Microsoft's Response to the Request for Information of the National Institute of Standards and Technology

Developing a Privacy Framework

I. Introduction

Microsoft Corporation ("Microsoft") welcomes the opportunity to provide these comments to the National Institute of Standards and Technology ("NIST") in response to the request for information on the development of a framework that can be used to improve the management of privacy risk by organizations for individuals that arises from the collection, storage, use, and sharing of their information (the "Privacy Framework").

As NIST has recognized, the Privacy Framework should be developed through a consensus-driven, open, and collaborative process that will include workshops and other opportunities to provide input.[1] Microsoft shares NIST's goal of developing a voluntary framework that consists of outcomes and approaches that align policy, business, technological, and legal approaches to improve risk management processes.[2]

NIST's challenge is to create a Privacy Framework that can subsist with global privacy regimes and bring new value to the existing privacy ecosystem. To achieve that goal, Microsoft encourages NIST specifically—and the U.S. Government more broadly—to pursue a comprehensive approach to privacy that is: (1) interoperable with other global approaches, (2) forward-looking, and (3) risk-based and outcome-focused. This approach can build on NIST's successful Cybersecurity Framework, mapping global privacy regimes and regulatory obligations to actionable engineering, policy and operational choices.

II. Microsoft's Approach to Privacy

Microsoft believes that privacy is both a fundamental human right and a foundation for trust. As people live more of their lives online and depend more on technology to operate their businesses, to engage with friends and family, to pursue opportunities, and to manage their health and finances, the protection of privacy becomes more important than ever.

At Microsoft, we know that people will use only technology they trust. Ultimately, trust is created when people are confident that their personal data is safe and they have a clear understanding of how and why it is used. This means that companies like Microsoft have a responsibility to safeguard the privacy of the personal data they collect and manage. Our commitment to privacy has a multiplying effect. Our practices support strong privacy practices by our customers: from enterprise customers serving thousands of individuals to small and medium businesses that may not be able to independently achieve the same level of privacy protection. So when we develop products and services that are privacy

---

[1] *See* Department of Commerce, National Institute for Standards and Technology, Notice; Request for Information, Nov. 14, 2018, *available at* https://www.govinfo.gov/content/pkg/FR-2018-11-14/pdf/2018-24714.pdf ("Privacy Framework RFI" or "RFI").

[2] *Id.*

protective, the businesses that use them become more privacy protective, which ultimately inures to the benefit of all consumers.

Microsoft is a strong supporter of efforts to create risk-based, interoperable privacy regimes. In the United States, Microsoft has advocated for national privacy legislation since 2005. We also are committed to taking concrete steps to strengthen consumers' privacy protection now, as the debate about data privacy continues in the U.S. That is why in May, we extended the rights at the heart of the European General Data Protection Regulation ("GDPR") to all consumers worldwide. Those include the right to know what data we have collected about you, to correct that data, to delete it, and even to take it elsewhere. We are struck by how clearly the desire for these controls resonates globally, including with Americans. In fact, on both an absolute and per capita basis, the largest number of people using our tools to exercise these rights comes from the United States.

Microsoft's commitment to privacy is reflected throughout our business. We focus on six key privacy principles that shape the way we build our products and services: (1) *control*: we will put you in control of your privacy with easy-to-use tools and clear choices; (2) *transparency*: we will be transparent about data collection and use so that you can make informed decisions, (3) *security*: we will protect the data you entrust to us through strong security and encryption; (4) *strong legal protections*: we will respect your local privacy laws and fight for legal protection of your privacy as a fundamental human right; (5) *no content-based targeting*: we will not use your email, chat, files or other personal content to target ads to you; and (6) *benefits to you*: when we do collect data, we will use it to benefit you and to make your experiences better.[3] Our privacy principles are based on the Fair Information Practice Principles ("FIPPs") and stand as a cornerstone of our privacy program, which we have expanded to apply to a number of international regulatory regimes.

III. The Privacy Framework Should Be Interoperable.

The Privacy Framework must be able to support U.S. businesses that operate globally—and that are subject to privacy regimes across the world, derived from widely divergent cultural, contractual, and regulatory requirements. To do this, Microsoft urges NIST to use the Cybersecurity Framework as a model for the Privacy Framework, which should identify functions and categories of privacy obligations relevant to privacy laws and regulations worldwide and map those obligations to standards and tools that businesses can implement to achieve compliance. In this way, the Framework would support interoperable technological, operational, and policy controls and standards that can be repurposed to achieve compliance with global privacy regimes.

A. Need for Interoperability

Microsoft strongly supports NIST's view in the RFI that the Privacy Framework "should take advantage of existing privacy standards, methodologies, and guidance" and be "compatible with and support organizations' ability to operate under applicable domestic and international legal or regulatory regimes."[4] Like many companies, Microsoft's products and services rely on an internet that is

[3] *See* Microsoft, Privacy At Microsoft, available at https://privacy.microsoft.com/en-US/.

[4] *See* Privacy Framework RFI at 56825.

interoperable, open, and globally accessible to as many people as possible. That requires interoperable privacy frameworks.

