SIIA Accelerating Innovation in Technology, Data & Media

202.289.7442 1090 Vermont Ave NW Sixth Floor
www.siia.net Washington DC 20005-4905

June 2, 2016

The Honorable Lawrence E. Strickling
Assistant Secretary for Communications and Information
U.S. Department of Commerce
Washington, DC 20230

Dear Mr. Strickling,

On behalf of the Software & Information Industry Association (SIIA), thank you for the opportunity to respond to the National Telecommunications and Information Administration's (NTIA) April 6, 2016 request for comments concerning the benefits, challenges and potential roles for the government in fostering the advancement of the Internet of Things (IoT).

The Software & Information Industry Association (SIIA) is the principal trade association for the software and digital content industries. SIIA provides global services in government relations, business development, corporate education, and intellectual property protection to the leading companies that are setting the pace for the digital age.

Introduction

Earlier this year, SIIA published a white paper, *Empowering the Internet of Things*, which provides an in-depth analysis of the technological, social and economic benefits—transformative benefits—and the challenges presented by the IoT. Based on this assessment, we also pose a series of public policy recommendations to guide policymakers seeking to enable the benefits while assessing and addressing key risks.[1]

In summary, SIIA's Report explains that the IoT represents an evolutionary technological development, encompassing a wide range of technologies, devices and platforms. Therefore, overarching policies and regulations would stifle innovation and growth. Rather, policymakers should rely heavily on the current framework which is sufficiently flexible to promote exciting new IoT innovations and enable the transformative benefits of the IoT that promise to fundamentally improve the way business is done and the way people live. Following are a set of six recommendations we pose to accomplish this objective:

1. Do not seek an overarching IoT Policy Framework. Existing laws have functioned effectively and provide substantial consumer protection, even in light of rapid technological innovation.

[1] SIIA, Empowering the Internet of Things: Benefits, Solutions and Recommendations for Policymakers, 2016.

2. Privacy rights for the IoT should be based on risk and societal benefits. Public policies must balance principles of privacy against societal values such as public health, national security, economic growth, and the environment.

3. Encourage best practices for privacy and cybersecurity. In a dynamic technological environment, new regulations risk stifling burgeoning innovation – industry best practices and self-regulatory codes of conduct provide more flexibility to evolve and adapt over time.

4. Promote technology neutrality and avoid technology mandates. These principles are especially important in IoT's complex ecosystem, which will be inherently subject to constant innovation.

5. IoT standards should be open and industry-led. Open standards are critical to combining a wide range of data sets across myriad analytics environments and applications; attempts to dictate interoperability could reduce the marketplace to a standardized set of products and services.

6. Policies for embedded software should provide for product integrity. Unrestricted ability to access and modify embedded software will threaten the reliability, safety and usability of IoT devices; product integrity is critical to the full development of the IoT's potential.

Drawing from this Report and these policy recommendations, below are detailed answers to many of the specific questions posed by the Department.

1.Are the challenges and opportunities arising from IoT similar to those that governments and societies have previously addressed with existing technologies, or are they different?

The IoT represents an evolutionary technological development. The last decade has brought about significant advances in information technology (IT), representing an evolution of IT from a specialized tool into a pervasive influence on nearly every aspect of everyday life. This rich new environment has arisen from the convergence of several technological advancements such as the increasing use of sensors, actuators, and data communications technology, and the increasing availability of pervasive analytics and the evolution towards "cloud" or remote internet computing, where data storage and processing is available as a service on demand, provided with greater efficiency and increased security.

The IoT is an enabler of data-driven innovation that will have a significant impact on the global economy today and into the future. Connecting sensors in everyday objects to computer networks is a crucial part of the IoT, but much of the value of the IoT is generated by the application of analytics to the new flow of data. In an earlier white paper on data-driven innovation, SIIA highlighted the essential role of analysis in creating numerous usable insights from data. Governments and enterprises have an increasing capacity to utilize this type of information, creating jobs and enabling economic growth on a massive scale.[2]

[2] Software & Information Industry Association. "Data-Driven Innovation: A Guide for Policymakers: Understanding and Enabling the Economic and Social Value of Data." 2013.

Therefore, given the evolutionary role of technology, the challenges and benefits in many ways are similar to those which have recently been encountered regarding cloud computing, the proliferation of mobile and social technologies and applications, and "big data." But in many ways, because the IoT represents a convergence of these IT developments, it presents many new opportunities for innovation, and sometimes new challenges.

