IEEE Project 1912, Response to

National Institute for Science and Technology Request for Comments Regarding
"Developing a Privacy Framework"
January 2019

Katie MacFarland
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899
privacyframework@nist.gov

RE: Request for Information on Developing a Privacy Framework
Docket No.: 181101997-8997-01

Dear Ms. MacFarland,

We submit the following comment on behalf of The Working Group for IEEE Project 1912, the Standard for Privacy and Security Architecture for Consumer Wireless Devices.[1]

Developing a Privacy Framework

IEEE (Institute of Electrical and Electronics Engineers) Project 1912, Standard for Privacy and Security Architecture for Consumer Wireless Devices' are submitting these comments to the National Institute of Standards and Technology (NIST) in response to its November 14, 2018, Federal Register Notice requesting input on Developing a Privacy Framework.

We are in support of the NIST's efforts to develop a privacy framework that can be used to improve organizations' management of privacy risk for individuals arising from the collection, storage, use, and sharing of their information. Application of the NIST Privacy Framework as An Enterprise Risk Management Tool ("Privacy Framework"), is intended for voluntary use and is envisioned to consist of outcomes and approaches that align policy, business, technological, and legal approaches to improve organizations' management of processes for incorporating privacy protections into products and services.

Why this is the time to develop a privacy framework?

The network computing communication environment evolved from rivers and streams of information formed by two-way data flows over coaxial cable or twisted pair connections among networked devices. Later, these rivers and streams formed ponds, pools or lakes created by wireless area networks. Today, we are on the verge of creating vast oceans of digital data-rich environments that serves a home, office complex, industrial park, city blocks, towns, cities or nations depending on the resources allocated and the innovations that enable the Internet of Things (IoT) and Artificial Intelligence (AI).

[1] https://standards.ieee.org/project/1912.html

We offer the following comments to further the work as described by the November 14, 2018, NIST Federal Register Notice.

Contributors:

- *Lillie Coney, Chief Innovator Bruce Corporation and Chair, IEEE Project 1912, a Standard for Privacy and Security Architecture for Consumer Wireless Devices*
- *Jennifer Dukarski, Shareholder, Butzel Long*
- *Claudia Rast, IP, Cybersecurity, and Technology Practice Group Chair, Butzel Long and Member of the American Bar Association's Presidential Cybersecurity Legal Task Force*
- *João Paulo Barraca, Assistant Professor at University of Aveiro, Portugal*
- *Vitor Cunha, Researcher at Telecommunications Institute, Portugal*

Our thanks to the National Institute of Standards and Technology (NIST) for its efforts to develop a privacy framework that can be used to improve organizations' management of privacy risk for individuals arising from the collection, storage, use, and sharing of their information.

The Working Group for IEEE Project 1912 is working toward a Standard for Privacy and Security Architecture for Consumer Wireless Devices and appreciates this opportunity to comment on "Developing a Privacy Framework" to help to identify, understand, refine, and guide the development of the Privacy Framework. We strongly support the objective of the Privacy Framework to be a consensus-driven, open, and collaborative process that will include many opportunities for engagement and collaboration with stakeholders.

IEEE Project 1912 Background

IEEE Communication Society approved Par 1912 on December 12, 2015, to become a Project. Project 1912 is affiliated with IEEE Committees: COM/EdgeCloud-SC - Edge, Fog, Cloud Communications with IoT and Big Data Standards Committee. IEEE's Consumer Electronics Society and the Standards Committee jointly sponsor Project 1912. The Consumer Electronics Society serves as the premier technical association in the Consumer Electronics Industry striving to advance the theory and practice of electronic engineering in the areas of multimedia entertainment, digital audio/visual systems, smart home products and IoT devices, electronic games, smartphones, and more. We commend the dedicated hard work of the technical, legal, policy, academic, and research professionals for their commitment to make this standard a reality.

What is IEEE Project 1912?

