January 17, 2019

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

Re: Symantec Response to Request for Comment on “Developing a Privacy Framework”

Symantec is pleased to submit the following comments on the privacy framework that NIST is developing in cooperation with the private sector. Privacy and data security now has the attention of the average citizens, Boards of Directors, and government at all levels. We applaud NIST for undertaking this effort and are pleased that it is following the process used to develop the successful Framework for Improving Critical Infrastructure Cybersecurity (CSF).

Symantec is the world’s largest Cybersecurity company, and has extensive experience implementing privacy protections globally. Our submission reflects more than two decades securing privacy, and is divided into two sections. Section one provides General Comments on a potential Privacy Framework, while section two provides Specific Comments to provide data points for NIST’s consideration.

General Comments:

Security facilitates Privacy: Strong security and data protection are indispensable underpinnings of true and lasting privacy, yet too often privacy and security are portrayed as being in opposition. In the digital world this is a misconception – if your infrastructure or your data are not secure, then neither is your privacy. If you do not take steps to secure your own personal information, or the companies to which you entrust it do not do so, you are gambling with your privacy. Thus, when it comes to personal information, security measures and data protection are not an infringement on privacy but are in fact the foundations of maintaining privacy. As such, the Privacy Framework needs to acknowledge the role of security and should be tied to the CSF.

Defining Privacy: There is no singular definition of privacy, particularly in the context of operationalizing privacy protections and data security. Rather than search for a one-size-fits all description, the privacy framework will be most effective if it encourages organizations to take a hard look at their own privacy needs and build outward from there. To facilitate this, NIST should consider soliciting guidance from industry on how they use the term and what it means for their particular circumstance.

Privacy AND Security by Design: In order to be the most effective, both privacy and security controls should be “baked in” to a product or services design, not “bolted on” afterwards. This means adhering to “*X* by Design” principles from the beginning of every new product, system, service, or process effort. The Privacy Framework should help an organization assess whether it is following “*X* by Design” principles.

Specific Comments:

Organizational Considerations:

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

- A lack of privacy awareness poses a significant challenge to improving privacy protections. With the advent of digital technologies and networked communications, personal information has become ubiquitous. Data – and the ability to access it wherever and whenever you choose – has become an essential aspect of our economy and our everyday life. However, most people have poor awareness of the risk to data and lack the training, skills, or knowledge to handle properly the personal information to which they have access. If organizations and their employees do not understand the risk, they cannot mitigate it. As a result, the risk of inadvertent, negligent, unnecessary, improper or otherwise undesirable exposure of personal information, and through that, the risk of compromise of individual privacy, is enormous. A privacy framework is a starting point to address this risk.

An additional challenge to improve privacy protections for an individual is how an organization responds to a privacy incident. Can an organization prioritize remediation where possible, or measure and manage residual privacy risk when remediation has to wait? Moreover, if an organization needs to increase privacy protections, including tightening access controls to personal information, are they willing to do so at the expense of profitability, productivity or user convenience and satisfaction?

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

- "Privacy" itself is not easily given to a cross-sector definition; it is contextual and application-specific. Without a common starting point, it is difficult to develop a single set of guiding principles. We recommend that NIST embrace this diversity and focus on a high-level set of common principles followed by a framework that recognizes the myriad circumstances in which it may be used. The privacy framework should include guidance to help organizations assess and understand the scope of privacy as relevant to their specific circumstances, as well as examples or case studies on how similar risks have been addressed.

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

- The challenge of incorporating privacy risk into enterprise risk management is due to an assumption that privacy risk captured through a security risk assessment. There is a fundamental difference between security and privacy risk management and how the two are incorporated into an organization. Whereas enterprise risk management is focused on analyzing, mitigating and managing the risk to the organization itself, privacy risk management is about the risk to a third party, i.e. the individual whose privacy and information are at stake. Accordingly, security risk management requires an internal examination, understanding risk tolerances, and mitigating risk. Only then does an organization shift focus to factor external elements into a risk management plan.

On the other hand, privacy risk management starts externally and then shifts to internal. Among other things, it begins by assessing whether the organization has obtained consent to collect data, who owns it, and what happens if the data is lost. At that point the focus shifts to internal considerations, such as whether appropriate safeguards are in place to protect the data and how to dispose of data that is no longer needed.

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

- Privacy protection is a ubiquitous requirement that needs to be cascaded down to and enforced in every part of an organization. A Chief Privacy Officer or even a Corporate Privacy Office cannot single-handedly embed proper privacy practices throughout a large, diverse organization. So while a commitment to privacy must start at the top, it must be practiced at every level to ensure an organizational culture of privacy. In our experience, this works best when senior officials lead by example and lower level managers reinforce this message with regular communications about the importance of embedding proper privacy protection practices into day-to-day work.