Consumers, citizens, and society as a whole stand to benefit greatly from the IoT. The exponential increase in the availability of data from the IoT and its innovative uses have the potential to improve health outcomes, streamline and enhance financial services, strengthen education and learning, and improve our physical infrastructure. Different sectors of the economy will experience various levels of utility, but all will benefit greatly from IoT advances.

2. The term "Internet of Things" and related concepts have been defined by multiple organizations, including parts of the U.S. Government such as NIST and the FTC, through policy briefs and reference architectures. What definition(s) should we use in examining the IoT landscape and why? What is at stake in the differences between definitions of IoT? What are the strengths and limitations, if any, associated with these definitions?

As noted, there are myriad definitions of the IoT. For our purposes, SIIA refers to the IoT to describe ubiquitous interconnectivity, where people don't just interact with devices, but devices also interact directly with each other. More important than an exact definition of the IoT for policy purposes, is to recognize that the significant change is the development of the internet away from a computer-to-computer communication network into a ubiquitous network linking electronic devices and everyday objects.

3. With respect to current or planned laws, regulations, and/or policies that apply to IoT: a. Are there examples that, in your view, foster IoT development and deployment, while also providing an appropriate level of protection to workers, consumers, patients, and/or other users of IoT technologies? b. Are there examples that, in your view, unnecessarily inhibit IoT development and deployment?

The IoT is already visible across many facets of everyday life, from industrial uses, to education, smart cities and enhanced government, transportation and personal aspects, including wearables, domestic appliances and our automobiles. The issues surrounding the IoT are just beginning to be framed for public debate. The IoT is developing healthily in the presence of many well-understood legal doctrines that protect health, safety and property rights.

SIIA's overarching policy recommendation is that given the complexity of the IoT, with myriad different devices, platforms and inter-related technologies, there is no overarching policy or singular framework that could be expected to effectively apply across the board. For example, a rule that makes sense when applied in a consumer IoT context might be inappropriate when applied in a business or commercial context. Similarly, internet-connected light bulbs are very different than "wearables," which are also different from items such as connected appliances and automobiles.

With respect to existing laws, more often than not, these are continuing to function quite effectively and provide substantial consumer protection, even in light of rapid technological innovation over the

last decade—again many of the issues associated with the IoT have been debated for many years as relevant to the rise of "big data." For instance, the current U.S. sectoral approach to privacy and security serve as excellent examples of how policies can effectively protect consumers without taking a comprehensive, one-size-fits-all approach. Under the current approach, security, responsibility and accountability for data are commensurate with the associated risk. This approach is absolutely critical as we move further towards an "Internet of Everything" environment with such a diverse set of applications across so many different sectors of the economy and facets of our lives.

The goal is for a flexible policy framework, rather than a prescriptive approach, where innovation can continue to thrive, but where regulations can provide a backstop to prevent significant harm. For instance, in 2014, the FTC settled its first IoT enforcement action against TRENDnet, the maker of home security cameras deemed to provide inadequate security. The Commission alleged, and ultimately prevailed, in making the case that contrary to claims of providing secure, internet-connected home cameras, that TRENDnet cameras had faulty software that left them open to online viewing, and in some instances listening, by anyone with the cameras' Internet address.

The FTC described this settlement with TRENDnet as the agency's first enforcement action "against a marketer of an everyday product with interconnectivity to the Internet," demonstrating very effectively that new challenges presented by Internet-connected devices are not outside the scope of current regulation. Under current authority, the FTC can continue to enforce its Section 5 prohibitions against unfair or deceptive acts or practices as it pertains to the IoT, just as it has for other related technologies. In cases where entities violate the FTC's long-standing consumer protection principles, causing harm to individuals, they can and should be subject to robust enforcement.

The same is largely true with respect to copyright law. There is significant ongoing debate about the role of, and legal framework surrounding, embedded software. Indeed, IoT devices operate and connect to each other and to computer networks through software contained in the devices themselves. Manufacturers typically use technology and contract obligations to control access to these products. To the extent that laws and policies need to be clarified to address the IoT, a crucial principle that should guide this policy discussion is the need to ensure product integrity. Cars need to function as the manufacturer intended; so do airplanes and heart monitors. Unrestricted ability to access and modify embedded software will threaten the reliability, safety and usability of IoT devices. In many cases, ensuring the product's integrity will require users to abide by the terms of software licenses and other contractual terms. This principle of product integrity is critical to the full development of the IoT's economic and social potential, and it is one that existing law generally respects.

