Microsoft's Response to Request for Comment
Department of Commerce, National Telecommunications and Information Administration

The Benefits, Challenges, and Potential Roles for Government in Fostering the Advancement of the Internet of Things

I. Introduction

Microsoft Corporation ("Microsoft") appreciates the opportunity to provide comments to the U.S. Department of Commerce ("Commerce") and specifically the National Telecommunications and Information Administration ("NTIA") in response to its request for comments on the benefits, challenges, and potential roles for the government in fostering the advancement of the Internet of Things ("IoT").

As a global technology company, Microsoft is a provider of the hardware, software, and cloud services that power IoT. Through the technological phenomenon of IoT, real objects can now interact with software code and perform actions that improve the daily lives of consumers, enable greater efficiency in enterprises, and empower new approaches to governmental functions.[1] At Microsoft, we help our customers connect, monitor, and manage millions of devices and related assets, and we power the cloud services that help organizations unlock the value of new business models that are possible only through the combination of connected devices, machine learning, and big data analytics. The broad diversity of our offerings gives us a unique—and, we believe, uniquely balanced—perspective on the issues raised by NTIA.

Microsoft commends NTIA for opening up these technology policy questions from an interdisciplinary perspective and for engaging with the private sector on these important issues. NTIA can draw from its work with the private sector on related topics, including through the 2010 creation of the Internet Policy Task Force ("IPTF"), which identifies policy and operational issues impacting the private sector's ability to grow jobs through the Internet,[2] and the 2015 establishment of the Digital Economy Board of Advisors, which ensures the agency regularly receives advice from leaders in industry, academia, and civil society.[3]

Microsoft encourages NTIA, Commerce and the federal government to more broadly to support efforts that will advance consumer and enterprise trust in IoT technology and help IoT realize its full potential. The government should encourage efforts to address potential security concerns with IoT technologies through proven practices; modernize privacy frameworks to fit IoT scenarios; encourage open, voluntary, consensus-based, and globally-relevant standards that

[1] *See* Microsoft, Microsoft HoloLens and the Internet of Things. Two Sides of the Same Coin? available at https://blogs.msdn.microsoft.com/premier_developer/2015/02/09/microsoft-hololens-and-the-internet-of-things-two-sides-of-the-same-coin.

[2] *See* Department of Commerce, National Telecommunications and Information Administration, Notice of Inquiry, Information Privacy and Innovation in the Internet Economy, April 23, 2010, available at https://www.ntia.doc.gov/legacy/frnotices/2010/FR_PrivacyNOI_04232010.pdf.

[3] *See* Department of Commerce, National Telecommunications and Information Administration, Notice of Establishment and Call for Nominations to Serve on Digital Economy Board of Advisors, Nov. 27, 2015, *available at* https://www.ntia.doc.gov/files/ntia/publications/fr_deba_notice_11272015.pdf.

foster greater interoperability; and engage internationally about IoT issues. Specifically, Microsoft believes that public policies affecting IoT development should recognize and emphasize the following:

- Best practices for IoT cybersecurity that are appropriately addressed by key actors in the IoT ecoystem.
- Modernization of traditional privacy frameworks, such as the "notice and consent" framework to increase the focus on transparency, context, and consumer expectations for scenarios where notice and consent are impractical.
- Support for industry efforts to develop open, voluntary, consensus-based, and globally-relevant standards that promote innovation and preserve interoperability, to ensure new IoT systems and legacy technology systems can work together.
- International engagement that takes into account other countries' IoT strategies and initiatives as well as international trade commitments.

Ultimately, IoT may benefit from the creation of a Federal interagency task force that can coordinate with existing organizational bodies to foster balanced perspectives among security, economic benefits, and potential risks. NTIA, Commerce, and the federal government more broadly may also consider convening and facilitating a government and industry standing body that can coordinate, collaborate and leverage industry IoT consortia. In addition, the Office of Science and Technology Policy should review current research and development investment, and recommend future research and development funding for fundamental IoT security challenges.

II. Framework For Considering Challenges and Opportunities Posed by the Internet of Things (IoT)

A. The "Internet of Things" Describes a New Phenomenon in Global Connectivity.

IoT is a new technological phenomenon unlike prior technological advances.[4] IoT surpasses the confines of traditional computer networks and establishes connections directly with objects in the physical world. IoT is again revolutionizing our ability to leverage technology—but on a far larger scale.

IoT is distinct from historical IT advancements because of the scale of its potential reach, in terms of the number of devices, the scope and demographic span of deployments, the heterogeneity of systems, and the technical challenges of deployment into new and potentially unsecure environments.[5] While estimates vary, it is believed that in five years there may be up

[4] This section is in response to RFC at 1a, 1b, 2, and 4 (regarding defining IoT, classifying IoT, and identifying the new technological and policy challenges presented by IoT).

[5] *See* The President's National Security Telecommunications Advisory Committee, NSTAC Report to the President on the Internet of Things, Nov. 19, 2014 ("NSTAC Report") at 2.1, available at: https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf.

to 50 billion IoT devices deployed.[6] If that level is reached, IoT devices will be more than eight times as ubiquitous as mobile phones, which have approximately six billion devices in use.[7]

Market forces driving IoT growth show no signs of slowing down; thus NTIA's inquiry is both timely and highly relevant. Market analysts have highlighted four factors driving the growth and development of IoT: (1) reduced cost of Internet-connected sensors, which are a critical input into IoT functionality; (2) increased investment in IoT-focused companies and technologies, including acquisitions by major corporations; (3) growth in global Internet connectivity, which is anticipated to double from two billion Internet users globally in 2015 to four billion by 2025; and (4) significant adoption of mobile devices, such as tablets and smartphones, which are often used to manage IoT devices.[8] In addition to these factors, cloud service continue to mature in capability and overall sophistication, which in turn enables the collection, storage, and processing of data collected through IoT devices.[9]

The core concept of this phenomenon is that IoT allows for "things" to connect to the Internet, ranging from the significant—airplanes, elevators, solar panels, medical equipment—to the mundane—toys, soap dispensers, and countless other examples. Connected devices hold new benefits for consumers, the public sector, and private industry through unforeseen uses, increased efficiencies, security and warning capabilities, and improved reliability and resilience of the devices, underlying networks, and infrastructure.

