreciates the opportunity to respond to the National Institute of Standards and Technology's Request for Information on "*Developing a Privacy Framework*," posted on November 14, 2018.

McAfee, a world leading independent cybersecurity company, is focused on accelerating ubiquitous protection against security risks for consumers, businesses and governments worldwide. Inspired by the power of working together, McAfee creates cybersecurity solutions that make the world a safer place. For consumers, we help secure their digital lifestyle at home and away. For businesses, McAfee cloud security extends from device to cloud with data visibility, data loss prevention and advanced threat protection on a platform that supports an open ecosystem. Our holistic, automated, open security platform allows disparate products to co-exist, communicate and share threat intelligence with each other across the digital landscape. We enable the convergence of machine automation with human intelligence so our customers can streamline workflows more efficiently, be freed from operational burdens and be empowered to strategically combat threats from adversaries.

Our response includes answers to the specific questions asked in the Request for Information, as well as general comments on aspects of the proposed Privacy Framework and areas to be considered during the Framework development process.

Before beginning our comments, we want to express how pleased we are to see NIST leveraging their abilities as a successful convener of industry and governments to solve a problem whose solution is long overdue. Thank you.

Our General Comments

Focus of the Privacy Framework

McAfee agrees with the approach and goals NIST is taking in developing the Privacy Framework. The voluntary Privacy Framework needs to focus on helping organizations properly address their privacy needs and risks through the use of privacy best practices. It should be a tool to assist organizations understand how to improve their privacy programs, while being compatible with and supporting an organization's ability to operate under the various legal or regulatory regimes. We believe this would be a significant step forward in positioning organizations to better address current and future data protection and privacy needs.

Privacy Framework Development and Attributes

As discussed at the October 16, 2018, Kickoff Workshop in Austin, McAfee is pleased to see that NIST is using a similar development process and goals to that used with the Cybersecurity Framework's (CSF) development. We are highly supportive of NIST's efforts to develop a risk-based, outcome-based, voluntary and non-prescriptive Privacy Framework, and we welcome the opportunity to add our comments to those of other stakeholders and champions.

A Strong Advocate of Consumer Privacy and Data Security

Individuals and corporations must be able to trust technology for it to be the most effective. We believe that trust in the integrity of systems – whether a corporate firewall or a child's cell phone – is essential to allowing individuals and corporations to benefit most from the power of technology. McAfee is committed to enabling the protection of customer, consumer and employee data by providing robust security solutions.

The General Data Protection Regulation (GDPR), the E.U. Network and Information Security Directive, the California Consumer Protection Act (CaCPA) and other new laws from countries around the world are making compliance with privacy, data protection and security regulations an important part of bringing products and services to market; understanding and complying with these laws and regulations is crucial to our mission as a leading cybersecurity provider. Our customers also are subject to many of these laws and demand that we be able to explain what data our products collect, how data is processed and secured and what options are available for end users to delete or correct data about themselves.

McAfee strives for transparency in its data protection processes: our privacy notice and cookie policy are posted on our website and describe our approach to protecting data privacy and ensuring security. We use a combination of policy, standards, procedures and guidelines to drive the effective management of personal data in our operational business processes and in the development of our products and services, enabling our customers, consumers and employees to better trust their digital devices.

Why Privacy and Security Matter to McAfee

At McAfee, we put the customer at the core of everything we do. Protecting our customers' data is an essential component of this value. Our products support the protection of personal data (including the data of our customers' customers and their employees) and our customers' intellectual property. Robust privacy and security solutions are fundamental to McAfee's strategic vision, products, services and technology solutions. Our data protection and security solutions enable our corporate and government customers to more efficiently and effectively comply with applicable regulatory requirements.