As processing power permits the creation of smaller and smaller devices, formerly "dumb" goods—whether refrigerators, thermostats or televisions-- will become appreciably smarter. It is important to recognize that the distinction between "software" and so-called "embedded software" is one that does not exist. There is only "software," and its use, licensing, and sale is governed by a body of well-established law. For example, the Computer Fraud and Abuse Act provides protection from unauthorized hacking, whether the software is "embedded" or not. Similarly, a person who causes physical harm to another by hacking a pacemaker remains subject to long-standing (and technologically neutral) criminal and civil doctrines. Such doctrines preserve product integrity exactly

because they do not create artificial distinctions. Innovation in the IoT continues to grow not in spite of these laws, but because of them. We encourage policymakers to engage in careful study before disturbing current statutory regimes, or applying new technology-specific laws or regulations.

4. Are there ways to divide or classify the IoT landscape to improve the precision with which public policy issues are discussed? If so, what are they, and what are the benefits or limitations of using such classifications? Examples of possible classifications of IoT could include: Consumer vs. industrial; public vs. private; device-to-device vs. human interfacing.

There are myriad ways to categorize various IoT technologies. From a policy perspective, there are two main categories, commercial and consumer applications. The first, industrial or commercial technologies, applies to situations where internet connected devices are advancing business and production processes. The second, commercial applications, refer to those products and services that are marketed to, and used by, consumers. These two distinctions are most important because they generally pertain to different legal situations. That is, commercial IoT solutions in general have a greater opportunity for the use of contracts between IoT providers and customers to dictate data collection and use terms. Consumers in many cases will have choices and the ability to customize data collection and use, but in other cases will not have these choices. The challenges are often greater with consumers to provide true and informed consent about data use.

Some experts have gone further to segment IoT consumer applications, for instance along the lines of "smart home" application, vehicular and wearable, etc., but we haven't identified a practical purpose to make such distinctions when assessing public policy at this time. Of course, consumer expectations are likely different among IoT applications in their home, automobiles or public consumer services. However, the current U.S. policy framework provides for greater protection of sensitive data, such as sensitive health, financial or eligibility information. IoT applications would appear to fit within this framework based on whether data is personal and the sensitivity of such data.

When assessing classifications for different IoT technologies, it is important not to make false distinctions that could be unhelpful when assessing the application of current or new public policies.

5. Please provide information on any current (or concluded) initiatives or research of significance that have examined or made important strides in understanding the IoT policy landscape. Why do you find this work to be significant?

There are a number of writings on policy considerations of the IoT, SIIA would like the highlight the several that we feel are well informed assessments of the need to focus on fostering innovation, and warning about the very real threat of over-regulation. Drawing from our experiences over the last decade talking with policymakers about emerging issues such as "cloud computing" and "big data," it is SIIA's conclusion that there is a very real threat of over-regulation as policymakers initially assume that existing policies cannot be sufficient and look for "fixes," rather than looking for new policies that could encourage innovation and economic growth. Of course, it is always important to assess potential gaps in current policy, but there shouldn't be a rush to enact new market restrictions where the current policy framework can, and does still function effectively.

- How to Regulate the Internet of Things Without Harming its Future: Some Do's and Don'ts; Remarks of Joshua T. Wright, Commissioner, FTC, May 21, 2015.

- The Internet of Things: When Things Talk Among Themselves, Remarks of Maureen K. Ohlhausen, Commissioner, FTC, November 19, 2013.

- The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation, Adam Thierer, November 2014.

- Why Countries Need National Strategies for the Internet of Things, ITIF, 2015.

6. What technological issues may hinder the development of IoT, if any? a. Examples of possible technical issues could include: i. Interoperability; ii. Insufficient/contradictory/proprietary standards/platforms; iii. Spectrum availability and potential congestion/interference; iv. Availability of network infrastructure; v. Other. B. What can the government do, if anything, to help mitigate these technical issues? Where may government/private sector partnership be beneficial?