The Privacy Framework should fundamentally aim to reduce fragmentation of privacy operations, both nationally and globally, by identifying technological, operational, and policy controls that can be used to satisfy global privacy regimes.[5] The Privacy Framework also should be mapped to, and be customizable with, local privacy regimes. For example, the Cybersecurity Framework is built on a set of functions and categories. In considering the functions and categories to be included in a new Privacy Framework, NIST should ensure that those functions and categories are consistent with existing privacy regulatory and legal obligations worldwide, and with existing international standards. The Framework would add significant value in synthesizing these disparate obligations and mapping them to engineering, operational and policy choices that businesses can implement to achieve their desired outcomes, including choices that can be used to satisfy multiple global obligations. Indeed, the biggest challenge in improving organizations' privacy protections for individuals is ensuring that businesses can readily identify tooling and standards that achieve compliance with the range of privacy obligations to which they are subject.

Reducing fragmentation also reduces compliance costs, for companies of all sizes. U.S. companies that operate globally must meet legal and regulatory obligations in jurisdictions worldwide, as do small and medium businesses that seek to serve a global customer base. An interoperable Framework would help reduce compliance costs by helping to contain the cost of adhering to global privacy regimes, by identifying technological controls that can be used to satisfy multiple global privacy obligations. In contrast, if the new Framework imposed a new or additional set of requirements, it would increase costs and thus disincentivize its adoption by industry and particularly by small businesses that may have limited compliance operations. While large multinational companies may have the experience, people, and resources to reconcile complex international regimes, small and medium enterprises may be disproportionately harmed by a Framework that is not interoperable.

To date, the privacy compliance efforts of many companies have focused on law and policy requirements without sufficient engineering or operational controls in place to validate that those requirements are met.[6] Now, with new global privacy laws including the General Data Protection Regulation, there are more clear privacy laws with substantive similarities among jurisdictions than ever before. NIST should leverage these clear rules in establishing a Privacy Framework that will be a tool for companies to interpret how technological, operational, and policy controls and standards that enable compliance with country-specific requirements relate to each other. It should also embody a risk-based approach to deciding where companies should most effectively focus their efforts. For example, the Framework may help companies interpret the technological, operational, and policy controls and standards needed for compliance with global privacy regimes, including in countries such as Canada, Brazil, Australia, New Zealand, Canada, South Korea, Japan, the United Kingdom, and Europe, to name only a few jurisdictions, or states including California. Microsoft and many other multinationals already have implemented privacy management systems such as ISO/IEC 27018 to enable the fulfillment of privacy requirements, both those imposed directly by government regulation and those imposed indirectly by the regulatory requirements to which our corporate and public sector customers are subject. A new Framework adds value by helping U.S. businesses take into account the myriad existing

[5] This paragraph responds to RFI question 1.

[6] This paragraph responds to RFI question 11.

privacy obligations and identify and interpret controls for meeting those obligations, rather than imposing additional or entirely new and potentially redundant sets of controls.

NIST has long recognized that "[t]he development of international standards [] promotes U.S. interests by facilitating interoperability, security, usability, and resiliency, improving trust in online and offline transactions, promoting innovation and competitiveness, and helping U.S. products and services compete in global markets."[7] Although that statement was made in the cybersecurity context, the same is true of privacy. Just as NIST recommended that "[f]ederal agencies should use relevant international standards for cybersecurity, where effective and appropriate," NIST should do the same for privacy.[8] Doing so also would align with NIST's recommendation to use relevant international standards to achieve mission and policy objectives.[9]

The National Telecommunications and Information Administration ("NTIA") has committed to an international approach, working "with its international partners toward an industry-led global marketplace that promotes innovation for IoT and supports the free flow of information, and the ability of American companies to compete fairly around the world."[10] We believe this approach makes sense, and we urge NIST to embrace it.

The need for interoperability and strong management practices are particularly acute for new technologies such as the Internet of Things ("IoT") and Artificial Intelligence ("AI"). Voluntary, consensus-based standards provide a basis for facilitating these objectives. The Privacy Framework should not only be interoperable with other frameworks and standards, but also ensure that IoT and AI systems developed in consultation with the Privacy Framework will be able to interoperate with other devices and systems. Several other countries have national strategies expressing support for standards that facilitate this type of globally-connected IoT devices, including the U.K. and South Korea.

B. Benefits of Interoperability[11]

The more interoperable the Privacy Framework is, the more compliance solutions and concepts can scale and be cost effective, the more they will enable companies to focus on innovation and expanding their business models, rather than on country-by-country legal obligations. Interoperable solutions also allow customers to enter markets that they might otherwise refrain from entering due to regulatory barriers. In contrast, regulatory fragmentation creates barriers to entry and limits the growth of small and mid-size companies, including many of Microsoft's customers.

---

[7] *See* National Institute for Standards and Technology Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity, Dec. 2015, at 11, *available at* https://csrc.nist.gov/CSRC/media/Publications/nistir/8074/vol-1/final/documents/nistir_8074_vol1_draft_report.pdf ("NIST IR 8074").

[8] *Id*. at 13.

[9] *Id*.