IEEE Project 1912 is a standards development initiative working to develop a standard for Privacy and Security Architecture for Consumer Wireless Devices by use of a common communication architecture for diverse wireless communication devices such as, but not limited to, devices equipped with near field communication (NFC), home area network (HAN), wireless area network (WAN) and wireless personal area network (WPAN) technologies, or radio frequency identification technology (RFID), and the proximity considerations attendant to these *areas. The standard developed may specify approaches for an end user security through device discovery/recognition, simplification of user authentication, tracking items/people under user control/responsibility, and supports alerting, while supporting privacy through user-controlled sharing of information independent of the underlying wireless networking technology used by the devices.*

Project 1912 Comment Synopsis

The stakes are high for those organizations that understand the importance of both privacy and security at the dawn of what may be the most significant technologically innovative period in human history. It is highly likely that it will not be one significant advancement but many that centered around computing and real-time communication among people, places and things.

Privacy is the most recent of the recognized human rights, first articulated in an 1890 Harvard Law Review article, The Right to Privacy, written by Samuel D. Warren; Louis D. Brandeis. As technology advanced, the authors noted that "[i]nstantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life, and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'" 4 HARV. L. REV. 193, 195 (1890). The United States passed the Privacy Act, the world's first federal privacy law in 1974, which governed the collection, maintenance, use, and dissemination of personally identifiable information, but only in records maintained by federal agencies. Since that time, the regulatory and legal frameworks outside of the United States—most notably in the European Union—have an advanced policy in this area.

Today, opportunities for innovation are present in the proliferation of wireless devices that consumers use to better manage personal devices, user content, or wireless technology. Consumer adoption of portable technology supports customization on an individual level making personal devices more valuable to users. This enhanced value is inherent in the personal data regarding consumers and preferences related to programming or use of wireless devices. To sustain the value of portable devices, better and more easily adaptable methods of securing digital devices is essential. Establishing a common architecture providing privacy and security options to consumers can assist users in seamlessly integrating these technologies into their lives. The IEEE Project 1912 architecture is intended to address safety issues in the interior or immediate exterior of private homes and commercial spaces. This IEEE standards development process provides an opportunity to voluntarily achieve greater consumer and user control over physical devices and technologies that fit the unique needs of individual users. The Project 1912 standard works to extend greater control to owners or legitimate users through a shared architecture, while supporting innovation and broad adoption of consumer communication devices and technologies.

Accompanying the rise in wireless technology is a shifting of roles from human-driven activity to automation of decision-making that supports AI. The assumption of automation for human decision-making has risks especially when the result embeds within machines the ability to self-edit, self-correct, and self-manage.

The work that NIST seeks to undertake is necessary and, if successful, would offer for the first time a measure by which an organization, no matter what its purpose, composition, or size, can objectively determine its actual privacy posture.

Organizational Considerations

1. The most significant challenges in improving organizations' privacy protections for individuals;

The greatest challenge in improving organizations' privacy protection for individuals is organizational behavior, corporate culture, and the organization's business model including the drive for the monetization of data.

A. Organizational Behavior and Corporate Culture

An organization behaves in manners that are often inconsistent with promoting privacy as a value. For example, technology professionals are often perceived as individuals who approach all problems through the lens of up time and configurations rather than assuring that restraints are in place on the transfer of data or the identification of data as private. Marketing functions often push the realm with the notion of profit and customer engagement as a primary mission rather than the security of the individual's data that may be accessible. In this traditional structure, change happens with a shared belief that an opportunity exists for a product, service, or innovation that is not currently met, and that meeting that need would be profitable, not just financially, but in other ways that may include political, social, or cultural benefits. These benefits may not necessarily include privacy considerations. This behavior thus often limits an organization's sense of responsibility for privacy, leading to lower awareness of privacy risks and ill-mapped organizational policies and practices.

B. Monetization

The use of data and analytics to generate revenue growth has increased exponentially over recent years. In late 2018, Business Wire projected in its Global Data Monetization report that the global market had a value of $1.17 billion (USD) and that it is estimated to grow to $3.07 billion (USD) by 2023.

This drive to monetize the personal data of individuals or metadata from devices tightly coupled to a single individual often implicates privacy considerations regarding notice and consent. Additional related issues include: tiered access policies regarding data use, sharing or repurposing individual data, sharing data that has higher levels of protection for organization members.