Still, IoT is surrounded by definitional challenges. There is no universally agreed-on definition of IoT, just as there is not universal agreement that the phenomenon itself is named IoT.[10] Rather than defining IoT narrowly, in a manner that may limit the scope of its potential applications, we urge NTIA to consider recognizing that the term IoT does not simply describe a new type of technical architecture, but a new concept that defines how we interact with the physical world.

At a high level, IoT has been described as referring to a decentralized network of objects, applications and services that can sense, log, interpret, communicate, process, and act on a variety of information, scenarios, or control devices in the physical world.[11] IoT networks generally share three common principles:

[6] *See* Dave Evans, Cisco Internet Bus. Solutions Grp., The Internet of Things: How the Next Evolution of The Internet is Changing Everything 3 (2011), *available at* http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

[7] *See* NSTAC Report at 2.1.

[8] *See* Business Insider, Here Are The Four Key Elements That Will Make The "Internet of Things" an Absolutely Massive Market, Dec. 3, 2014, *available at* http://www.businessinsider.com/four-elements-driving-iot-2014-10

[9] *See* NSTAC Report at Executive Summary.

[10] *See* NSTAC Report at 2.1 (noting that the phenomenon we know as IoT may also be called the Industrial Internet or Cyber-Physical Systems); Federal Trade Commission, Internet of Things, Privacy & Security in a Connected World, January 2015 at 5 (noting that while the term IoT first appeared in literature in 2005, "there is still no widely accepted definition.").

[11] *See* NSTAC Report at 1.0.

> (1) ordinary objects are instrumented such that objects within a network can be addressed individually;
>
> (2) the physical objects are interconnected by way of a shared platform (e.g., Microsoft's Platform-as-a-Service cloud offering called the Azure IoT Suite); and
>
> (3) the devices are "intelligent" or "smart" in that they transmit and receive information related to their use, which can lead to the devices performing functions adaptively through cloud-powered machine learning and big data analysis.[12]

As IoT grows, smart devices will become ubiquitous and, in some cases, essentially invisible to humans that interact with them. These smart devices will touch all aspects of our lives, creating new and unknown dependencies. This presents a number of technological challenges, because IoT networks often involve a vast proliferation of devices, exhaustive volumes of data created by those devices, a presumption that IoT devices will likely communicate with each other, and a blurring of the roles and functions between traditional Information Technology ("IT") and Operational Technology ("OT") environments.[13]

Data is both a critical input to—and a by-product of—IoT networks. Data aggregation and big data analytics will allow individuals and organizations to leverage data for innumerable uses, such as improving the performance of their IoT deployments and informing organizational practices outside of the IoT realm. However, this data may also become a new focal point for security attacks and/or privacy compromises. Because IoT straddles classic IT and OT functionality, addressing such threats through data and devices requires development of a common set of practices and hybrid processes that recognize and assess the technologies involved.[14]

B. Policy Perspectives on IoT Should be Driven by IoT Deployment Scenarios

Policies that relate to IoT should be rooted in consideration of real-life examples about how the technology is actually deployed.[15] Through Microsoft's experience in the IoT ecosystem, we have participated in a number of innovative IoT deployments in the government and public sector, enterprises, and at the consumer level.

Governments and public sector organizations are already undertaking initiatives that use IoT to empower cities to be more sustainable, prosperous, and economically-competitive, thereby allowing citizens to lead safer, healthier and more educated lives. In Germany, the Urban Institute is a software and consulting company working on smart city solutions. Leveraging the Azure IoT Suite, the Institute has built a multi-faceted IoT platform called Urban Pulse, which

[12] *See* NSTAC Report at 2.1.

[13] For example, an industrial manufacturer that uses Internet-connected sensors to monitor production its facilities would need to simultaneously manage both Information Technology (IT) (e.g. smart device sensors) and Operational Technology (OT) (e.g., process control board) in a harmonized manner.

[14] *See* NSTAC Report at 2.2.1.

[15] This section is in response to RFC at 1c (significant new opportunities or benefits created by IoT) and 28 (additional issues not raised in RFC).

brings together city-wide devices, sensors and infrastructure to translate diverse data into actionable intelligence.[16] In the critical infrastructure space, Nav Canada, a privately-run not-for-profit corporation that owns and operates Canada's civil air navigation system, uses IoT technology powered by Microsoft to track planes and send a constant stream of data while in flight. This creates new insights and efficiency that benefit aviation more broadly by reducing flight delays and improving air traffic safety.[17]

Enterprises are also realizing new efficiencies through IoT. For example, industrial automation firm Rockwell Automation uses the Azure IoT Suite to automate the collection and analysis of data from remote installations across its petroleum supply chain.[18] Elevator company ThyssenKrupp continues to work with Microsoft to create a connected, intelligent line of sensors that monitor millions of elevators around the world in real time, allowing the company to improve maintenance and building efficiency.[19] Similarly, Gojo, maker of Purell antibacterial hand sanitizer, uses IoT technologies to detect the number of hand-washing opportunities at hospitals, with the goal of increasing sanitization and reducing infection.[20]

IoT also impacts individual consumers. Microsoft is working with Care Innovations to provide remote care management solutions, including using IoT devices to collect patient data discretely through motion sensors installed in a residence or care facility, helping people with chronic health conditions live more independently.[21] In Tanzania, Uganda, and Kenya, M-KOPA is using IoT devices powered by Microsoft to provide users affordable on-demand power via sensors, solar panels, and mobile payment apps, in regions where children previously did homework by candlelight.[22] The Microsoft Band enables individuals to track aspects of their physical life, providing data so that users can meet fitness goals, sleep targets, or even ensure they don't sit still too long.[23] The possibilities will only continue to evolve and increase.