[10] The Department of Commerce Internet Policy Task Force & Digital Economy Leadership Team, Fostering the Advancement of the Internet of Things, January 2017, *available at* https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf ("NTIA IoT Green Paper").

[11] This section responds to RFI question 14.

For businesses, the ultimate goal is to build and release a product or service globally, but make as few adjustments as possible during the product engineering process. A Framework that does not harmonize privacy engineering in this manner would increase costs, without providing the same value as a unified Framework. Moreover, a successful, globally-relevant, and widely-adopted Framework may also influence the development of policymaking in regions where privacy practices and policies are either still in development or under-developed.

C. How to Achieve Interoperability

In creating the Privacy Framework, NIST should take care to differentiate between the global legal and regulatory regimes to which businesses are already subject and the controls and standards that businesses can meet to satisfy those legal and regulatory obligations. To make the Framework interoperable, NIST should identify technological, operational, and policy controls and standards that can be applied to achieve compliance with legal and regulatory obligations around the world. For example, the Privacy Framework will be interoperable if it can be mapped to, and customizable with, local privacy regimes and with well-established sector-specific requirements such as those for healthcare and the financial industry. The Framework should identify the standards and controls businesses may use to meet those requirements.

To create an interoperable Framework, NIST can adopt the approach used by the Cybersecurity Framework: creating a structure that connects a vast number of controls from standards to be aggregated at a summary level, to enable company executives to discuss functional capabilities. In this way, the Framework allows businesses to decode and meet existing global requirements, rather than functioning as a set of compliance standards itself. During the drafting process, NIST also can ensure interoperability by testing the draft Privacy Framework against global legal and regulatory requirements, to ensure that businesses may use the new Framework to comply with privacy requirements worldwide. For example, this may include tabletop exercises, mapping, or other compatibility checks, throughout the drafting process.

NIST also should ensure the new Privacy Framework is compatible with applicable ISO/IEC standards.[12] Specifically, and as discussed in more detail in Section VI.A.2 below, the Privacy Framework should be compatible with and interoperable with the ISO/IEC 27001 and 27002 family of standards on information security management systems. It also should align with the privacy-enhanced controls in section 6 of ISO/IEC 27552 and the privacy-specific controls in sections 7-8 of ISO/IEC 27552; that standard defines a privacy information management system based on, and as the extension of, ISO/IEC 27001 and 27002.

In identifying global privacy requirements that may inform the functions, categories, and subcategories of a new Privacy Framework, NIST should also take into account existing bilateral and multilateral frameworks. These may include the EU-U.S. Privacy Shield, the APEC Cross-Border Privacy Rules, and the U.S.-Mexico-Canada Agreement. Creating interoperable frameworks also may encourage countries to engage in bilateral and multilateral conversations about making the various cross-border transfer frameworks interoperable, such that one set of technological, operational, and policy controls can be followed to enable compliance with multiple legal regimes.

[12] This section responds to RFI question 13.

IV. The Privacy Framework Should Be Forward-Looking.

The Privacy Framework needs to do more than fit today's technology. It also must be designed to accommodate tomorrow's technology—and tomorrow's innovative privacy controls and new global privacy regimes. This requires a forward-looking framework that is both flexible and adaptable. For example, the new Privacy Framework must at a minimum allow businesses to apply existing privacy standards and tooling to existing technologies to achieve compliance with existing privacy obligations. But to add meaningful value to the privacy ecosystem, the Privacy Framework should also be flexible enough to apply to new technologies and to incorporate new privacy controls that do not yet exist. In addition, the Framework should be able to adapt to new global privacy regimes. In the United States, we have already seen an evolving privacy legislative landscape, with calls for a federal privacy law and new privacy legislation in California. Microsoft accordingly urges NIST to design the framework in a flexible manner that leaves room for innovation.

A. Need for Forward-Looking Framework[13]

The Privacy Framework should help organizations use and build upon upcoming new technologies including AI and IoT and reflect the use of data in the development of those technologies. U.S. leadership is critical for protecting U.S. consumers, institutions, and industry competiveness and innovation in the era of digital transformation.

Privacy is an important component of trustworthy new technologies, including AI and IoT. The new Privacy Framework therefore should be usable and relevant to the development of AI and IoT and make sense for a range of technologies. For example, the rapid development of IoT devices raises unique privacy concerns, as it dramatically increases the number of devices facilitating the creation, collection and transmission of data. At the same time, IoT devices without screens or other direct user interfaces create significant practical challenges for privacy regimes premised on notice and consent. The notice and consent model was built on the premise that users can be given comprehensive information about an organizations privacy practices at a point in time before data is collected, as well as an opportunity to consent to those practices. That model does not translate well to IoT devices that have a limited ability to display traditional notices or collect traditional consents. The Privacy Framework should accordingly recognize that important outcomes like an informed user may be achieved in other ways.

Focusing on outcomes, rather than imposing prescriptive requirements, also reflects the core principle of technology neutrality. Neutral frameworks are premised on principles and focus on outcomes, rather than prescriptions, which can inhibit innovation over time. This allows the Framework to easily be applied to current and future technology, supporting both privacy goals and innovation. For example, a law focusing on outcomes can require that consumers be informed of certain business practices, but allow businesses to inform consumers in different ways depending on how their service operates. By contrast, a law requiring a business to obtain a specific type of check-the-box consent may be unattainable for new technologies that lack screens or direct user interfaces.