The ability of devices to increasingly communicate with each other, and with people, is integral to the IoT, as is the ability to integrate multiple data sources and analytics to enable data-driven innovation. After all, machine-readability is the key to data analytics, and the "connectability" of data to other data. Therefore, open standards are critical to combining a wide range of data sets—including both structured and unstructured—across myriad analytics environments and applications. Open application programming interfaces (APIs) also enhance innovative uses of data that that enable applications to interact effectively. Conversely, the advantages of the IoT and data-driven innovation could be squandered where boundaries are erected unnecessarily by proprietary data standards and closed APIs.

As IoT technologies continue to evolve, practical, cost effective new practices will continue to drive data analytics and network architectures based on open standards. Industry-led standards development organizations are well suited to determine which standards will best implement the policy goal of data interoperability.

Governments can play a key role as a facilitator and convener, applying open standards practices to their own data, and encouraging and facilitating coalescence around open standards. However, governments must resist the temptation to enact policies that impose requirements around specific technical standards or try to create new standards where they may not exist. Attempts to dictate interoperability conditions could have the undesirable consequence of reducing the marketplace to a standardized set of products and services.

7. NIST and NTIA are actively working to develop and understand many of the technical underpinnings for IoT technologies and their applications. What factors should the Department of Commerce and, more generally, the federal government consider when prioritizing their technical activities with regard to IoT and its applications, and why?

As noted above, the Department of Commerce, particularly the NTIA and NIST, have led effective multistakeholder initiatives across a wide range of technical and policy issues, addressing such key issues as standards acceleration, security and privacy. We encourage the Department to continue exploring opportunities around IoT where a stakeholder convening role could be valuable, or where technical expertise, such as in the case of NIST, can be leveraged for the benefit of continued IoT development and implementation.

13. What impact will the proliferation of IoT have on industrial practices, for example, advanced manufacturing, supply chains, or agriculture?

In manufacturing, the value added by IoT technologies ranges from $0.9 trillion to $2.3 trillion per year by 2025, according to a McKinsey Institute study.[3] Benefits from IoT technologies in the manufacturing sector are similar to those in the energy sector. In the energy sector, estimates show that its value could add $14.2 trillion to the global economy by 2030.[4] These same estimates also show that the value of the internet of things in the global energy sector is expected to reach approximately $22 billion by 2020 with a compound annual growth rate of 24.1% over the next 5 years.[5]

In the energy sector, IoT technologies like the incorporation of smart meters for measurement allow for predictive maintenance, platform security, logistics, compliance and risk management, analytics, energy management, monitoring and analytics. Sensors can account for electrical energy needs and preferred temperatures to optimize conditions to lessen waste and cut energy costs.

On the renewable energy front, IoT can help manage smart grids, and allow systems to balance loads and decrease equipment wear and tear. Sensors can help identify if parts need repair and better ensure worker safety as workers will be able to monitor equipment from a safe distance.

The estimated value of IoT in the agricultural sector is around $100 billion per year by 2025.[6] Again, similar to energy and manufacturing, the agricultural sector can utilize IoT technology for predictive maintenance for farming as well as equipment upkeep. Sensors can provide workers with real-time analytics which can help determine the best time to harvest crop or when equipment needs to be repaired or replaced. Currently, the agricultural sector is one of the larger beneficiaries of IoT technologies with workers already utilizing smart devices to accomplish their goals.

The IoT in healthcare is predicted to generate between $1.1 trillion and $2.5 trillion per year by 2025.[7] Here, IoT technologies can be used to help monitor the human body for predictive

[3] McKinsey & Company. "Disruptive Technologies: Advances that will transform life, business, and the global economy." May 2013.
[4] Accenture. "Winning with the Industrial Internet of Things."
[5] "Internet of Things in the Energy Sector worth US $22bn by 2020." Metering & Smart Energy International. 13 October 2015.
[6] McKinsey & Company. "Disruptive Technologies: Advances that will transform life, business, and the global economy." May 2013.
[7] McKinsey & Company. "Disruptive Technologies: Advances that will transform life, business, and the global economy." May 2013.

maintenance and to detect unnatural activity or trauma.[8] Sensors can detect illness and warning signs for more serious conditions. Wearables can help monitor individuals living in the home such as elderly persons living alone. Not only do IoT technologies aid in patient care through monitoring, but they can also aid in drug management. They can enhance the management of high drug production costs and monitoring of fraudulent activities.