The common themes across these examples are the reliance on a free flow of data, the relevance of machine learning, and the importance of big data analytics.[24] For IoT innovations to thrive, data must be able to flow not only within the IoT network but also, in many cases, back to the cloud platform that hosts the network. Likewise, an IoT-powered device must be capable of

[16] *See* Smart Cities Council, Making Urban Data Usable Via Cloud Technology, available at http://smartcitiescouncil.com/resources/making-urban-data-usable-cloud-technology.

[17] *See* Microsoft, Azure IoT Technology Helps NAV CANADA Revolutionize Air-Traffic Control, available at http://blogs.microsoft.com/iot/2016/03/17/azure-iot-technology-helps-nav-canada-revolutionize-air-traffic-control.

[18] *See* Microsoft, Moving From Insight to Action with Azure IoT Services, available at https://www.microsoft.com/en-us/server-cloud/customer-stories/rockwell-automation.aspx.

[19] *See* Microsoft, Giving the World's Cities a Lift with IoT, available at https://www.microsoft.com/en-us/server-cloud/customer-stories/Thyssen-Krupp-Elevator.aspx.

[20] *See* John Patrick Pullen, How Microsoft is Helping Make Hospitals Cleaner, TIME, Nov. 18, 2015, updated Nov. 20, 2015, available at http://time.com/4118499/microsoft-hospitals-study.

[21] *See* Microsoft, Customer Solution Case Study, available at https://customers.microsoft.com/Pages/Download.aspx?id=21581.

[22] *See* M-Kopa Solar, More Data. More Intelligence. More Power, available at http://solar.m-kopa.com/about/our-technology.

[23] *See* Microsoft, See What's New With Microsoft Band, available at https://www.microsoft.com/microsoft-band/en-us.

[24] This section is in response to RFC at 28 (asking about additional issues not raised by the RFC).

transmitting and receiving information related to its use, and in many cases adapting its performance based on information received from the larger IoT network.[25] Finally, the underlying IoT platform must be able to process and analyze immense volumes of data and deliver actionable insights both to the human network operators and, in many cases, the other machines connected to that network.

III. Trust Pillars for IoT Growth: Security, Privacy, Standards and Interoperability, and International Engagement

A. IoT Growth Depends on Trust in Technology

Microsoft believes that people will not use technology that they do not trust, and a common concern about IoT is that connected devices and underlying services may be untrustworthy.[26] There are extensive reports of innovative IoT use cases that have been compromised due to unanticipated threats. For example, in the consumer market, repeated hacking of connected cars has attracted media[27] and legislative attention,[28] and security and privacy failures in home video systems have prompted FTC action.[29] Hacking of IoT devices is a now a feature at major security research conferences.[30]

To ensure that consumers around the world trust in IoT technology, the Commerce and, more generally, the federal government should support efforts to increase security of IoT networks and devices generally and to ensure an adequate security baseline addresses all IoT elements. In addition, it should modernize privacy frameworks to respond to IoT innovations, encourage standards that support interoperability, and pursue international engagement on these important issues.

B. Best Practices for Cybersecurity Differ Across the IoT Ecosystem

The cybersecurity issues IoT faces are in some ways similar to cybersecurity issues faced decades ago when the protocols governing the Internet were developed, in that security has not been a significant consideration for many IoT companies.[31] Each element of the IoT ecosystem has the potential to introduce additional security risks, and new IoT devices and systems are

[25] *See* Microsoft, Creating the Internet of Your Things, available at https://www.microsoft.com/en-us/server-cloud/internet-of-things/.

[26] This section is in response to RFC at 15 (main policy issues affected by IoT).

[27] *See* Andy Greenberg, Hackers Remotely Kill a Jeep on the Highway—With Me In It, Wired, July 21, 2015, available at https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway.

[28] *See* Sen. Ed Markey, Sens. Markey, Blumenthal Introduce Legislation to Protect Drivers from Auto Security, Privacy Risks with Standards & "Cyber Dashboard" Rating System, available at http://www.markey.senate.gov/news/press-releases/sens-markey-blumenthal-introduce-legislation-to-protect-drivers-from-auto-security-privacy-risks-with-standards-and-cyber-dashboard-rating-system.

[29] *See* Federal Trade Commission, FTC Approves Final Order Settling Charges Against TRENDnet, Inc., available at https://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc.

[30] *See* Kelly Jackson Higgins, Information Week, Internet of Things Hacking Village Debuts at DEF CON, July 13, 2015, available at http://www.darkreading.com/endpoint/internet-of-things-hacking-village-debuts-at-def-con/d/d-id/1321281.

[31] *See* NSTAC Report at 4.0. This section is in response to RFC at 16 (cybersecurity issues posed by IoT).

being deployed at a rate faster than those risks can be understood.[32] The diversity of deployment models, heterogeneity of devices and interconnected networks, and sheer number of devices across sectors globally present unprecedented security challenges. Moreover, many connected devices will be deployed into environments with older legacy systems that cannot be easily managed and updated, and they may fall under multiple regulatory jurisdictions with different requirements, or into consumer environments with fewer resources for significant security management.[33]

Effective IoT cybersecurity requires organizations to adopt a rigorous security-in-depth strategy, and consumerization models to support these capabilities for end users. Starting from securing data in the cloud, to protecting data integrity while in transit over the public internet, and providing the ability to securely provision devices, each layer builds greater security assurance and trust in the overall infrastructure. This security-in-depth strategy can be developed and executed with active participation of core players involved in the IoT ecosystem.