The challenge of implementing the Framework for a business or organization will vary depending on the volume of personal data involved. The greater the amount of data, the greater the challenges. This underscores the need for a scalable Framework.

[13] This section responds to RFI questions 24-25.

B. Benefits of a Forward-Looking Framework

A forward-looking Privacy Framework will allow U.S. companies to demonstrate that they can use data responsibly and support U.S. interests, such as the use of AI across all industries and across borders. It also will support innovation. When businesses can ensure the protection of their customers' private information, consumers will come to new innovations like IoT and AI technologies with greater confidence and adopt the technologies more rapidly. Microsoft has long been a supporter of baseline privacy legislation—and of robust enforcement for those that breach that legislation—for exactly that reason. Consumers need to have faith that the rules are being followed as they embrace new technologies. By incorporating today's privacy practices and leaving room for practices that are developed tomorrow, a new Privacy Framework will help these innovations thrive.

C. How to Achieve a Forward-Looking Framework

To support innovation in both technology and in privacy-protective practices, the Framework should take into account practices that include: (1) privacy-promoting technologies (2) grounds for processing beyond consent, (3) transparency, and (4) data minimization. At the same time, it should recognize that privacy issues may not only be addressed by tooling and solutions developed today, but by new mechanisms that may be developed tomorrow. As NIST has recognized in the cybersecurity context, "[g]reater understanding of how to identify privacy risks and integrate mitigations into [] standards or their deployment in information systems will require further research."[14] For this reason, Microsoft urges NIST to develop a Privacy Framework that is flexible enough to accommodate privacy-protective mechanisms not yet developed.

- *Privacy-Promoting Technologies.* The Framework should recognize the privacy benefits of new technologies, such as de-identification techniques, homomorphic encryption, and secure multi-party computation. In doing so, the Framework should seek to help organizations determine when to use new privacy-promoting technologies, based on their risk profile and assessment.

- *Grounds for Processing Beyond Consent*. The Framework should recognize that traditional concepts of notice and consent may not be the best method of informing and empowering users of their privacy choices, particularly for new technologies. Too often, notice and choice has resulted in long, legal, regulator-focused privacy notices and check boxes that do not effectively advance the privacy of most individuals. Indeed, regulators, advocates, academics, and consumers around the world increasingly are skeptical of notice and choice and believe that the shortcomings associated with consent in this framework are enabling companies to do what they want with personal data without sufficiently protecting privacy. The Framework can instead focus on enabling the protection of consumer privacy through tools that empower individuals to control how their personal data is used, as well as through continuous risk-based analyses designed to ensure the protection of individuals' information. The Framework also should recognize that consumers reasonably expect companies to engage in certain types of data processing in the context of their relationship and activity, and that consent may not be needed when the collection or use of data is either obvious from the context of the transaction or sufficiently accepted or necessary for public policy reasons.

[14] *See* NIST IR 8074 at 10.

- *Transparency*. Providing transparency is the key to earning and maintaining trust in the digital world—particularly in the context of new technologies such as AI and machine learning. The key to transparency is delivering the most relevant information in a helpful way that does not overload individuals with unnecessary information or choices. At the same time, transparency is a challenge in the era of big data. The effectiveness of any notice provided to a consumer often hinges on the expectations of that consumer. Those expectations can be set through effective notices that enable an understanding of what happens to personal data and why, delivered at a time that allows for meaningful decision-making. The Framework should support transparency and recognize that design decisions are critical to ensuring a proper level of transparency.

- *Data Minimization.* The concept that companies should limit the collection, storage and use of personal data to the purposes for which the data is processed is a longstanding privacy principle. This principle should not be applied narrowly, which may constrain the development of AI and IoT technologies. For example, AI systems rely on data to verify the integrity of their systems and to guard against bias and inequitable outcomes. Accordingly, the Framework should reflect the principle of data minimization in a manner that recognizes that the processing of large amounts of data for continuous machine learning may be necessary for AI to be accurate and effective. At the same time, organizations should proactively articulate and document why they need to collect and process data, why other data sources may be necessary, and what they expect to accomplish by processing the data. In this way, organizations may demonstrate commitment to the data minimization principle while ensuring they can process data needed for reliable AI systems.

One example of a new technology where all of these challenges come together is facial recognition, which brings important and even exciting societal benefits but also carries the potential for abuse. As with all new technology, the uses of facial recognition are multiplying in both predictable and surprising ways. Microsoft is one of several companies playing a leading role in developing this technology. We have also called for government regulation of facial recognition technology[15] and in December we published six principles for developing and deploying facial recognition technology.[16] As facial recognition technology develops, it will be critical to identify privacy-protective technologies that can be leveraged to reduce the associated privacy concerns, and to ensure that individuals are aware when the technology is used—even outside the traditional contexts where notice and consent have been applied. The use of facial recognition technology should also be transparent, and the data used by the technology should be minimized. The Framework should help businesses identify and satisfy these important concerns.

