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

30 January 2019

Re: Developing a Privacy Framework (Docket No. 181101997-8997-01)

Dear Ms. MacFarland,

The IEEE Standards Association (IEEE-SA) commends NIST in its effort to develop a Privacy Framework to serve as a voluntary tool for organizations to better identify, assess, manage, and communicate about privacy risks so that individuals can enjoy the benefits of innovative technologies with greater confidence and trust. As a globally recognized standards developing organization (SDO) grounded in an open, inclusive, transparent, and consensus-building process, we appreciate NIST's Request for Information (RFI) process to gain information regarding organizational considerations for privacy risk management, the structure of the Privacy Framework, and the specific privacy practices to be included. We are pleased to provide general observations and feedback on specific questions NIST has posed.

About the IEEE-SA
The IEEE-SA, a globally recognized standards-setting body within IEEE, develops consensus standards through an open process that engages industry and brings together a broad stakeholder community[1]. IEEE standards set specifications and best practices based on current scientific and technological knowledge. IEEE-SA has a portfolio of over 1,250 active standards and over 650 standards under development.

About IEEE
IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity. IEEE and its members inspire a global community to innovate for a better tomorrow through its highly-cited publications, conferences, technology standards, and professional and educational activities. IEEE is the trusted "voice" for engineering, computing, and technology information around the globe.

Organizational Considerations
Looking at improving organizations' privacy protections from a broad perspective, 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. Challenges in developing a cross-sector standards-based

[1] http://globalpolicy.ieee.org/wp-content/uploads/2016/05/16011.pdf

framework for privacy include: (lack of) commonality of privacy problem sets across vertical areas; accepted practices for privacy treatments in product sets in various markets; and addressing the variance in regulatory guides as it relates to privacy for different industry sectors.

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. Of course, basic organizational policies and procedures, depending upon the size of the organization, should be in place. These may include such components as data contracts, contribution licenses, PCIC and GDPR oriented processes, as well as employee education on associated processes.

How senior management communicates and oversees policies and procedures for managing privacy risk depends on the organizational structure, size of the organization, and the role that privacy plays in the organization's offerings. Businesses with footprints and structures large enough to require a form of communication and policy and procedures may leverage established best practices, may utilize the existing NIST Risk Framework or an alternate Risk/ERM Framework, or may utilize an internally designed framework altogether. From communications approach, Senior Leadership may opt to share directly with the business unit leads for business planning purposes and establish a closed feedback mechanism reflected in plan reviews. They may opt to share with the full staff around specific risks regarding privacy such as list usage guidelines and storage procedures or they may also share such information with customers, vendors, and partners as a means to demonstrate a level of organizational integrity and quality that stands above other players in the marketplace.

An outcome-based approach to privacy should result in increased trust, and reduced opportunities for discrimination and economic loss. In order to achieve this, the approach would ideally offer a practical methodology as well as conceivably a supporting toolkit and toolset, which should include global standards, to aid in organizational and market-based calibrations associated with identified privacy risk sets. Depending on level of effort expected, offering a registry of compliant or certified organizations that meet the "CMM" levels would be beneficial. Aligned with this may be audit components that demonstrate the validity of both of framework to cross-markets as well as to vertical applications, offering regulators a clearer view toward the value of such outcome-based approaches, and encouraging policy development and providing markets a value proposition opportunity across geographic borders.

Relative to standards and how 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, standardization can reduce cost and administrative burdens on governments and they can provide an alternative to technical regulations and reduce the need for government to develop regulations. Further, standardization facilitates the ability to stay on pace with current technology. When a regulation is needed, by referring to the most recent standard(s), a regulation can be as current as the state-of-the-art standard in that field. Standardization supports

technical excellence and encourages innovation. Because technology is an enabler for global interconnection and interdependence, mechanisms for unifying technology are foundational to increased growth and trade. By enabling global interoperability, standardization also provides building blocks for innovation, helps facilitate economies of scale, and lowers the risk of vendor lock-in.

When considering mandates to use such instruments, we suggest that the framework encourage the globally inclusive, market-driven standards approach so that the benefits of technical excellence and global interoperability are available to all. When considering the role of national/international standards and organizations that develop national/international standards in providing confidence mechanisms for privacy standards, frameworks, models, methodologies, tools, guidelines, and principles, it is important that standardization paradigms are open and consensus-driven, and retain the flexibility to respond to the pace of innovation and the breadth of applications, as embodied in a globally inclusive, market-driven standards approach, such as that of of IEEE, which has demonstrated the necessary agility to meet modern society's needs. Open, market-driven standards offer an opportunity to demonstrate viability and value of a framework. Such platforms where confidence mechanisms, models, methodologies, tools, guidelines, and principles are developed and utilized offer a base to leverage the privacy output.

In addressing **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,** education programs should be considered. Such programs can be a means to train technologists and those impacted in the privacy implications of collection, use, and disclosure of personal information, and about business, legal, and policy issues that will influence technical development and deployment of data-rich products and services. Inclusion of courses in ethics, design, data protection law, and public policy in engineering education can help engineers in real-world environments where technical requirements are complemented or constrained by ethical, legal and policy factors. Information about privacy-related standards should be considered as part of the Privacy Engineering education, as well as broader educational programs in engineering, technology, and computing. Overall, the Privacy Framework can serve as an element of a collective approach to increase the application of privacy-oriented methods reflected in market-oriented solutions and offerings.

Specific Privacy Practices

Global standards can play a role in supporting privacy policies. To help illustrate this, examples of IEEE standards that address core privacy practices with global implications are noted below.