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

- There are some existing structures in place that could be used as a starting point to develop specific outcomes. For example, the Fair Information Practice Principles (FIPPs) are internationally recognized principles that have informed existing Privacy regimes such as the GDPR in the EU. The principles of Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, Accountability and Auditing could be used in a similar role as Categories in the CSF, with specific outcomes being derived from each principle.

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.

- As a global, multinational organization, we rely on international standards to shape our overall approach to privacy. The final privacy framework should not set policy, but like the CSF should strive to work with existing US and international standards. Following the CSF model, an Informative Reference section in the Privacy Framework would help facilitate integration with other privacy frameworks and standards. We suggest including Asia-Pacific Economic Cooperation (APEC), Cross-Border Privacy Rules (CBPR), HIPAA Privacy Rule, GDPR, ISO27001, and ISO27018 in an Informative Reference Section.

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

- A Privacy Framework that attempts to set policy or is in conflict with established frameworks/standards (GDPR for example) could have serious and disruptive implications to global businesses.

<u>Framework Structure:</u>

16. Please describe how your organization currently manages privacy risk.

- Symantec has organized its privacy management by combining multiple complementary approaches. Organizationally we have stood up a global Privacy Operating Model tiered into three lines of defense:

- The first layer is our network of approximately 100 Privacy Ambassadors deployed across all frontline units of the corporate organization worldwide.

- The second layer is the group of business leaders accountable for each of these ambassadors and their units. These leaders are gathered in a Global Privacy Steering Committee that takes operational privacy decisions.
- The third layer is then itself a three-pronged structure, composed of:
    - the Global Privacy Council (C-suite executives representing all areas of the organization, setting strategic directions and arbitrating escalated disputes);
    - an independent external Data Protection Officer (appointed under the EU GDPR's requirement) with direct access and an advisory role to the C-suite and to the Board of Directors;
    - and global Enterprise Risk Management (i.e. the internal audit function) which monitors, measures and reports on privacy compliance throughout the organization.

All three layers are backed by a dedicated Global Privacy Office composed of a Privacy Legal function (attorneys assigned to assist specific areas of the business on privacy matters), a Compliance and Response function (directorate in charge of maintaining or restoring compliance and responding to any privacy incidents) and a Privacy Operations function (the program management team ensuring that privacy resources are properly maintained and the privacy program is implemented).

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 success of the CSF is largely due to its structure. It starts with Functions and provides more detail with the Categories and Subcategories and allows for flexibility in how an organization assesses and communicates its security posture. Since privacy and cybersecurity are so closely related it would be useful if the privacy framework uses the same structure as the CSF. The Core could set the common denominators while Profiles could help organizations define the scope of privacy as relevant to their specific circumstances.

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 […].

- Given the interrelationship of security and privacy, the new framework should follow the same general construct as the CSF. This will encourage use of the privacy framework. The privacy framework will require its own unique Functions, so we recommend "The information life cycle" or FIPPs as possible candidates.

<u>Specific Privacy Practices:</u>

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

- Protecting an individuals' privacy starts with being able to control what happens to, or who has access to the data an organization has collected about the individual. As such, data access, security, and lifecycle management are absolutely critical. An organization needs to have the ability to identify all user data no matter wherever it may be stored or used, and to be able to label data that needs privacy protections. Privacy related data should be wrapped with protections in order to control who has access and how it is used as well as to detect any privacy policy violations. Encryption and/or Tokenization should be applied to private data to render it useless if stolen which reduces the risk to the individual.

Other privacy-relevant measures and capabilities should be used as relevant to the particular risk profile of each organization. These include pseudonymization, data availability and system resiliency, user authentication and identity management, incident detection and response, policy enforcement and compliance automation and monitoring.

25. Whether these practices are relevant for new technologies like the Internet of Things and Artificial Intelligence.

- Privacy by Design (PbD) principles should be integral to the development of any new or emerging technology. IoT devices often collect personal data and frequently lack privacy protections. Artificial Intelligence (AI) systems process considerable amounts of data, including personal data. PbD can be utilized to address privacy in IoT, AI and other yet to be invented technologies. Adherence to a well-developed PbD program facilitates strong privacy provisions independent of the technology under development. An effective PbD program will in particular enable organizations to gauge their privacy risk profile and determine what privacy-protecting and privacy-enhancing measures and capabilities are relevant to implement.

Still, the privacy framework should be independent of specific technologies (cloud or AI) or implementations (mobile or IoT) and should be applicable no matter where data resides or how it is being managed on a technical level.

Conclusion

We are glad that NIST is taking on this important issue, and we appreciate the opportunity to provide our input on this effort. We look forward to the upcoming workshops.

Sincerely,

Jeff E Greene

Jeff Greene
Vice President, Global Government Affairs and Policy
Symantec Corporation
700 13th Street, NW, Suite 1150
Washington, DC 20005
202-383-8708
Jeff_Greene@symantec.com