---

[15] *See* Brad Smith, Microsoft, *Facial Recognition Technology: The Need for Public Regulation and Corporate Responsibility*, July 13, 2018, *available at* https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility/; Brad Smith, Microsoft, *Facial Recognition: It's Time for Action*, Dec. 6, 2018, *available at* https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action.

[16] *See* Rich Sauer, Microsoft, *Six Principles to Guide Microsoft's Facial Recognition Work*, Dec. 17, 2018, available at https://blogs.microsoft.com/on-the-issues/2018/12/17/six-principles-to-guide-microsofts-facial-recognition-work.

V. The Privacy Framework Should be Risk-Based and Outcome-Focused.

Microsoft strongly supports NIST's commitment in the RFI to providing a "prioritized, flexible, risk-based, outcome-based and cost-effective approach that can be compatible with existing legal and regulatory regimes."[17] Microsoft also supports the manner in which NIST seeks to achieve this goal: by providing a "catalog of privacy outcomes and approaches to be used voluntarily, rather than a set of one-size-fits-all requirements, in order to: foster innovation in products and services; inform education and workforce development; and promise research on and adoption of effective privacy solutions."[18] As NIST has recognized, the Framework should "assist organizations to better manage privacy risks within their organization without prescribing the methods for managing privacy risk."[19]

A. Need for Risk-Based, Outcome-Focused Framework

Risk management is at the core of privacy protection. Companies should be responsible for conducting rigorous and documented risk assessments, which can be reviewed upon request by relevant government authorities. Identified risks should be mitigated through documented safeguards, such that the benefits of processing personal data outweigh the residual risks. This is fundamental to ensuring that users are protected and safeguarded.

A consistent risk-based, outcome-focused approach helps businesses develop the trust of their customers by helping them demonstrate the controls in place to process and collect personal data. In the related context of cybersecurity, regulators, standards organizations, and industry have long recognized the benefits of a risk-based approach. The Cybersecurity Framework expressly states that it is "not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure" because "[o]rganizations will continue to have unique risks—different threats, different vulnerabilities, different risk tolerances—and how they implement the practices in the Framework will vary."[20] Moreover, the Cybersecurity Framework maturity model recognizes that an "adaptive" approach to cybersecurity risk management is the most sophisticated.[21] Similarly, in the financial institutions context, the Federal Financial Institutions Examination Council has issued a Cybersecurity Assessment Tool, based largely on the Cybersecurity Framework, to assist organizations in determining the relationship between their inherent risk and readiness to address that risk.[22]

A risk-based approach is needed for privacy. As with the Cybersecurity Framework, the Privacy Framework should enable businesses to conduct an assessment of their businesses' current compliance practices and their compliance goals, based on an informed perspective of the relevant risks. That

---

[17] *See* Privacy Framework RFI at 56824.

[18] *Id.* at 56825.

[19] *Id*.

[20] National Institute for Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, Feb. 12, 2014, at 2, *available at* https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[21] *Id*. at 9.

[22] Federal Financial Institutions Examination Council, Cybersecurity Assessment Tool, *available at* https://www.ffiec.gov/cyberassessmenttool.htm.

approach allows businesses to innovate and to determine the appropriate solution for their products and services, rather than merely adopt the lowest common denominator. In contrast, an inventory of prescribed controls would render the Framework useless for businesses that do not fit its mold and would transform the document into a compliance checklist, rather than a dynamic tool for identifying and managing privacy risk. The Cybersecurity Framework also exemplifies an outcome-focused approach, by identifying five functions relating to cybersecurity and potential outcomes within each function. The same approach should be used here.

B. Benefits of a Risk-Based, Outcome-Focused Framework[23]

Microsoft's practices illustrate the benefits of a risk-based, outcome-focused approach to privacy, which is more durable, useful and effective than prescriptive approaches. Overall, Microsoft focuses on risks using an "all hazards" approach, under which we assess our entire organization to identify what is most important to us and our stakeholders (including customers, partners, re-sellers, shareholders, and employees). For example, at the corporate level, Microsoft's Enterprise Risk Management ("ERM") strategy aligns with both the Committee of Sponsoring Organizations' Enterprise Risk Management-Integrating with Strategy and Performance and ISO 31000: 2009, Risk management—principles and guidelines. Alignment with international standards ensures an agile best practice structure, which provides the basis for effective collaboration across stakeholder groups for risk assessment and reporting purposes.

An ERM risk assessment process has three closely-related components. While they are managed as discrete processes, the outcome of the trio informs how we treat and manage risk programmatically across the corporate enterprise. They are:

- *Risk identification*. The risk identification process is led by ERM, but subject matter experts in the business units who are responsible for the risk drive the execution and identification activities. For example, we identify our most important services, legal requirements and customer commitments and then identify their key dependencies, which include systems and data. This enables significant internal oversight and coordination across the corporation.

- *Risk analysis.* Our ERM teams analyze inherent and residual risk levels and map identified risks to common risk descriptions, drivers, and domains. Throughout this process, there are several quantitative and qualitative analyses that are applied including evaluating cross-category risk exposures and setting priorities.