Privacy and Security by Design

"Privacy and Security by Design" requires companies to proactively consider privacy and security on the drawing board and throughout the development process for products and services going to market. It also means protecting data through technology design that considers privacy engineering principles. This proactive approach is the most effective and efficient way to enable data protection because the data protection strategies are integrated into the technology as the product or service is created. McAfee believes Privacy and Security by Design encourages accountability in the development of technologies, making certain that privacy and security are foundational components of the product and service development processes.

Internal Software Development

A challenge for security professionals throughout the United States is that many corporate information technology, network and infrastructure staff develop specific applications, middleware, operational tools and integration components for specific corporate needs. These development efforts are often "quick and dirty," meant to solve a specific integration problem or patch a short term "gap." The software is often meant for short-term use but often ends up in production environments, making the organization's infrastructure much more vulnerable to attack, and potentially exposing customer, consumer and employee data. It is critical that organizations also consider Privacy and Security by Design while internal tools are being developed. These types of tools are often not appropriately identified and understood and are often overlooked. Internally developed tools need to have just as many privacy and security reviews and focus as vendor-developed tools, and in many cases, more.

Processing Threat Data

Along with many of our colleagues in the cybersecurity industry, McAfee processes threat data from hundreds of millions of internet points of presence (the local access points that allow users to connect to the internet with their internet service provider) to protect customers from cybersecurity attacks and support them in meeting their privacy compliance obligations. The ability to gain operational insight into attack vectors through the appropriate and responsible use of data also enables the cybersecurity industry to continue to bring innovative solutions to market that increasingly drive the ability to detect and defeat "zero day" attacks (attacks that have zero days between the time a vulnerability is discovered and the initial attack).

Device to Cloud Concerns

As more digital devices are connected to the internet, there is an increased need for data and applications to be shared among devices and stored remotely, including in the cloud, with augmented focus on the balance of performance, power management and security. The move from device to cloud adds additional complexity to the data landscape and subsequent complexity to the threat landscape, multiplying the number of possible threat vectors. For there to be appropriate protections for this data, there will need to be an increased focus on the security of networks, the gaps between and among cloud providers, and individual endpoint devices. As more devices are connected to the internet, carefully selected device information (e.g., IP addresses) will need to be processed to provide device security. It is important that this processing of device information is recognized as a necessary mechanism for protecting privacy by better securing the data.

Specific Responses to the RFI Questions:

Below are our answers to the specific questions asked in the RFI.

Organizational Considerations

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

   A privacy program faces many challenges: attention, resources, perceived conflicts with business aims, carelessness and human error, regulatory pressures, legal mandates, a complex compliance scheme for those of us operating internationally and the complexity that comes with today's data-heavy enterprises. With each additional vendor, acquisition or product, the organization's complexity increases. It is difficult to identify a single challenge to improving privacy protection, but the increasing complexity of products, services and internal systems, coupled with the difficulty of tracking and complying with a broad range of regulatory schemes, make improving the maturity of privacy programs difficult. Privacy programs are a cost center and rely on specialist legal advice; they are but one of many competing risks a company must take into consideration and attempt to mitigate. With limited budgets, ever-changing laws and demands from all aspects of the business and internal operations, a typical privacy program may be stretched. While state-of-the art privacy is evolving, it lags behind information security as a time-tested discipline. These and other challenges make for a welcome environment for the NIST Privacy Framework.

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

Cross-jurisdictional standards are constantly changing, and priorities are different in different business sectors.

Cultural differences affect attitudes toward data sharing and privacy. There is an inherent conflict between privacy and security in that one person's surveillance or cookie tracking is another's security technology. Other challenges include a lack of standards for negligence; consumer fatigue; competitive pressures for faster deployment; an imperative to know how users use products and websites; and confidentiality expectations from users, who expect that you be able to help them but not know what they are doing.

The greatest challenge may be the perspective that those developing an applicable cross-sector privacy framework take. If the overarching perspective is to develop something to address the legal aspects of existing laws and regulations, the effort will be of short-term use and too narrow to be able to address emerging and future issues and concerns.