Cybersecurity policy should account for the roles of major IoT ecosystem players and determine appropriate security practices for each role. At a high level, the IoT ecosystem depends on manufacturers/integrators, developers, deployers, and operators. Microsoft's experience with IoT networks and devices has helped us to identify and support best practices relevant to each of these roles that can improve cybersecurity across the IoT ecosystem.[34] The roles and recommended practices below are intended to demonstrate to NTIA and other policymakers that different elements of the IoT ecosystem have a broad and diverse range of cybersecurity concerns. These examples are not intended as direct recommendations for policy initiatives, but may have utility in public outreach initiatives promoting best practices on cybersecurity (e.g., the FTC's "Start with Security" campaign). Moreover, considering best practices for each of these roles can be useful to policymakers trying to understand the complexity of the IoT ecosystem and how security responsibilities are distributed across it.

> <u>IoT hardware manufacturer/integrator</u>: Typically, these entities manufacture hardware being deployed into IoT systems, or integrate and assemble hardware from various manufacturers, or supply hardware for an IoT deployment manufactured or integrated by other suppliers. For these entities, best practices include:

- *Scope hardware to minimum requirements*: Hardware should be designed to include the minimum features required for its operation, and nothing more. For example, USBs should be included in hardware only if they are required for the operation of the device. Additional features such as USBs open a device to unwanted attack vectors, which should be avoided.

- *Make hardware tamper proof*: Build in mechanisms to detect physical tampering of hardware, such as opening of a device cover or removing a part of the device. Tamper

[32] *See* NSTAC Report at 2.2.1.4.

[33] *See* NSTAC Report at Appendix E.

[34] *See* Microsoft Azure, Internet of Things Security Best Practices, April 5, 2016, available at https://azure.microsoft.com/en-us/documentation/articles/iot-security-best-practices.

signals may be part of a data stream that is uploaded to the cloud, enabling a cloud system to alert an operator of potential tampering.

- *Build around secure hardware*: If the business model permits, build security features such as secure and encrypted storage and Trusted Platform Module-based boot functionality into the hardware. These features make devices more secure, protecting the overall IoT infrastructure.

- *Make upgrades secure*: Upgrading firmware during a device's lifetime is inevitable. Devices should be built with secure paths for upgrades and cryptographic assurance of firmware version to allow devices to be secure during and after upgrades.

IoT solution developer: These entities are responsible for developing IoT solutions and may be an in-house team, or a System Integrator specializing in this activity. The IoT solution developer can create various components of the IoT solution from scratch, integrate off-the-shelf or open source components, or adopt pre-configured solutions with minor adaptation. For these entities, best practices include:

- *Follow secure software development methodology*: Developing secure software requires thinking about security from a project's inception through its implementation, testing, and deployment. The choice of platforms, languages, and tools are all influenced with this methodology.

  At Microsoft, the Microsoft Security Development Lifecycle ("SDL") provides a step-by-step approach to building secure software. This software development process helps developers build more secure software and address security compliance requirements while reducing development cost.[35] Microsoft created the SDL more than ten years ago as means to ensure a consistent approach to security practices across the thousands of software engineers that develop products and online services. It has been since been adapted and implemented at companies like Adobe[36] and Cisco.[37]

  The SDL's holistic approach to secure software development can also be applied by smaller development teams working on IoT software. Indeed, Microsoft publishes SDL implementation guidance specific to Agile development practices.[38]

- *Choose open source software with care*: Open source software provides an opportunity to quickly develop solutions. When choosing open source software, consider the activity level of the community for each open source component. An active community ensures software will be supported and that issues will be

[35] *See* Microsoft, Security Development Lifecycle, available at https://www.microsoft.com/en-us/sdl.

[36] *See* Microsoft, Cyber Trust Blog, Microsoft & Adobe: Protecting Our Customers Together, June 17, 2009, available at https://blogs.microsoft.com/cybertrust/2009/06/17/microsoft-adobe-protecting-our-customers-together.

[37] *See* Cisco, The Cisco Secure Development Lifecycle: An Overview, April 5, 2010, available at http://blogs.cisco.com/security/the_cisco_secure_development_lifecycle_an_overview.

[38] *See* Microsoft, Security Development Lifecycle for Agile Development, available at https://msdn.microsoft.com/en-us/library/windows/desktop/ee790621.aspx.

discovered and addressed. Alternatively, an obscure and inactive open source software is unlikely to be supported and many issues may not be discovered.

- *Integrate with care*: Many software security flaws exist at the boundary of libraries and application programming interfaces ("APIs"). Functionality that may not be required for current deployments may still be available via an API layer. Ensuring that all interfaces of components being integrated are secure ensures overall security.

IoT solution deployer: Once an IoT solution is developed, it needs to be deployed in the field. Entities that act as IoT solutions deployers are responsible for the deployment of hardware, interconnection of devices, and deployment of solutions in devices, or in the cloud. For these entities, best practices include:

- *Deploy hardware securely*: IoT systems may require hardware to be deployed in unsecure locations, such as public spaces or unsupervised locales. In such situations, ensure that hardware deployment is tamper proof to the maximum extent possible. If USB or other ports are available on the hardware, ensure they are covered securely. Many attack vectors can use these as entry points for attacks.

- *Keep authentication keys safe*: During deployment, each device requires device identifiers and associated authentication keys generated by the cloud service. Keep these keys physically safe even after deployment. Any compromised key can be used by a malicious device to masquerade as an existing device.

IoT solution operator: Post-deployment, IoT solutions require long term operations, monitoring, upgrades, and maintenance. Entities acting as IoT solutions operators may be an in-house team comprising information technology specialists, hardware operations and maintenance teams, and domain specialists who monitor the correct behavior of overall IoT infrastructure. For these entities, best practices include:

- *Keep system up to date*: Ensure device operating systems and all device drivers are updated to the latest versions. Windows 10, with automatic updates turned on, is kept up to date by Microsoft, providing a secure operating system for IoT devices. For other operating systems, such as Linux, it is important to keep the operating systems up to date to ensure they are protected against malicious attacks.