- *Risk evaluation.* Once risk identification and analysis activities are completed, the internal process applies an accountability model as well as evaluates common theme areas and domains for changes to its existing enterprise risks.

Our company-wide standards also allow senior management to oversee policies and procedures for managing privacy risk, including the Microsoft Privacy Standard ("MPS"), which is our corporate-wide policy that encapsulates global privacy laws and is acted on by teams across the company. This and other company-wide policies are applied to the security and privacy risk management process followed by our engineering team, which maps policies to a set of privacy controls designed to meet the policy.

[23] This section responds to RFI questions 3-7 and 15-16.

Those controls are then mapped to technical and organization measures to achieve the appropriate level of risk control.

Our other policies and procedures for managing risk—and for allowing our customers to manage their risk—include: (1) our Data Protection Impact Assessment ("DPIA") process, (2) our Service Trust Portal, which provides GDPR documentation to IT administrators on how to delete, view and export data that is being captured as telemetry and also identifies to customers how we classify data, and (3) our processes for responding to a privacy incident or a personal data breach within Microsoft. For example, DPIAs cover all processing across the company, helping to ensure that products and services are designed with appropriate privacy protections. These rigorous and documented risk assessments are reviewable upon request by appropriate government authorities, and are fundamental to ensuring that our customers' information is protected. We also implemented ISO/IEC 27018, which applies to handling of personal data by processers, on cloud-based services and use a structured risk-based approach to privacy risk management for all products and services where either regulations or our customers require privacy management. As a result, we have defined and developed granular controls for security and privacy risk management based on internally-accepted best practices and share these with our customers.

These policies assume a dynamic risk landscape and are designed to address risks that suddenly may increase. For example, our engineering teams continually re-evaluate risk profiles and respond accordingly, such as by issuing security and privacy protection updates to our products and services. Microsoft has invested significant effort into building a strong incident response program for both security and privacy. Our incident response programs have been in place for many years and include teams that respond to both company-focused incidents (how we protect Microsoft) and incidents related to our products (how we protect our customers). As with risks, we see the importance of managing security and privacy incidents with a common approach and leverage many of the same teams and processes. Should an incident escalate to a crisis level, our Enterprise Crisis Management team can be called upon to support with coordination and communication. This team is made up of Corporate Vice Presidents from across the company and has components that tie into our Senior Leadership team and Board of Directors, if necessary.

This risk-based, outcome-focused approach ensures that companies like Microsoft can identify and implement a set of privacy controls that aligns with the risks relevant to their business. That helps Microsoft comply not just with our own national, regional, and industry-specific requirements governing the collection and use of customer data, but also to choose privacy controls that we can pass on to our customers. For example, we provide business and enterprise customers with audit reports, security assessment documents, in-depth details of how we implement and test security and privacy controls, and technical white papers, among other information, to help our customers manage their risks.

A risk-based, outcome-focused Privacy Framework also will help create a privacy-focused workforce. Harmonizing privacy engineering practices and developing an interoperable framework will create common privacy operations in organizations globally and help to standardize and develop privacy workforce skills. Harmonization also creates a career-boosting skillset around the world, because skills learned in one country will be readily useful in another.

C. How to Achieve a Risk-Based, Outcome-Focused Framework[24]

The new Framework should enable businesses to both assess their current state of privacy compliance and to identify tools that can help them achieve greater compliance. The Framework can do this by helping businesses identify privacy-related risks and mapping those risks to technology solutions that can mitigate the identified risks, consistent with existing obligations imposed by global privacy regimes.

The Framework may help businesses break down their assessment of privacy risks into multiple parts, taking into account issues including the type of data the business collects, the uses applied to that data, and the data governance measures in place to mitigate against privacy risks. For example, a business using the new Framework could begin by assessing the type of data the business collects (e.g., personal data or other data), the uses applied to that data (e.g., to identify a person or process a transaction), and the data governance measures applied to the data (e.g., encryption, access controls, limited retention period). In this way, Framework would help businesses identify their highest-risk areas and allow them to target those areas for additional investment in new privacy controls.

In determining which privacy standards to include in the Framework, Microsoft urges NIST to take an outcome focused approach that begins with identifying the desired outcomes and then determining which standards and practices deliver those outcomes. Microsoft believes the most important outcomes are a reasonably informed user (Transparency), empowered to meaningfully express privacy preferences (Control), whose personal data is continuously protected through rigorous, documented risk assessment and mitigation cycles designed to ensure that products and services are inherently designed with appropriate privacy protections (Risk Management), as Microsoft has previously urged to NTIA.[25]

In line with these outcomes, the Privacy Framework should support strong risk management practices through documented risk assessments. These risk assessments could be used to demonstrate to relevant authorities a valid and credible decisional process in designing online experiences. In particular, they can demonstrate consideration of the context of data processing, the affected parties to which a disclosure is made, and the purpose and desired effect of a disclosure. If the risk assessment determines that the potential risks to the individual whose data is to be processed outweigh the benefits associated with the processing, then companies may proceed with the individual's informed consent.