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

The greatest challenge in developing a cross-sector standard-based framework for privacy in the United States is the political will to do it. The European Union General Data Protection

Regulation (GDPR) became effective on May 25, 2018, yet there were objections, policy debates, and in-depth discussions spanning the prior five years. With the multi-year advanced notice of its effective date, the GDPR readily shaped the business processes of data processors, with fines already being issued. A vital aspect of the GDPR is that the regulation is not specific to a sector, but applies its regulatory framework to all personal data according to its relevance to its association with individuals. This objective effectively allowed the creation of legislation that is cross-sector, and not automatically deprecated by new technologies.

A similar national data protection legislative process has not been undertaken in the United States and has not resulted in such a broad set of privacy protections in a single law. The trigger for such a U.S. Federal privacy law would be a significant event that would push other policy considerations or concerns aside. September 11, 2001, was a trigger event that shifted the nation to a commercial aviation security focus that forever changed commercial aviation travel. Before September 11, 2001, preventing the family from meeting commercial flights at arrival gates, removing all shoes to get through security, or requiring gender, birth date, and names for all travelers would not have been possible. Here in the United States, it is clear that significant events, including the unconsented tracking by Vizio of over 100 billion data points collected daily on millions of television or the Facebook–Cambridge Analytica data collection of millions of Facebook profiles collected and used for political purposes without consent, have been insufficient to initiate action.

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

How an organization defines and assesses risk generally, and privacy risks specifically, is determined by the regulations and laws relating to the security of individual data and the burden placed on organizations to meet certain expectations for that data security. To a high degree, the organizational behavior of specific industries can influence the development of laws, regulations, and business practices of privacy risks. The danger arises, however, when there is no transparency involved with the influence of these specific industries as they drive privacy practices. Greater transparency regarding the scope of organization practices related to personal data collection, retention, use, reuse, and sharing is critical; these practices must be better understood and routinely disclosed. Transparency can provide policymakers, stakeholders and the public with sufficient understanding and background to make data privacy practices uniform.

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

Therein lies the unknown—we are well aware of organizations that must meet obligations regarding privacy statutes and regulations with well-established experience and known regulatory frameworks. This is the case for public utilities, banking institutions, healthcare providers, and other areas addressed by federal sectorial privacy laws. Organizations new to the establishment and management of privacy legal and regulatory obligations must navigate in the gaps of the existing patchwork of laws while accommodating consumer expectations regarding privacy.

The reality is that the bulk on data collected on data subjects is unregulated. The lack of regulations or laws for new forms of data collection creates a vacuum in legal guidance for processes to establish and maintain privacy obligations.

The gap between heavily regulated data managers and those who have little to no regulatory obligations means that we do not have a clear understanding of the data practices of non-regulated industries or entities. The more considerable risk is the lack of transparency on data practices of unregulated data managers and controllers increases the potential for obscuring of data management practices so that they may never be fully understood.

5. Current policies and procedures for managing privacy risk;

The proliferation of IoT devices, supported by cloud environments with complex stacks and jurisdictions, dramatically increases the complexity of organizations engaged in data management. In this context, organizations must be aware of the privacy risks associated with the technology stack in use at the company when they provide their services or products. The data stored at the devices, processed by the software and exchanged in communication channels, as well as the metadata for said actions in a current organization, rapidly increase the complexity of managing the privacy risk. The adoption of mechanisms that limit data collection and enforce the notion of data lifecycle and data aging are vital for a future privacy framework. The ubiquitous nature of IoT devices supports a mandate requiring organizations to adopt policies focusing on a clear identification of the data gathered by organizations, its domain, and the associated lifecycle, which includes its eventual deletion.

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

When developing a Privacy Framework, it is clear that many use cases demonstrate the need to contemplate international implications. Whether it is wearable health technology, connected automotive technology, or interactive and connected children's toys, it is inevitable that these devices will be marketed and sold across multiple international platforms. In addition, given the territorial reach and pre-existence of other jurisdictional privacy standards, such as the EU's GDPR, the UK's Data Protection Act 2018, and similar data protection laws and regulations throughout the world, careful attention must be made with an ultimate goal of harmonization, not conflict. It is clear that a U.S. Privacy Framework would best operate if it were consistent with the principles currently established in multiple foreign jurisdictions.

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.