- *Protect against malicious activity*: If the operating system permits, place the latest anti-virus and anti-malware capabilities on each device operating system. This can help mitigate most external threats. Modern operating systems, such as Windows 10 IoT[39] and Linux, can protect against this threat by taking appropriate steps.

- *Audit frequently*: Auditing IoT infrastructure for security related issues is key when responding to security incidents. Most operating systems, such as Windows 10, provide built-in event logging that should be reviewed frequently to confirm no

[39] *See* Microsoft, Windows 10 for the Internet of Your Things, available at https://www.microsoft.com/en-us/WindowsForBusiness/windows-iot.

security breach has occurred. Audit information can be sent as a separate telemetry stream to the cloud service and analyzed.

- *Physically protect the IoT infrastructure*: Protecting against malicious use of USB ports and other physical access is an important safety and security practice. Logging of physical access, such as USB port usage, is key to uncovering any breach that may have occurred. Again, Windows 10 enables detailed logging of these events.

- *Protect cloud credentials*: Cloud authentication credentials used for configuring and operating an IoT deployment are possibly the easiest way to gain access and compromise an IoT system. Protect the credentials by changing the password frequently, and not using these credentials on public machines.

C. IoT Growth Should Catalyze the Modernization of Privacy Frameworks

IoT raises unique privacy concerns.[40] IoT will dramatically increase the number of devices facilitating the creation, collection and transmission of data. In parallel, IoT devices without screens or other direct user interfaces, create significant practical challenges for privacy regimes based primarily on notice and consent. To address these unique privacy challenges, traditional privacy frameworks must be modernized.

To support novel IoT scenarios traditional "notice and consent" privacy framework should evolve to increase emphasis on transparency and user control. The notice and consent framework was built on premise that users can be given comprehensive information about an organization's privacy practices at a point in time before data is collected, as well as an opportunity to consent to those practices. The framework makes sense for many applications, but it does not translate well to applications of ambient collection where many IoT objects have a limited ability to display traditional notices or collect traditional consents.

Rather than abandoning notice and consent, these concepts should be strengthened and reapplied for the 21st century. For example, an increased focus on transparency and individual control would extend the concepts of notice and consent to the IoT space. Instead of focusing on "notice" as a one-time, one-way disclosure, "transparency" can extend this concept through continuous activity involving both the data collector and the individual. In addition to static privacy notices, companies involved in IoT should look for additional ways to be forthcoming about the data they collect and how they will use it. For example, IoT devices can use online dashboards, apps, customer support, "just in time" notices and notices in the real world to increase transparency about data practices.

Aligning IoT data collection and use with both the context of the collection and with consumer expectations will also help manage privacy concerns associated with IoT. These principles suggest that companies may engage in certain data practices without offering consumer choice if the collection or use of data is either obvious from the context of the transaction, sufficiently accepted or necessary for public policy reasons. By emphasizing context and consumer

[40] This section is in response to RFC at 17 (privacy concerns relating to IoT).

expectations, privacy frameworks can encourage companies to base decisions about data collection and use on the reasonable expectations of their users.

New data protection frameworks should reflect 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 for new data protection frameworks to easily be applied to current and future technology, supporting both privacy goals and innovation. For example, a law focusing on outcomes can allow companies to meet requirements in different ways depending on how their service operates. By contrast, a law requiring a specific type of check-the-box consent may be unattainable for IoT technologies that do not have screens at all.

Microsoft is an active innovator in the IoT space. We know one of the most significant barriers to adoption of new technologies, like IoT, is a lack of consumer trust. When consumers know there are robust laws protecting their privacy, they will come to new innovations like IoT with greater confidence and adapt the technologies more rapidly. Microsoft has long been a strong supporter of baseline privacy legislation—and of robust enforcement for those that breach that legislation—for exactly this reason. People need to have faith that the rules are being followed s they embrace IoT and other new technologies. Modernizing privacy frameworks for IoT to ensure strong privacy protections will help ensure these innovations thrive.

D. Successful Development of an IoT Marketplace Depends on Standards and Interoperability

The development of open, voluntary, consensus-based, and globally-relevant standards is a major driver of a robust and competitive IoT marketplace.[41] Standards are particularly crucial for IoT because standards provide the basis for interoperability, which is needed to ensure that new IoT systems and legacy technology systems can work together. Standards development organizations ("SDOs"), national initiatives, and industry consortia in a broad range of market segments are identifying new and in some cases unique requirements for IoT standards reflective of their current and evolving market needs. These standards range from overarching guidelines to specific technical protocol criteria that help to ensure increased interoperability in IoT networks.

Collaboration with industry is key to the development of any new IoT standards. Openness and interoperability between hardware, software, and services will help both enterprises and government transform how they operate. Microsoft is working to achieve such interoperability through several IoT SDOs and consortia. Our IoT standards development work has been driven through engagement in standards organizations such as the Internet Engineering Task Force, Object Management Group, Open Connectivity Foundation, Open Mobile Alliance, Organization for the Advancement of Structured Information Standards, and consortia such as the Industrial Internet Consortium and OpenFog. While some of the organizations are industry focused and some are horizontally focused, our work centers on standards for IoT devices, on the establishment of open and interoperable technologies and interfaces, IoT security, device

[41] This section is in response to RFC at 6 (technological issues hindering development of IoT) and 20 (international engagement).

management, and semantic integration of information that flows between clouds, endpoints and services.