VI. To Support These Outcomes, the Privacy Framework Should be Based on the Cybersecurity Framework.

To create an interoperable, forward-looking, risk-based, outcome-focused Privacy Framework, NIST should begin with the Cybersecurity Framework, which possesses all of these traits.[26] Like the Cybersecurity Framework, the Privacy Framework should map policies and laws into actionable

[24] This section responds to RFI question 9.

[25] *See* Response of Microsoft Corporation to the Department of Commerce National Telecommunications and Information Administration, In the Matter of Developing the Administration's Approach to Consumer Privacy, Nov. 9, 2018, *available at* https://www.ntia.doc.gov/files/ntia/publications/msft_response_to_ntia_privacy_rfc.pdf.

[26] This paragraph responds to RFI questions 17-18.

engineering choices. As NTIA recognized, the Cybersecurity Framework "can be scaled to organizations' different needs, allowing them to take into account their particular business models, assets, and other variables. This structure enables organizations to adapt to an ever-changing, dynamic environment."[27] Although NTIA made this statement with respect to IoT technologies, this approach is well-suited to the full range of technologies and industries seeking to manage privacy risks.

Like the Cybersecurity Framework, the new Privacy Framework should be cross-sector and technology neutral.[28] Different sectors have some degree of uniqueness. But companies largely do businesses with companies not in their sector, making a shared cross-sector standard-based Framework more relevant. The primary challenge for NIST is to enable unique sector-specific requirements to fit atop the broader Privacy Framework. This cross-sector model should be scalable from small and medium-sized businesses to multinational companies and government agencies and should pivot at the risk defined by the organization. Moreover, the Privacy Framework should be cost-effective for companies seeking to use it. One way of achieving that goal is by prioritizing the functions and categories of the Privacy Framework to distinguish foundational principles that enable a variety of capabilities from more specialized ones. Basing the Privacy Framework on the Cybersecurity Framework also will enable businesses already using the Cybersecurity Framework to adopt the new Privacy Framework to handle security and privacy consistently and harmoniously.

For all of these reasons, Microsoft believes that the Cybersecurity Framework should be the model for the Privacy Framework. To the extent NIST uses other guidance as a model for the Privacy Framework, it may miss the opportunity to create a truly interoperable Framework that meaningfully advances the ability of U.S. businesses that operate globally to implement privacy standards that are relevant worldwide. For example, the Cybersecurity Framework helps organizations manage their cybersecurity risk by determining which security controls from NIST 800-53 they may utilize to achieve their security risk profile. Similarly, the Privacy Framework should help organizations manage their privacy risk by determining which privacy controls to utilize from the final version of NIST 800-53 Rev 5 or from other comparable standards. Building an interoperable, relevant Framework requires starting with a model that is designed for interoperability, like the Cybersecurity Framework.

The core privacy principles to be reflected in the Framework should be developed throughout the open process, based on stakeholder input.[29] In the RFI, NIST set out a number of practices with the goal of better understanding how widely used the practices are, how they relate to international standards, and whether they should be considered for inclusion in the Framework. These practices include 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; data management, including tracking permissions or other types of data tools, metadata, machine readability, data correction and deletion, and usable design or requirements. Microsoft believes all of these practices are important in protecting privacy, although their best applications are dependent on the context. Microsoft is therefore ready and prepared to work with NIST in the open process of developing the Framework to identify how each

[27] NTIA IoT Green Paper at 27.

[28] This paragraph responds to RFI question 2.

[29] This paragraph responds to RFI questions 19-26.

of these processes may appropriately be used to manage privacy risks and the appropriate scenarios for using each practice.

A. Key Components of Privacy Framework

1. *Attributes*[30]

Microsoft strongly supports the attributes that NIST has identified for the Privacy Framework:

- *Compatible with or may be paired with other privacy approaches*. As detailed above, Microsoft believes that NIST's highest priority in designing the Privacy Framework should be ensuring its interoperability. As a result, Microsoft strongly supports this attribute. The Privacy Framework should support and enhance the ability of businesses to operate globally and to unify privacy operations. For example, the Framework can support this goal by incorporating existing international standards. This will allow businesses that have worked to achieve compliance with international standards to leverage that work in demonstrating their compliance with the voluntary Framework and other privacy regimes.

- *Adaptable to many different organizations, technologies, lifecycle phases, sectors, and uses*. A flexible Privacy Framework enables hyperscale compliance solutions, and thus allows customers to leverage those solutions to enter markets that they otherwise might refrain from entering due to regulatory barriers. Microsoft accordingly strongly supports this attribute.

- *Common and accessible language*. Microsoft supports this attribute. As part of ensuring the Privacy Framework is accessible to a broad audience, NIST may also help identify operational approaches to implement the Privacy Framework, while allowing companies to determine the most effective governance structure for implementation.

- *Risk-based, outcome-based, voluntary, and non-prescriptive*. Microsoft strongly supports this attribute. A risk-based, outcome-focused, voluntary Framework helps customers. As noted above, Microsoft believes the most important outcomes are a reasonably informed user (Transparency), empowered to meaningfully express privacy preferences (Control), whose personal data is continuously protected through rigorous, documented risk assessments designed to ensure that products and services are inherently designed with appropriate privacy protections (Risk Management).[31]

- *A living document*. Microsoft strongly supports this attribute. As technology, culture, user expectations and the political and regulatory landscape develops, so should the

[30] This section responds to RFI question 8.