If Framework participants start with the attitude that the goal is to produce a framework that privacy professionals and others can use to build the proper privacy controls, processes and programs with a non-sectorial or geo-political influence, then the effort will have a better chance of creating something adaptable to the needs of organizations operating under multiple and differing legal regimes.

Focusing on the best ways to approach and protect the privacy of customer, consumer and employee data, irrespective of the current legal landscape, will allow for the proper outcome. The Cybersecurity Framework (CSF) took this approach to a minor extent and produced an outcome that is global in impact. The organizational risk management focus was why it was successful. As with the CSF, national and global standards and guidelines should be mapped to the privacy subcategories identified. This mechanism will assist by enabling the ability to incorporate sector specific privacy guidelines into the proposed Privacy Framework.

3. How organizations define and assess risk generally, and privacy risk specifically;

At McAfee, responsibility for business risks is generally held at the business unit level; legal risks, including privacy, are evaluated, defined, and recorded by, and (to the degree they can be) mitigated at the direction of the Privacy Office, an organization sitting within the Legal Department and reporting to the Chief Compliance Officer. Comprised of U.S. and European attorneys, interns and an operations manager, the Privacy Office has a Data Impact Assessment Process that is a required element of the Security Development Lifecycle for products and vendors. Other aspects of data use are also reviewed for their risks.

4. The extent to which privacy risk is incorporated into different organizations' overarching enterprise risk management;

We cannot address how other organizations may incorporate privacy risk management into their risk management programs. We can only discuss how we do so. 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. These risks are incorporated into current operating practices of various groups within the organization. In this way we ingrain privacy-related process and controls into our daily operational practices.

5. Current policies and procedures for managing privacy risk;

The McAfee Privacy Office uses traditional data protection and information security policies and procedures. Some of the policies and procedures the Privacy Office owns, and some are owned by other groups, primary amongst them the Information Security team. An external-facing Privacy Notice, an internal-facing Privacy Policy (created in preparation for Binding Corporate Rules), a Data Classification Policy and an associated procedure, Data Retention (really deletion) Policies, Incident Response, HR Data Handling, Acceptable Use, Marketing Policies, etc., handle a variety of specifics. A corporate Code of Conduct speaks generally to the expectations and values that guide the organization. Ongoing information security, privacy and data handling training and awareness and evangelism assist in alerting the workforce of what to be on the lookout for and what issues should be raised with the Information Security and Privacy teams.

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

McAfee senior management is regularly briefed by the organization's CISO and the Privacy Office. The CISO, the Chief Legal Officer, the Compliance Officer and the Privacy Office's lead attorney and other corporate leaders are in regular contact about the current risk profile, the privacy risk landscape and future state expectations. This includes our ongoing work to comply with both U.S. and foreign laws as they come into focus and force.

7. Formal processes within organizations to address privacy risks that suddenly increase in severity;

The Privacy Office strives to use existing formal processes rather than privacy-specific processes whenever possible and utilizes company-wide communication and strategic response teams for issues that require escalation and/or cross-functional assessment. Incident response procedures are in place for a variety of scenarios, as are Business Continuity and Disaster Recovery plans.

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;

McAfee agrees with the complete set of minimum attributes listed in the RFI. These were the same general set successfully used in the Cybersecurity Framework development that produced a valuable outcome. We do, however, feel that within the list of attributes there are process attributes and outcome attributes.

Development Process attributes comprise:

- Consensus-driven and developed and updated through an open, transparent process, and;
- A living document.

The resulting Framework needs to address the outcome attributes of being:

- In a common and accessible language.
- Adaptable to many different organizations, technologies, lifecycle phases, sectors, and uses.
- Risk-based, outcome-based, voluntary and non-prescriptive.
- Readily usable as part of any enterprise's broader risk management strategy and processes.
- Compatible with or may be paired with other privacy approaches.