Standards for IoT must reflect the fact that IoT relies on functions that are both traditionally IT and traditionally OT. Standards organizations should therefore be developing when necessary and adopting when available OT and IT aligned reference models, architectures and open interfaces for IoT. For example, in the case of Smart Manufacturing, existing standards alone are insufficient to fully enable Smart Manufacturing especially in the areas of cybersecurity, cloud based manufacturing services, supply chain integration, and data analytics. Today, there are a number of existing standards that must be considered in an integrated fashion to enable Smart Manufacturing: ISO/IEC 27000 (information security); ISO/IEC 28000 (supply chain security); and IEC 62433 (industrial control systems and automation). Looking forward, industry-led initiatives hold the most promise for overcoming such complexity.

The partnership between the U.S. federal government and some standards organizations has been long-standing and successful. For example, the Office of Management and Budget has directed agencies to use voluntary consensus standards in lieu of government-unique standards, unless doing so is inconsistent with law or impractical.[42] In doing so, the government recognizes that harmonizing standards between government and industry encourages long-term growth for U.S. enterprises, promotes efficiency, and provides incentives and opportunities to establish standards that serve national needs.[43] These collaborative efforts should continue in considering IoT.

In a similar vein, it is important to consider the role of intellectual property in IoT innovation. In recent comments[44] filed in connection with an ongoing U.S. Copyright Office (the "Office") study on copyright and software embedded in consumer products, Microsoft urged the Office to proceed with caution before recommending changes that would alter copyright protection for software embedded in consumer products, including always-connected IoT devices. In our view, the evidence is overwhelming that software innovation—including in embedded software—is flourishing and that consumers and the public are benefitting enormously. By contrast, there is remarkably little evidence that copyright protection for software embedded in consumer products is causing any systemic problems.

Indeed, when Commerce's IPTF recently completed its 2016 study on novel copyright issues in the digital economy, it found the U.S. copyright regime to be sufficiently flexible to adapt to the evolution of software in consumer products, and therefore did not recommend any change to existing copyright protections for such software.[45] At this time, there is no reason to believe that a different regime would be more effective in spurring innovation or at balancing the interests of creators, users, and the public. Businesses of all sizes and across numerous sectors of our economy today rely on the certainty that the existing copyright system provides for embedded

[42] *See* Office of Management and Budget, Circular A-119, Revised Feb. 10, 1998.

[43] *Id.*

[44] *See* Initial Comments of Microsoft Corporation (Feb. 16, 2016), available at*:* https://www.regulations.gov/#!docketBrowser;rpp=25;po=0;dct=PS;D=COLC-2015-0011

[45] *See* Department of Commerce, Internet Policy Task Force, *White Paper on Remixes, First Sale, and Statutory Damages,* 64 (2016), available at: http://www.uspto.gov/sites/default/files/documents/copyrightwhitepaper.pdf.

software. Even the potential for changes to that system could deter investment and innovation, as inventors and companies seek to avoid even the risk that they may be unable to recoup their investments in software development.

This is not to say that tensions in the system never arise. But when they do, existing provisions in the Copyright Act, combined with agency rulemaking, judicial interpretations, and voluntary private-sector efforts have proven up to the task of maintaining the appropriate balance.

E. International Engagement Should Be Informed by National Strategies and International Trade Commitments

1. National Strategies for IoT Are Emerging Globally

Governments around the world are developing IoT strategies and similar national initiatives to propel their engagement in the IoT marketplace.[46] The U.S. government should study other countries' strategies and initiatives to inform its international engagements related to IoT.

Overarching frameworks that support responsible growth and anticipate future challenges are common in national IoT-related strategies. With this global policy wave in its first stages, the first-movers for strategic approaches to IoT have been major producers and consumers of IoT technologies in Europe and Asia, such as the United Kingdom,[47] South Korea,[48] India,[49] and Malaysia.[50] Similarly, several countries have launched initiatives to utilize the transformation that IoT brings to their domestic industry. For instance, Germany[51] has established a platform in which the industry collaborates to drive domestic adoption of IoT, whereas France[52] and the Netherlands[53] have identified roadmaps and action agendas to support the industrial renewal in their countries.

While the scope of those policies is very broad, they tend to emphasize the following areas, many of which mirror the policy areas highlighted by Commerce in the RFC:

[46] This section is in response to RFC at 20 (international engagement).

[47] *See* Government Office for Science, Government of the UK, *The Internet of Things: making the most of the Second Digital Revolution*, *available at* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf.

[48] *See* Ministry of Science, ICT and Future Planning, Government of South Korea*, Master Plan for Building the Internet of Things (IoT)*, *available at* https://www.rfid-alliance.com/KOREA-IoT%20Master%20Plan.pdf.

[49] *See* Ministry of Communications & IT, Government of India, *IoT Policy Document*, Draft Version, *available at* http://deity.gov.in/sites/upload_files/dit/files/Draft-IoT-Policy%20(1).pdf.

[50] *See* Ministry of Science, Technology and Innovation, MIMOS, Government of Malaysia, *National Internet of Things (IoT) Strategic Roadmap: A Summary*, *available at* https://www.ida.gov.sg/~/media/Files/Infocomm%20Landscape/iN2015/Reports/realisingthevisionin2015.pdf.

[51] *See* Federal Ministry for Economic Affairs and Energy, Government of Germany, *Platform Industry 4.0*, *available at* http://www.plattform-i40.de/I40/Navigation/EN/Home/home.html;jsessionid=43109D17EE3D178FC02F23AF1763AF8C.

[52] *See* Government of France, *Industry of the Future*, *available at* http://www.economie.gouv.fr/files/files/PDF/pk_industry-of-future.pdf.

[53] *See* Government of the Netherlands, *Action Agenda Smart Industry*, *available at* http://www.smartindustry.nl/site/assets/files/1740/smart-industry-action-agenda-summary.pdf.

Smart manufacturing: The manufacturing sector is a key component in many national strategies for IoT. These strategies typically emphasize government-supported opportunities for IoT innovation, such as the funding of resource centers such as in India.[54] Similarly, the creation of test beds and field labs, such as in the Netherlands[55] and South Korea,[56] can create ecosystems of interrelated networks of companies and institutions to facilitate knowledge transfer across sectors.