[31] *See* Response of Microsoft Corporation to the Department of Commerce National Telecommunications and Information Administration, In the Matter of Developing the Administration's Approach to Consumer Privacy, Nov. 9, 2018, *available at* https://www.ntia.doc.gov/files/ntia/publications/msft_response_to_ntia_privacy_rfc.pdf.

Framework. This concern underlies Microsoft's belief that the Privacy Framework must be forward-looking.

- *Consensus-driven and developed and updated through an open, transparent process*. Microsoft strongly supports the development of the Privacy Framework in an open process.

- *Readily usable as part of any enterprises' broader risk management strategy and processes*. Microsoft strongly supports this attribute. Microsoft believes privacy risk management should be implemented as part of the broader information security risk management system and has done so in our business. This allows harmonization and streamlining across risk management operations.

2. *Existing standards*[32]

Microsoft believes the Privacy Framework should incorporate a range of voluntary existing standards including:

- *Cybersecurity Framework.* As described above, Microsoft believes the Cybersecurity Framework should be a model for the new Privacy Framework.

- *ISO/IEC standards*.

  - *ISO/IEC 27000 family of standards.* The latest member of this family, ISO/IEC 27552 defines a privacy information management system based on and as the extension of, ISO/IEC 27001 and 27002. In this way, it builds on the existing standards and adds privacy controls to the existing information security controls. That approach allows organizations that have already standardized around ISO/IEC 27001 and 27002 to extend their existing investments to address privacy, as part of the overall information security management system framework they have developed. In addition, ISO/IEC 27018 addresses controls for data processors. The new Framework should be compatible with these standards. Compatibility may be achieved by mapping between the controls in ISO/IEC 27552 and the new Framework. This will demonstrate to businesses that the frameworks are compatible and that they will not need to invest in separate incomparable efforts to address both approaches.

  - *ISO/IEC 20889.* Microsoft uses this standard as a foundational guide for enhancing de-identification technologies. It is an essential component of the toolbox for data processing for the purpose of privacy protection. Having clear definitions and common understanding about de-identification methods as described by this international standard is an essential requirement for achieving interoperability with various privacy regimes worldwide.

  - *ISO/IEC 19944*. Microsoft uses this guidance in handling personally identifiable information, as it describes a taxonomy of digital data and contains a data use

[32] This section responds to RFI questions 10, 12, and 21.

statement structure. These types of data use statements, especially when it involves the use of de-identified data to various degrees, allow for more precise description of data use and processing. Such statements provide more clarity and certainty for customers. In addition, clauses 8, 9, and 10 provide data categories and data use grammar.

- *ISO/IEC 19941*. This international standard comprehensively covers nuances of interoperability and portability, with a deep emphasis on data portability for customers of online service providers. A framework for privacy of users of digital services would strongly benefit by considering the nuances of data portability described in this standard. Microsoft follows the portability of user data in digital online services in this guidance.

- *ISO/IEC 19086*. Part 1 describes a list of components for consideration in cloud services agreements. Part 4 focuses on security and privacy. Together they provide a helpful checklist for topics, issues and concerns that the customers of digital services need to keep in mind, along with proposed approaches for addressing those concerns. Security and privacy concerns are addressed in part 4 of this international standard.

- *NIST guidance*.

  - *NIST 800-53 - Security and Privacy Controls for Information Systems and Organizations*. This guidance establishes mandatory controls or federal information systems and organizations, but can be implemented within any organization or information system that processes, stored, or transmits information. Microsoft uses this guidance for privacy and security.

  - *NIST 8062 - An Introduction to Privacy Engineering and Risk Management in Federal Systems*. This guidance lays the groundwork for other guidance on how federal agencies may incorporate privacy as an attribute of trustworthy systems through managing it as a collaborative, interdisciplinary engineering practices and provides a roadmap for evolving preliminary concepts of privacy engineering into actionable guidance.

  - *NISTR 8228 - Considerations for Managing Internet of Things Cybersecurity and Privacy Risks*. This guidance identifies high-level considerations that may affect the management of cybersecurity and privacy risks for IoT devices, as compared to conventional IoT devices and identifies three high-level risk mitigation goals.

  - *Encryption, cryptography, and identity management*. In addition to the specific guidance identified above, the Framework should recognize and incorporate NIST's extensive work on encryption, cryptography, and identity management, which are the subject of both international standards and NIST guidance.

VII. Conclusion

Microsoft appreciates the opportunity to provide these comments to assist NIST in the development of the Privacy Framework. Microsoft appreciates NIST's commitment to developing the Privacy Framework through a consensus-driven, open, and collaborative process that includes workshops and other opportunities for input. Microsoft would welcome opportunities to work with NIST, and with the Department of Commerce more broadly in considering how to address the important privacy issues raised by the Privacy Framework.

Respectfully submitted,

Jason P. Matusow
General Manager
Microsoft Corporation

January 14, 2019