Legislation and regulation supporting fair information practice principles (FIPPs) would likely reshape many organizational processes and solutions, as well as organizational cultures. In the fields of software and hardware design, these simple principles, applied in a cross-sector manner, bring the need for hiring a skilled workforce. Under that regime, requirements for products and services related to privacy will be increased, resulting in the need for additionally *skilled privacy practitioners across management and across industries. Maintaining stability and adherence to a set of privacy norms and codes of conduct—from the lowest level employee to the most senior executive—helps to perpetuate the value proposition of an organization's privacy ethos.*

Structuring the Privacy Framework

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:

c. The NIST privacy engineering objectives of predictability, manageability, and dissociability or other objectives;

Predictability and manageability are critical objectives for a privacy framework. Special care should be given to dissociability in communicating and software systems, as the number of identifiers and locators used across layers, produce metadata that creates privacy risks for individuals. As the technology curve moves the world closer to quantum computing and sustainable AI, the types and range of emerging wireless technology architectures will establish greater complexity. This complexity will consist of communication within environments that devolve from the focus on the individual to a mix of communication uses for a range of functions that may lend themselves to associating an individual with metadata and functionality far beyond what is understood today.

d. Use cases or design patterns;

Use cases will continue to be relevant to the development of a Privacy Framework. As an example, use cases have been significant to the development of the Project 1912 Standard. At this time, no privacy standards that can follow every aspect of work associated with data management exists. It has been essential in the drafting of standards for Project 1912 that use cases are used in those instances when a control's description may not adequately convey the objective of the control. Storytelling is the oldest form of collective instruction or information sharing, and use-cases may serve the goals of introducing the concept of a privacy standard based upon desired outcomes for the data subject while allowing engineers the freedom to pursue compliance with standards using the full scope of their training and knowledge.

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:

The Project 1912 Working group worked for two years to outline areas that will be addressed in its standard. We observed that innovations in data management occurred while others became outmoded. It is essential to keep in mind that AI, IoT, quantum computing and Cloud services will make possible applications and use cases that are unheard of today. The idea that people will be engaged and prepared to respond to all requests for data or its use may be too ambitious.

Today, a phone entering an area may automatically see every server, public and private, accompanied by an invitation to join one of the networks. This all occurs without requesting this information. The design of the network software automatically sends out the requests, and the design of the firmware on phones automatically presents the options and blocks use of the device until the request is dismissed or accepted. A privacy-centric approach would allow the phone user to connect with any communication environment. It made sense, during the early days of mobile phone technology, to make free wireless network connectivity available to users given how few networks existed and the cost of data plans required for sending text, email, or reading online content. Today, in contrast, it is more of an annoyance to prospective consumers when service is not required. This invasiveness is just one example of specific privacy practices assessed under IEEE's Par 1912.

Tracking permissions or other types of data tracking tools,

The applications that fuel commercialization of just-in-time service provision also creates greater transparency in the lives of technology users. Application developers create targeted services and apps that are often minimally priced or are free of cost, in exchange for access to user data. Applications requests access to address books, location data, or other user tracking activity. The transactional relationship between users and App Developers should be transitory, but in some instances use is conditioned upon mandatory access to location data at all times and not just when the App is being used. These practices are transparent, but only to the degree that they may be discovered through examination of the App's location service. This may be buried deep within the App or within the user's mobile device. Moreover, it may be unclear as to the extent to which tracking may occur. A process for establishing reasonable requests for collection of data, limitations on tracking of users, and creation of norms that govern the conduct of Apps is essential to holding any system accountable to an agreed upon set of privacy norms.

Metadata,

In many cases, metadata allows the disclosure of the identity of an individual, or at least of the individual's preferences and behavior. The current lack of dissociability in engineering solutions has led to a proliferation of this type of disclosure of individual identity. In this realm, it is also vital that devices and applications cease to share information covertly without user consent. Current applications are apt to share data or respond to request for access by wireless technology sharing a communication space. Wireless devices transmitting non-user specific telemetry can create privacy risks to individuals. It is essential that the predictability principle consider both users created data and device/software metadata.

Conclusion

We are grateful to NIST for undertaking this initiative and applaud the goal of inclusion of a wide array of stakeholders in this process. The successful conclusion of the work to develop a Privacy Framework will bring the nation closure to the creating of a crosscutting effective Privacy Standard.