The successful development of the outcome attributes will determine the overall success of the Privacy Framework, and as such, should be the primary focus during development. It is extremely critical that what is developed can be applied, and in a way that improves an organization's ability to implement the outcomes consistent with the organization's needs and resources.

One attribute we believe is missing is assuring that the Privacy Framework is lightweight enough to be useable by all sized organizations. It is important that it not be so costly to implement that it requires dedicated resources solely for its implementation. We believe the document should instead be directly useful to all, regardless of the size of the organization.

The document should focus on best practices and not be a structure itself. In this manner, the Privacy Framework will benefit a wider spectrum of companies.

9. What an outcome-based approach to privacy would look like;

Similar to the Cybersecurity Framework, the Privacy Framework should allow interested users to assess their organization's current privacy-related protection posture, assist with establishing a simplified/common language to be used consistently throughout the organization, help with identifying areas that need improvement and assist in tracking program improvements over time.

An outcome-based approach to privacy would recognize that data is now on a continuum and that there is a difference in the need to protect IP addresses versus electronic medical records. It would also help formulate some norms for customer service expectations It should stress accountability in all sizes of organizations that would support the punishment of the weak link and not the deepest pockets.

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;

There are several variants on Fair Information Practices, but the original OECD's Eight Fair Information Practice Principles from the "*OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*"[1] remain the most useful means by which to describe the data lifecycle and its protections. The Basic Principles of National Application remain relevant many years after their issuance.

Many privacy program tools and technologies are still new, unstable, expensive and generally not overly flexible.

Best practices include:

- Interaction with other privacy and security professionals
- An engaged, aware and well-trained workforce
- A culture of open discussion about risks and issues
- Communication and evangelization internally, with vendors and customers
- More competition in the privacy professional organization space, especially in the international context

[1] http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

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;

There are two types of regulatory reporting requirements: post-breach requirements and record-keeping requirements. The first is well-served by a Security Event and Incident Management platform and a well-equipped Security Operations Center.

12. Any mandates to use specific standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles or conflicts between requirements and desired practices;

Compliance with laws requires many standards and frameworks to be considered: Privacy and Security by Design and Default (GDPR); encryption (GLBA, PCI-DSS, state laws, and often a safe harbor provision against notice); third-party risk management (EBA guidelines, OCC guidelines, other country laws); and audit requirements (GDPR, EBA guidelines and conservative readings of the guidance from the OCC).

Conflicts abound when considering confidentiality provisions versus third-party risk management (especially in cloud computing), the regulatory investigation space and the GDPR's right to audit provisions.

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

There are two parts to this question.

First, what should those organizations do today? It would be exceedingly helpful if the European Data Protection Board would issue more guidance and offer some limits on the expectations of privacy programs. While a risk-based approach is strongly favored, the perception that anything could come under regulatory scrutiny makes it difficult to consider anything outside of the scope of a privacy program.

The second part focuses on the future needs for privacy risk management. We have not seen any serious effort to develop a foundational privacy framework that could be globally applicable. This is sadly missing. Efforts such as the Cybersecurity Framework, while developed in the U.S. initially, were targeted at improving any organization's cybersecurity program incorporating people, processes and technology needs to achieve that improvement.

It has had a positive global impact and as a side benefit has helped align thinking on cybersecurity legislation in various countries.

An appropriate Standards Development Organizations (SDO), such as NIST, would serve the global community well by having an open dialog with the global community on privacy and developing a privacy framework targeted at improving the privacy practices of organizations. A framework such as this could also have a secondary benefit of potentially aligning thinking on new and emerging privacy legislation as well.

14. **The international implications of a Privacy Framework on global business or in policymaking in other countries; and**

Business is so global that an appropriate solution must take into consideration its impacts on other legal regimes.

If there were a fundamental and consistent understanding of what appropriate privacy best practices were in relation to protecting consumer data, global business would benefit greatly. When governments and the global community of commercial providers and consumers are on the same page as to best privacy practices, it could greatly help to align regulations globally.