16. How should the government address or respond to cybersecurity concerns about IoT? a. What are the cybersecurity concerns raised specifically by IoT? How are they different from other cybersecurity concerns? b. How do these concerns change based on the categorization of IoT applications (e.g., based on categories for Question 4, or consumer vs. industrial)? c. What role or actions should the Department of Commerce and, more generally, the federal government take regarding policies, rules, and/or standards with regards to IoT cybersecurity, if any?

The need to maintain adequate security has been a fundamental pillar of electronic commerce and internet-based communications and services for decades, but the risks of unauthorized access to computer networks and sensitive data inherently increases with the IoT, where there are larger networks with more devices, including cars, medical devices, wearables and home appliances.

IoT threat scenarios range from practical to far-fetched, but many of these threats are not entirely new. For instance, the potential to hack into critical infrastructure and services could cut off a power plant, disrupt the electrical grid, shut down water supplies, or cause a heart to stop. Many of these threats have existed for years, and some have become more complex with IoT technology evolution.

In 2013, researchers successfully hacked into a Jeep Cherokee and several other cars which were connected to a wireless mobile network through embedded software called UConnect.[9] These researchers were able to successfully utilize a zero-day exploit in the UConnect software to disable the breaks and control the vehicle's steering mechanism making for a truly terrifying situation. Although the vulnerability was patched quickly, this example represents a clear and present concern about IoT technologies that could lead to significant physical harm and if not implemented effectively.

The need to protect connected devices in the home has also received considerable attention, where home-based IoT equipment often uses the home Wi-Fi network to connect to a cloud-based service provider. There have been multiple reports of hackers exploiting vulnerabilities in routers to serve as a starting point to home networks and connected devices.[10]

Fortunately, along with the opportunity to provide enormous benefits, there are also opportunities to develop and provide IoT technologies and services with adequate security. For instance, smarter routers, working in conjunction with the related devices and back-end data centers, can provide a more secure home network, where the router serves as an automated firewall that understands the customer's smart home and works behind the scenes to safeguard it. While early applications often

[8] Wladawsky-Berger, Irving. "Measuring the Economic Potential of the Internet of Things." *Wall Street Journal*. 17 July 2015.
[9] Greenberg, Andy. "Hackers Remotely Kill a Jeep on the Highway – With Me In It." *Wired*. 21 July 2015.
[10] Fleishman, Glenn. "An Internet of Treacherous Things." MIT Technology Review. 13 January 2015.

lacked adequate security, providers are exploring opportunities to design IoT devices and networks that truly can defend themselves, where antivirus/antimalware software is kept up to date and smart homes can become as secure as physical homes with locks on every door and window.[11] As with the physical comparison, there is no such thing as perfect security. For instance, in most cases door and window locks are sufficient to keep out intruders. However, in some circumstances, bars on the windows, reinforced deadbolt locks, and possibly an alarm system that detects break-ins and alerts the police are necessary. While many consumer IoT devices operate outside of a home, the home network model provides an example of how existing technologies such as routers can evolve to not only become more secure as threats increase, but also serve as a secure gatekeeper for other IoT devices.

Ultimately, when it comes to IoT security, risk assessment is critical. Providers of IoT devices and services need to embrace security-by-design, beginning with risk assessment as part of the design process, testing security measures before products and services launch, and utilizing encryption for the storage and use of sensitive information. Of course, design is just the first step. Consistent with all IT infrastructures, maintenance is also critical. IoT systems should be monitored throughout their life cycle and a system for patching known vulnerabilities that arise is essential in certain instances. Employing hackers to find and fix vulnerabilities in their own networks or devices is one of several ways companies can constantly keep their products more secure for consumers.

IoT device-makers and service providers also need to provide reasonable security. Of course, what constitutes reasonable security for a given device will depend on a number of factors, including the amount and sensitivity of data collected, the device's functionality and the costs of remedying the security vulnerabilities. Security best practices will not apply uniformly across all uses of all IoT devices. Rather industry-specific codes are more likely to be properly designed to meet the specific security challenges in each economic sector. Uniform government regulations could not be effectively applied either.