- IEEE P2801, Recommended Practice for the Quality Management of Datasets for Medical Artificial Intelligence, that identifies best practices for establishing a quality management system for datasets used for artificial intelligence medical device. The recommended practice covers a list of critical factors that impact the quality and privacy protection of datasets, such as but not limited to data sources, quality, annotation, collection, transfer, utilization, storage, maintenance, and update. Recommendations also cover personnel qualification/training/evaluation, tools, equipment, environment, process control, and documentation.

- IEEE P802E, Recommended Practice for Privacy Considerations for IEEE 802 Technologies, specifies a privacy threat model for IEEE 802 technologies and provides recommendations on how to protect against privacy threats. By describing more precisely the threats posed by these pervasive attacks, and based on those threats, the internet technical community can lay out the problems that need to be solved in order to secure the Internet in the face of those threats.

- IEEE 11073, Personal Health Device (PHD) standards, where security for IEEE 11073™ PHD interfaces, including authentication, authorization, integrity, confidentiality, privacy, availability, accessibility, and traceability/audit trail are included. Privacy risk mitigation in the standard prevents the content of messages from being read by other than the intended recipients, assures that individuals' health information is properly protected while allowing the flow of health information (per HIPAA), and prevents undesired system use so that access is provided to the parties to which the information belongs and to parties that have explicitly been allowed access to certain information.

- IEEE P2418.6, Standard for the Framework of Distributed Ledger Technology (DLT) Use in Healthcare and the Life and Social Sciences, provides a common framework for distributed ledger technology (DLT) usage, implementation, and interaction in healthcare and the life and social sciences, addressing scalability, security, and privacy challenges.

Regarding the question **if there are other practices that should be considered for inclusion in the Privacy Framework**, we posit that the practice of Privacy Engineering should be considered. Per the IEEE Policy Position Statement in Support of Privacy Engineering,[2] Privacy Engineering is the use of engineering knowledge and techniques to systematically address risks associated with planned and authorized functioning of systems that collect, use, and disclose personal information. The emerging discipline of Privacy Engineering is a systematic approach that supports technologists in their efforts to ensure personal data is only used with full consideration of ethical and legal requirements and cultural norms. Other practices to consider include confidential communication, enabling users to request how they wish to be communicated with; having agency over the amount of their information that can be shared with other parties; and having the ability to request and obtain a record of those parties to which their information has been shared.

Regarding **how the practices we listed or there are other proposed practices relate to existing international standards and best practices,** we note that what we have provided aligns with international standards and best practices, as well as other regulatory frameworks such as GDPR. 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

[2] http://globalpolicy.ieee.org/wp-content/uploads/2018/11/IEEE18021.pdf

- IEEE P7005, Standard for Transparent Employer Data Governance

In considering **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 solutions of higher technical complexity may be more challenging for smaller organizations with fewer specialized resources, but having open standards addressing the relevant practices may simplify that. IEEE has standards and pre-standards activities in a number of privacy-related areas.

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.

IEEE P7012, Standard for Machine Readable Personal Privacy Terms, provides individuals with means to proffer their own terms respecting personal privacy, in ways that can be read, acknowledged, and agreed to by machines operated by others in the networked world. Telecom practice (5G, NG and others) will refer to the privacy practice standards mentioned above to ensure that the communication is secure, safe, and reliant.

These considerations are also addressed in the IEEE Blockchain family of standards, noted below

- IEEE P2418.1, Standard for the Framework of Blockchain Use in Internet of Things (IoT)
- IEEE P2418.2, Standard Data Format for Blockchain Systems
- IEEE P2418.3, Standard for the Framework of Distributed Ledger Technology (DLT) Use in Agriculture
- IEEE P2418.4, Standard for the Framework of Distributed Ledger Technology (DLT) Use in Connected and Autonomous Vehicles (CAVs)
- IEEE P2418.5, Standard for Blockchain in Energy
- IEEE P2418.6, Standard for the Framework of Distributed Ledger Technology (DLT) Use in Healthcare and the Life and Social Sciences
- IEEE P2418.7, Standard for the Use of Blockchain in Supply Chain Finance

Standards can serve as key components for any organization to maintain adherence to such privacy policies. Standards provide an operational framework where the design, creation, and implementation of privacy tools follow and meet user requirements. Standards around a comprehensive approach to address a privacy framework help minimize privacy non-compliance issues, while putting data ownership in the hands of the data subject. IEEE-SA recognizes that data privacy and governance is of paramount importance to our community and has initiated/supported the development of several standards projects in this area, such as:

- IEEE P802E, Recommended Practice for Privacy Considerations for IEEE 802 Technologies
- IEEE P1912, Standard for Privacy and Security Architecture for Consumer Wireless Devices
- IEEE P2025.2, Standard for Consumer Drones: Privacy and Security

- IEEE P2418.1, Standard for the Framework of Blockchain Use in Internet of Things (IoT)
- IEEE P7002, Data Privacy Process
- IEEE P7004, Standard for Child and Student Data Governance
- IEEE P7005, Standard for Transparent Employer Data Governance
- IEEE P7006, Standard for Personal Data AI Agent
- IEEE P7012, Standard for Machine Readable Personal Privacy Terms.

The IEEE Standards Association appreciates NIST's comprehensive questions. We look forward to continuing to engage with NIST as it develops the Privacy Framework.

Thank you,

Konstantinos Karachalios
Managing Director, IEEE Standards Association

Karen McCabe
Senior Director, Public Affairs and Marketing