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.**

Increasing the conceptual framework for individuals considering a career in privacy supports the growth of the profession and likely assists in the maturation of those candidates. 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.

Structuring the Privacy Framework

NIST is interested in understanding how to structure the Privacy Framework to achieve the desired set of attributes and improve integration of privacy risk management processes with the organizational processes for developing products and services for better privacy outcomes. NIST is seeking any input

from the public regarding options for structuring the Privacy Framework, and is particularly interested in receiving comment on the following issues, if applicable:

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?**

A combination of concepts mentioned: We focus on the data lifecycle with differentiated questions for business lines. We ask for pre-launch discussions with product teams and strive for Privacy and Security by Design and Default. We utilize a series of business-line specific questionnaires to investigate and confirm that the Fair Information Practice Principles were considered in the completed product offering.

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.**

When the first RFI for the Cybersecurity Framework was posted, McAfee was a wholly owned subsidiary of the Intel Corporation. McAfee was later integrated into Intel as the business unit Intel Security. In 2017, McAfee was spun out from Intel as McAfee LLC. During all this time, McAfee has been an extremely active participant in the development of the Cybersecurity Framework, submitting responses to drafts and participating/presenting in CSF Development Workshops. After it was published, we were active in outreach to governments of multiple nations communicating the value we saw in the CSF.

Once the initial version of the CSF was released, Intel/Intel Security began trying to determine if the CSF would be useful to a company of our size. Many thought the CSF was not intended for large companies with even larger security budgets. We created a proof of concept project across Intel within two of the five corporate operational domains. The successful results were documented in the first public paper from industry describing actual use of the CSF. The paper is available at: https://supplier.intel.com/static/governance/documents/The-cybersecurity-framework-in-action-an-intel-use-case-brief.pdf.

We are a firm believer that the Cybersecurity Framework is the best model for implementing a Privacy Framework. The CSF has proven to be a highly useful and implementable model. It is risk-based, outcome focused and lightweight enough for organizations of all sizes to implement and adopt. This has been demonstrated by the widespread voluntary adoption in the U.S. by the business community and its impact globally. It is easily understood as a language for communicating cyber risk management issues across the organization, from network and security experts, to the C-Suites. The flexibility of the CSF's structure allows for the proper tailoring needed to assure it can be adjusted to meet any organizational needs. While focused initially on enterprise evaluations, we are actively seeing its use in assessing operational projects, customer required infrastructure and new externally facing services.

NIST should leverage the CSF's success and global footprint in developing the Privacy Framework. It is understood, globally recognized and has been adopted by governments and businesses. The characteristics and structural components in the CSF seem a great match for a Privacy Framework with similar attributes. NIST initially had incorporated privacy as an aspect of an earlier discussion draft of the CSF. That work was a bit ahead of its time and a bit too heavy to satisfy the attributes of being *'Adaptable to many different organizations, technologies, lifecycle phases, sectors, and uses'* as well as lightweight and cost-effective. That said, much of that work was excellent and could be used as a start towards creating a Privacy Framework.

To be clear, we are not saying we should merge the two (CSF, Privacy Framework). They could easily be two standalone documents initially, with any discussion of merging them into one document saved for a later, community decision. We believe that while security is critical for privacy, there is little reason to blur the lines, as each has a specific focus. The CSF model, however, should be used as the basis for developing the Privacy Framework.

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. In a Privacy Framework, that same structure should be used. If used, it would assist organizations and staff already familiar with the CSF in integrating the Privacy Framework into their overall all risk management activities. The structure is being utilized today, it is understood and some organizations have developed internal tools to utilize the CSF. The consistent understanding of this approach would go a long way to integrating a Privacy Framework.