Market forces will continue to play a critical role to promote the advancement of risk-based security frameworks and commonly accepted standards for connected devices and new IoT services, and government oversight can help enforce reasonable security, even as industry standards progress over time. Policymakers should consider ways to incent the combination of security by design techniques and adherence to industry codes of conduct and best practices which establish responsible data security practices, rather than seeking to mandate a "check-the-box" legislative or regulatory approach.

The NIST Cybersecurity Framework provides an excellent example of the valuable role for government, particularly the DOC and NIST, in convening stakeholders to develop a flexible, risk-based security framework. Notably, the ongoing effort to update this Framework demonstrates the need for these frameworks and policies to evolve with technology and to be improved based on implementation and user experience.

17. How should the government address or respond to privacy concerns about IoT? a. What are the privacy concerns raised specifically by IoT? How are they different from other privacy concerns? b.

[11] Zeichick, Alan. "ISP opportunity: Protect the Internet of Things in the home." Network World. 23 June 2015.

Do these concerns change based on the categorization of IoT applications (e.g., based on categories for Question 4, or consumer vs. industrial)? c. What role or actions should the Department of Commerce and, more generally, the federal government take regarding policies, rules, and/or standards with regards to privacy and the IoT?

As technologies evolve towards an "internet of everything" environment, becoming more personalized and instrumental in all facets of our lives, social norms, and expectations about the flow of information and privacy also evolve along with user experiences. Policy frameworks pertaining to privacy therefore need to remain sufficiently flexible to accommodate these evolutionary changes, where the socially beneficial uses of data made possible by data analytics are often not immediately evident to data subjects at the time of data collection.

In the past, privacy was regarded as a matter of individual choice and responsibility, where consumers could make informed decisions about what data is collected about them. However, in the era of big data and the IoT, this is less the case. There is considerable tension between the opportunities and benefits presented by data-driven innovation, and the ability of individuals to make informed decisions about such a wide range of data collection and use enabled by the IoT.

For many years, Fair Information Practice Principles (FIPPs) have provided guidelines for policymakers and data stewards regarding responsible information management practices. FIPPs are flexible enough to continue applying in the IoT environment as a set of guidance in the collection, use and protection of personal information. That said, public policies will need to continue balancing principles of privacy against societal values such as public health, national security, economic growth, and the environment. The 2013 OECD Privacy Guidelines, which are based in part on FIPPS principles, are also worth referring to in this context. Global policymakers appropriately draw upon these flexible guidelines when considering policy. The Guidelines essentially update the 1980 OECD Privacy Principles, which have been influential around the world.

Implementation of FIPPs has met with considerable challenges with the rise of "big data," where for instance the challenges to notice and choice framework have been widely recognized. In 2014, the Obama Administration released two whitepapers that highlighted these challenges in the era of big data, noting that it will be "critical to look closely at the notice and consent framework that has been a central pillar of how privacy practices have been organized for more than four decades."[12] Another report released by the Administration concluded that the notice and choice framework is already "increasingly unworkable and ineffective," and that "policy attention should focus more on the actual uses of big data and less on its collection and analysis."[13]

In the IoT environment, Internet-connected devices are ubiquitous and sensors are not always visible, further limiting the practicality of a broad regime of notice and choice. To be sure, notice and choice, or transparency and control, will remain critical components across many applications of the IoT where sensitive data is involved. However, policymakers should continue to weigh the challenges associated with expanding consent requirements, exercising caution and recognizing that the

[12] Big Data: Seizing Opportunities, Preserving Values. Executive Office of the President. May 2014.
[13] Big Data and Privacy: A Technological Perspective. Executive Office of the President, President's Council of Advisors on Science and Technology. May 2014.

sensitivity of the data and context in which it is collected are critical factors. A uniform requirement for obtaining true and informed consent for all collection and uses of information that is personal, or linkable, to an individual, is increasingly unrealistic and would likely serve as a barrier to socially beneficial uses of information available through the IoT.

Similarly, other longstanding FIPPs such as purpose specification, data minimization, and use limitation need to be implemented in creative ways to avoid conflicts with potential gains from the IoT. For instance, the notion of collecting only a limited amount of information, for a specifically defined purpose and retaining the data for a set, limited amount of time is counter to the opportunities presented by the IoT.