Security and privacy: Governments, such as the United Kingdom[57] and South Korea,[58] acknowledge the importance of security and privacy issues in developing trust in IoT. The United Kingdom has published security best practices and privacy principles to support a secure and privacy-enhancing approach to IoT.[59]

Research and education: IoT will require a broad range of skills and investments in research and education to access its full potential. Human capacity building and a stronger integration of ICT into the education system are amongst the central pillars to foster innovation in the strategies of many countries, including India[60] and South Korea.[61] For instance, India will create an IoT Education and Awareness program that aims to develop the necessary skill sets for IoT in their country through the introduction of IoT curriculum at schools and universities as well as public awareness programs with the industry and academic institutions. India also envisions IoT education exchange programs with other countries to facilitate bilateral knowledge transfers.[62] Governments also recognize that investments in research and development can lead to commercial products that expand the IOT marketplace domestically and potentially

[54] *See* Ministry of Communications & IT, Government of India, *IoT Policy Document*, Draft Version, p. 8-9, *available at* http://deity.gov.in/sites/upload_files/dit/files/Draft-IoT-Policy%20(1).pdf.

[55] *See* Ministry of Economic Affairs, Government of the Netherlands, *Action Agenda Smart Industry*, p. 2-4, *available at* http://www.smartindustry.nl/site/assets/files/1740/smart-industry-action-agenda-summary.pdf.

[56] *See* Ministry of Science, ICT and Future Planning, Government of South Korea*, Master Plan for Building the Internet of Things (IoT), p. 5*, *available at* https://www.rfid-alliance.com/KOREA-IoT%20Master%20Plan.pdf.

[57] *See* Government Office for Science, Government of the UK, *The Internet of Things: making the most of the Second Digital Revolution*, p. 10, *available at* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf.

[58] *See* Ministry of Science, ICT and Future Planning, Government of South Korea*, Master Plan for Building the Internet of Things (IoT), p. 3*, *available at* https://www.rfid-alliance.com/KOREA-IoT%20Master%20Plan.pdf.

[59] *See* Government Office for Science, Government of the UK, *The Internet of Things: making the most of the Second Digital Revolution*, p. 10, *available at* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf.

[60] *See* Ministry of Communications & IT, Government of India, *IoT Policy Document*, Draft Version, p. 13-14, *available at* http://deity.gov.in/sites/upload_files/dit/files/Draft-IoT-Policy%20(1).pdf.

[61] *See* Ministry of Science, ICT and Future Planning, Government of South Korea*, Master Plan for Building the Internet of Things (IoT)*, p. 9, *available at* https://www.rfid-alliance.com/KOREA-IoT%20Master%20Plan.pdf.

[62] *See* Ministry of Communications & IT, Government of India, *IoT Policy Document*, Draft Version, p. 13-14, *available at* http://deity.gov.in/sites/upload_files/dit/files/Draft-IoT-Policy%20(1).pdf.

internationally; the U.K. has proposed an IoT advisory board to coordinate public and private sector funding.[63]

Global interoperability: Companies will develop IoT-related devices and services domestically, but ultimately want to sell them globally. Several national strategies express support for standards intended to facilitate global interoperability, such as the U.K. [64] and South Korea.[65] Moreover, South Korea plans to enforce joint demonstration projects with major countries including the EU using the Trans-Eurasia Information Network that connects 34 European and 19 Asian countries.[66]

2. International Trade Commitments and IoT

As countries explore how to make their IoT industries more competitive, there is a risk that some may resort to protectionism. The United States should continue to leverage its international trade and investment agreements as part of its approach to IoT, in order to continue to benefit from the gains already secured, avoid undermining existing rights and obligations, ensure regulatory humility and consistency across laws and regulations, and respond to protectionist threats. Many of these provisions are enforceable through binding dispute settlement. The government's approach should take into account the progress achieved in agreements that require transparency, predictability, and nondiscrimination in the application of laws and regulations and continue these practices. Beyond binding agreements, within the interagency process, the United States Trade Representative ("USTR"), the Departments of Commerce and State, among others, have additional consultative mechanisms on trade where IoT will need to be addressed.

In addition, the introduction of IoT raises new challenges related to the collection of international trade and economic data. Conventional economic statistics do not capture the full extent to which IoT is making industries across the economy more productive. Commerce has already initiated work in this area[67] and will need to press forward with the development of new ways to measure the IoT and its impact on the economy.

[63] *See* Government Office for Science, Government of the UK, *The Internet of Things: making the most of the Second Digital Revolution*, p. 10-11, *available at* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf.

[64] *See* Government Office for Science, Government of the UK, *The Internet of Things: making the most of the Second Digital Revolution*, p. 8, *available at* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf.

[65] *See* Ministry of Science, ICT and Future Planning, Government of South Korea*, Master Plan for Building the Internet of Things (IoT)*, p. 11, *available at* https://www.rfid-alliance.com/KOREA-IoT%20Master%20Plan.pdf.

[66] *See* Ministry of Science, ICT and Future Planning, Government of South Korea*, Master Plan for Building the Internet of Things (IoT)*, p. 11, *available at* https://www.rfid-alliance.com/KOREA-IoT%20Master%20Plan.pdf.

[67] Improvement of digital economy metrics is an area of focus for Commerce's Digital Economy Board of Advisors, in which Microsoft is privileged to be taking part. Microsoft also took part in a roundtable on improving digital economy metrics convened by NTIA and the Economics and Statistics Administration in May 2016. We look forward to more opportunities going forward to help the Commerce improve its metrics of how digital technologies, including IoT, are transforming the economy.