Privacy will have overlapping needs for security as defined in the CSF. Wherever there is a need for security-related categories and subcategories to be specified, the existing CSF references should be used. Privacy has its own needs for a clear and concise set of Privacy Framework Functions. The Identify, Detect, Protect, Respond and Recover Functions may not be appropriate, as they are more security-focused than privacy-focused. The participants in developing the Privacy Framework should investigate whether there are more appropriate Functions that could be used as the basis of implementing specific privacy-needed concerns. It is important to create a common language for privacy, just as was done in the Cybersecurity Framework. They will probably be similar but do not need to be the same.

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 [2] 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 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.

McAfee advocates an approach that:

1. Recognizes the relative risk associated with risks of misuse of different forms of data (IP address versus contact information versus electronic health records, to give an example of a spectrum)
2. Is harm-based (as opposed to abstract, edge-case potential harm)
3. Is technology and storage indifferent and is aware of the benefits of cloud and the difficulty of true segregated storage
4. Suggests safe harbors for encryption in transit and at rest and information security controls
5. Focuses on FIPPs and information life cycle and hopefully is future-proofed.

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:

[2] NISTIR 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems* at *https://csrc.nist.gov/publications/detail/ nistir/8062/final.*

- **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.**

19. Whether the practices listed above are widely used by organizations;

Core privacy practice	**Widely used in McAfee's experience?**	**Applicable in IoT**	**Applicable in AI**
• De-identification	Yes, but not always possible. Pseudonymization to one party needs to be considered anonymization to that party.	Same response	Maybe, but same caveat
• Enabling users to have a reliable understanding about how information is being collected, stored, used, and shared	Yes, but users are not always interested in the details, and regulators frown on complicated privacy notices. This is a crucial tension in this space that must be recognized and addressed. McAfee would advocate for a standardized format for communicating this to users.	Same response	Same response
• Enabling user preferences	Yes, considered a business differentiator.	Depends on the technology.	Depends on the technology.
• Setting default privacy configurations	Yes.	Depends on the technology.	Depends on the technology.

• Use of cryptographic technology to achieve privacy outcomes—for example, the disassociability privacy engineering objective	Yes, but disassociability can be considered pseudonymization under the GDPR, which has increased the complexity of what was before a binary standard. Cryptographic technologies, most specifically encryption, can be used in many situations, but can also have significant performance implications and cannot always work in the situations in which matches are necessary.	Same response	Same response
• Data management, including:	Yes, generally. The devil is in the details.	Same response	Same response
o Tracking permissions or other types of data tracking tools,	Tracking permissions can be difficult to implement and should be handled at a browser/ad tech level.		
o Metadata			
o Machine readability			
• Data correction and deletion	Yes, but overemphasized in the service sector and unrealistically applied in some Human Resources applications (users believe they have the right to question corporate data, such as reviews and ratings, while this right is more fact-based).	May not be worthwhile in IoT.	Unclear.
• Usable design or requirements	Maybe; depends on the definitions of usable design.	Same response	Same response

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

Security is critical for the proper protection of personal data. Proper privacy protections cannot be implemented without proper security measures. The Framework should discuss a safe harbor for good security practices. This will incentivize organizations to implement it while informing governments and helping to align future regulations.

21. **How the practices listed above or other proposed practices relate to existing international standards and best practices;**

A Privacy process requires good design, reference frameworks, and technical controls, i.e., privacy engineering objectives. NIST defined those objectives as manageability, predictability, and disassociability. These three objectives are similar to the principles of data processing mandated in jurisdictions that regulate the collection and use of personal data. Manageability is the layer of control given to individuals, whose data is being collected, used and shared with others. For an exercised control to be valid, international standards require it to be the fruit of substantive knowledge about the data collection and use. In other words, individuals have the right to control the collection and processing of their data by objecting or agreeing to such practice. Such acceptance or objection are valid only if the individuals were provided, at the time of data collection, clear and specific information about the collected data elements, purpose of such collection and use and/or share with any third party, i.e., predictability. The individual's consent is necessary and required in many countries. To ensure individuals' right to privacy is protected, several international regulations and laws require Privacy and Security by Design, such as the GDPR (applicable to the European Economic Area) and the Personal Information Protection and Electronic Documents Act (Canada).