To maximize the opportunities presented by the IoT, policies should continue encouraging transparency and control where feasible and applying an accountability framework where there is a greater emphasis on data users to exhibit responsible data stewardship and accountability.[14]

As noted above with respect to security, policymakers should encourage privacy-by-design practices, including privacy risk assessments, transparency and control for collection of personal information, as well as practices such as the use of de-identification techniques where appropriate. De-identified data, while not expected to provide for perfect privacy protections, can substantially help mitigate many of the risks when permitting connected devices to share data and provide for innovative data analytics that drives the IoT. Other privacy by design practices might include tamper-resistant audit logs, information transfer accounting, and PII anonymization (that falls short of full de-identification).[15] Privacy-enhancing technologies are less expensive and more widely available if they are included in products and services from the start rather than sold after the fact as a stand-alone.

Privacy and security by-design techniques and adherence to industry codes of conduct and best practices which establish responsible data principles, rather than mandating such practices through overly rigid legislative or regulatory approaches. Together, industry-driven best practices and responsible data stewardship practices, both of which can be enforced under current law, can create an effective responsible data use framework that balances privacy and security with innovation and account appropriately for risk.

20. What factors should the Department consider in its international engagement in: a. Standards and specification organizations? b. Bilateral and multilateral engagement? c. Industry alliances? d. Other?

In addition to the comments above regarding the value of the Government and the Department of Commerce in serving as a convener on critical issues such as interoperability and standards, The Department has a valuable role to play in continuing to promote technology neutral policies. Technology neutrality has long been a widely recognized guiding principle for technology policies, particularly Internet-based ICT. This was first recognized within the U.S. government in 1997, with the Framework for Global Electronic Commerce, a framework that has stood the test of time in establishing broad principles for regulating ICT, that "rules should be technology neutral (i.e., the

[14] Fred H. Cate and Viktor Mayer-Schonberger. Notice and Consent in a World of Big Data. November 2012.
[15] Cavoukian, Ann, and Jeff Jonas. Privacy by Design in the Age of Big Data. June 2012.

rules should neither require nor assume a particular technology) and forward looking (i.e., the rules should not hinder the use or development of technologies in the future)." [16] By contrast, Government-mandated technology standards can freeze the development of new technologies, or disadvantage entire categories of market players.

These long-held principles for resisting technological mandates and maintaining technological neutrality is especially important for a complex IT ecosystem that will comprise the IoT, one which will be inherently subject to constant innovation. For example, given the range of devices that enable to the collection and utilization of data, it is impractical and ineffective to create policies based solely on a specific type of device, or an arbitrary characteristic of a device, like whether it is mobile like a smartphone or automobile sensor, or whether it is stationary, such as a computer or a refrigerator. While it might seem practical to target specific devices or platforms, this approach is likely to become dated within a matter of months or years due to the rapid evolution of IoT technologies.

21. What issues, if any, regarding IoT should the Department focus on through international engagement?

The Department should monitor the global development of IOT and identify barriers to the full potential of IOT. This could, for instance, be part of the portfolio of the Department's Digital Attaches. From a policy perspective, the Department should continue, in concert with all relevant USG agencies, to promote cross-border data flows and prohibitions against data localization. This also involves continuing to promote interoperability mechanisms such as the EU-US Privacy Shield and APEC's Cross-Border Privacy Rules.

23. Are there policies that the government should seek to promote with international partners that would be helpful in the IoT context?

The government should seek to promote standards development processes along the lines of the NTIA-coordinated cybersecurity guidelines. Government are best positioned to convene such processes and then perhaps facilitate discussions with a view to taking advantage of on-the ground industry-informed solutions to identified problems.

24. What factors can impede the growth of the IoT outside the U. S. (e.g., data or service localization requirements or other barriers to trade), or otherwise constrain the ability of U.S. companies to provide those services on a global basis? How can the government help to alleviate these factors?

Data and/or service localization requirement can constrain the ability of U.S. firms to provide IOT services. The government can do at least two things alleviate these factors. First, provide information on the benefits of the IOT revolution. Second, continue to promote the passage of TPP in the U.S. Congress and work for e-commerce provisions in TISA and TTIP with the TPP's e-commerce chapter being the floor for such provisions.

[16] Framework for Global Electronic Commerce. The White House. 1 July 1997.

Conclusion

Again, thank you for the opportunity to comment on this important issue. If you have further questions or would like to discuss, please contact David LeDuc, SIIA's Senior Director for Public policy, at dleduc@siia.net or 202-789-4443.

Sincerely,

Ken Wasch
President