The United States' trade and investment agreements contain provisions that should counter barriers that are especially problematic for IoT, including:

- *Barriers to cross-border data flows*. Data flows are vital for producing and delivering IoT services, and should be restricted only to the extent necessary to achieve legitimate regulatory objectives.

- *Tariff and nontariff barriers to trade in goods,* such as opaque regulations and discriminatory product standards, block trade in devices critical to the IoT ecosystem. Existing rules and disciplines in the trade area are relevant.

- *Weak protection of intellectual property* reduces the scope for development and deployment of innovative IoT technologies.

- *Discriminatory practices that favor state-owned enterprises* ("SOEs") may unfairly disadvantage private providers of IoT devices and services.

The United States should continue to leverage binding commitments in multilateral, regional, and bilateral trade agreements to break down such barriers, including:

- World Trade Organization ("WTO") agreements that contain binding rules and commitments relevant to IoT, including all the goods-related agreements (in particular provisions related to standards); the General Agreement on Trade in Services ("GATS"); the Agreement on Trade-Related Aspects of Intellectual Property Rights ("TRIPS"); and the plurilateral WTO Information Technology Agreement ("ITA"), which eliminates tariffs on many high technology goods.

- The United States' free trade agreements contain binding commitments that deepen the rule of law and eliminate barriers to trade in goods and services, including high technology products and online services. Bilateral investment treaties ("BITs") promote open, transparent and non-discriminatory treatment of private investment.

- The Trans-Pacific Partnership ("TPP") includes new digital trade provisions important for the Internet of Things,[68] new disciplines on SOEs, and commitments to cooperate on clean and more efficient energy. Agreements still under negotiation, such as the Trade in Services Agreement ("TISA") and the Transatlantic Trade and Investment Partnership ("TTIP") can build upon these gains.

- Other mechanisms enable the United States to consult with partners on ways to facilitate trade and investment, including Trade and Investment Framework Agreements ("TIFAs"), Information and Communication Technology ("ICT") Dialogues, and Commercial Dialogues. Each of these should increase their focus on IoT.

[68] *See* Office of the United States Trade Representative, The Digital 2 Dozen, available at https://ustr.gov/about-us/policy-offices/press-office/reports-and-publications/2016/digital-2-dozen.

IV. The Role of Government in IoT

Government has an important role in ensuring that IoT innovation continues.[69] To advance trust in IoT technology, the Department of Commerce and, more generally, the federal government can support existing efforts to increase interoperability, address potential security issues, ensure collaboration between the government and the private sector, and enable funding to continue IoT innovation. Specifically, Microsoft recommends that NTIA, Commerce Department, and the federal government more broadly consider the following actions:

1. *Create an IoT interagency task force that coordinates with existing organizational bodies to foster balanced perspectives between security, economic benefits, and potential risks.* At a minimum, participants should include the Departments of Commerce, Defense, Homeland Security, and Transportation, as well as the Federal Communications Commission and the U.S. Trade Representative. Such a task force can set milestones for completion of the following activities that are reflective of the urgency of need to develop policies that reflect the growing presence of IoT:

    a. Direct the update of federal strategic documents to consider the security aspects of the explosive growth of and reliance upon IoT devices. Examples include the National Strategy to Secure Cyberspace, the Comprehensive National Cybersecurity Initiative, and Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program.

    b. Direct the update of existing awareness and training programs. The focus of the awareness should be to inform the public, as well as leaders and decision makers (private and public, including legislators), about both the benefits and risks of the rapid adoption of IoT and, thereby, encourage a culture of security around IoT device use and development.

    c. Encourage and incentivize academia to develop curricula focused on: (i) IoT, and the associated security challenges; and (ii) the convergence of the IT and OT disciplines, in order to educate future IT and OT professionals engaged in the design, administration, and security of computer networks.

    d. Encourage engagement in appropriate international forums for standards and policy development.

2. *Convene and facilitate a Government and industry standing body to coordinate, collaborate and leverage the various industry IoT consortia to develop, update, and maintain IoT deployment guidelines to manage cybersecurity implications and risks.* The result should enable an adaptive set of voluntary guidelines, focused cybersecurity and resiliency of the ecosystem that changes with the risk in a timely manner based on a continuous collaborative process. The executive agent of this standing body must have authority and oversight to enforce agreed-to deployment guidelines across governmental

[69] This section is in response to RFC at 7, 25, 26, 27 (role of government).

agencies and departments. Moreover, this body must adopt an international perspective that takes into account the significant work on IoT-related standards outside of traditional SDO channels (e.g., industry consortium).

3. *Direct the Office of Science and Technology Policy to review current R&D investment and recommend future R&D funding for fundamental IoT security and cyber-physical security research.* Identify the core research challenges related to scalability, security heuristics, trust recovery, and resilience of large complex IoT systems. Identify the key next generation IoT research needs based on national priorities and ensure that resources are available to the significant needs security needs of ubiquitous connected environments with ambient intelligence and operational technology.

As recommendations are considered and implemented, it will be important to: (1) establish metrics to measure and monitor the effectiveness of the recommendations; (2) incorporate IoT technology in a manner that minimizes risk; (3) incorporate IoT in current education and awareness programs; and (4) ensure IoT-related R&D projects are addressing evolving cybersecurity challenges.

V. Conclusion

Microsoft appreciates the opportunity to provide these comments to assist the NTIA and Commerce in considering the benefits, challenges, and potential roles for government in fostering the advancement of the Internet of Things. While IoT is growing rapidly, it is important to address security, privacy, interoperability and related issues to ensure consumers, enterprises, critical infrastructures, and governments can trust IoT technologies and benefit from the opportunities IoT brings. Microsoft appreciates the government's outreach on these important issues and would welcome opportunities to work with NTIA and Commerce in considering how best to address the benefits and challenges of IoT in the future.

Sincerely,

J. Paul Nicholas

J. Paul Nicholas
Senior Director
Trustworthy Computing
Microsoft Corporation