Furthermore, disassociability is the privacy engineering layer where cryptography can be applied to offer real privacy-preserving functionalities. It is about identity, identifiers and identifier linkage, a design and protection challenge. Disassociability is also the layer where techniques such as anonymity, de-identification, unlinkability, unobservability and pseudonymization are of importance. The use of cryptography plays a role in managing risks associated with breach of personal data. For instance, under the GDPR, in the event of a personal data breach, if the personal data was anonymized, the hidden burden of data breach costs associated with notifying data subjects will not be an issue, simply because the high risk to individuals' rights and freedoms becomes low risk, and consequently, notifying data subjects would no longer be required. Anonymization techniques include scrambling, encryption, masking, tokenization and data blurring.

With organizations providing goods or services to residents of the EEA, those core privacy standards are to be implemented and maintained to ensure the privacy compliance of such organizations and those acting on their behalf (subprocessors).

22. **Which of these practices you see as being the most critical for protecting individuals' privacy;**

Cryptography is one of the most critical practices for protecting individuals' privacy rights. Competent privacy engineers must be up-to-date with state-of-the-art research, technology and trends, as many cryptographic techniques are in the research phase.

23. **Whether some of these practices are inapplicable for particular sectors or environments;**

An effective risk-based privacy and security framework should apply to all collections of personal data. This does not mean that all framework solutions are equal. The risks of collection and processing the personal data must be weighed against the benefits of using the data. Transparency, choice and reasonable notice should always be a part of the risk framework solution set. The specific solutions will vary based on the risk and specific types of data. The key is a proactive evaluation (Privacy and Security by Design principles) to provide the most effective protection for the specific application and data use.

As a security company, McAfee encourages NIST to consider data collections for certain harm-prevention as special cases. In poorly drafted language, for example, cookie setting and device tracking for advertising and for security services can appear the same.

24. Which of these practices pose the most significant implementation challenge, and whether the challenges vary by technology or other factors such as size or workforce capability of the organization;

The most significant challenges come from the complexity of the data protection regulatory landscape and the ever-increasing complexity of systems and products, not from any one type of practice.

One of the significant challenges is to provide the user/consumer reasonable control over personal data given the numerous ways the data can be collected and shared. Control includes the ability to know when data is being collected, what data and where it is stored. Traditional privacy notices are ineffective because most consumers don't read them (too long and too much legalese). A significant challenge is to develop and implement more effective and efficient ways to proactively notify consumers regarding the collection and use of personal data.

The solutions need to be tailored to the technology, type of personal data and context in which it is collected. The challenge is to proactively evaluate risk and develop solutions that are best for the specific challenge (technology, data type and context). The solutions might include simplified notices (easier to read and understand), simple in-context notices (e.g., "clicking below will share personal data with ABC per the terms of our privacy policy") and using organizational accountability to help protect user personal data.

25. Whether these practices are relevant for new technologies like the Internet of Things and artificial intelligence; and

FIPPs and the Data Lifecycle remain relevant for all new technologies. For thoughts on the above practices, please see column in the above chart.

An effective, risk-based privacy and security framework should apply to all collections of personal data. The use of massive amounts of data to solve complex problems may have many societal benefits. Newer technologies such as IoT, cloud computing, big data analysis and artificial intelligence are all driven by the collection, use and analysis of large quantities of data. Some of the data will be personal data. The challenge is how best to implement reasonable privacy and data security frameworks for these data-hungry technologies.

Some of the challenges: the existence of IoT sensors may not be obvious and may not provide an easy way to provide traditional notice, as these devices may not have a user-facing screen; big data (and AI analysis) may process personal data from numerous sources. A risk-based privacy and data security framework should be used to drive a proactive analysis to manage the privacy and security risks. Where traditional privacy solutions are impractical (e.g., IoT sensors where there is no simple way to provide traditional notice), safeguards must be driven by organizational accountability to provide reasonable protections for personal data.

26. How standards or guidelines are utilized by organizations in implementing these practices.

The FIPPs and the Data Lifecycle are underlying principles for our Privacy and Data Protection Program. While standards and guidelines are useful in implementing our policies and procedures, ultimately it is the application of legal and regulatory requirements. We view the standards and guidelines as organizing principles rather than a basement or ceiling to compliance.

The privacy and data security practices should be well-documented in the organization and include analysis guidance for risk-based privacy and data security frameworks. There are several layers that should be included. Internal policies should clearly articulate what is permissible and impermissible in the organization. Specific departments should specify further granularity regarding policy requirements and best practices (e.g., HR, IT, legal and marketing will have different requirements and restrictions for the collection, use and protection of personal data). Privacy (legal and non-legal) and security professionals in the organization must have detailed documentation and process tools that streamline the implementation of the risk-based framework.

There should be ongoing organizational training regarding the importance of protecting personal data and best practices. The policy requirements should be tied to the organization's code of conduct and enforced as required when polices are violated. Finally, easy to understand external privacy and data security policies must be used to educate the user/consumer and to drive toward informed consent to collection and share data wherever possible.

McAfee Recommendations

McAfee believes clear privacy and security expectations are necessary prerequisites for companies to comply with the diversity of existing laws, grow businesses and improve efficiencies, and also for consumers to trust the organization and its technology.

An effective privacy framework should:

- Use a technology-neutral approach for effective, risk-based and flexible privacy and data security strategies to protect personal information that encourages accountability, innovation and efficiencies.
- Promote proactive Privacy and Security by Design to provide the most effective end-to-end privacy and security technology solutions.
- Require an integrated approach to privacy and data security, recognizing that there is a balance between the need to collect data to secure infrastructure and the need to provide for the privacy of the individual.
- Promote interoperability and data sharing as a means to enable effective threat analysis.
- Provide for processing of device information (e.g., IP addresses and other device fingerprints) that is necessary to connect to the internet and provide reasonable security for personal data.
- Use a flexible framework similar to the NIST Cybersecurity Framework, which provides guidance on how to develop and implement realistic operational models to meet organizational objectives.
- Address best practices in privacy while being compatible with and supporting an organization's ability to operate under various domestic and international legal or regulatory regimes. The privacy framework should not be focused on the specific legal aspects of privacy, but rather on what organizations need to consider in developing and continually improving their own privacy programs in support of regulations and customer promises.
- Include minimum procedural standards for breach notification (e.g., definition of a breach, clear standards for who should be notified and possible options as to how, etc.).
- Discuss safe harbor for encrypted data and other well-defined cybersecurity protections while encouraging good corporate behavior and approaches to privacy.
- Include proper informative references to the individual subcategories listed to assure the ability to investigate controls more completely.
- Lastly, we encourage that all elements of the Framework strive to have a direct impact on the protection of data.

We believe a Privacy Framework should focus on developing the means for assisting an organization create a tool for standing up, improving, evaluating and adapting to the changing privacy landscape.

Summary

Effective consumer privacy policies and regulations are critical to the continued growth of the U.S. economy, the internet and the many innovative and life-improving technologies that rely on consumer personal data. The development of a comprehensive Privacy Framework is an important step toward increasing consumer privacy and trust and will assist in aligning thought and potentially legislation globally.

The Privacy Framework must also include robust and clear data protection and cybersecurity frameworks to truly enable effective consumer privacy protection. The creation of a Privacy Framework should not weaken robust privacy protections currently provided by strong and effective state privacy laws that have achieved broad-based consensus among a wide array of stakeholders.

NIST has an important role to play in the efforts to improve privacy. McAfee would like to sincerely thank NIST for the opportunity to provide information on this issue, and we look forward to continued engagement on this and other topics.