Empowering the Internet of Things:

Benefits, Solutions, and Recommendations for Policymakers

SIIA

DEVELOPED BY THE PUBLIC POLICY DIVISION OF THE SOFTWARE & INFORMATION INDUSTRY ASSOCIATION

Table of Contents

SIIA is an umbrella association representing 800+ technology, data, and media companies globally. Industry leaders work through SIIA's divisions to address issues and challenges that impact their industry segments with the goal of driving innovation and growth for the industry and each member company. This is accomplished through in-person and online business development opportunities, peer networking, corporate education, intellectual property protection, and government relations. For more information, visit siia.net.

Internet of Things: A Primer and Policy Roadmap

Introduction

Today, we are at a key inflection point in the history of information technology (IT). The last several years have brought about significant advances in IT, representing an evolution for 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.

In the late 19th century, electricity was initially associated with the critical function of providing light. Of course, as was soon realized, the application of electricity as a driver for a wide range of not-yet-conceived devices and appliances would go on to revolutionize the world. So too is the anticipated impact of the Internet, as it further develops away from a computer-to-computer communication network into a ubiquitous network linking electronic devices and everyday objects. This development is often referred to as the "Internet of Things" (IoT), a phrase used to describe ubiquitous interconnectivity, where people don't just interact with devices, but devices also interact directly with each other. Whereas electricity powers devices and appliances themselves, the IoT powers services. By tracking the functionality of these devices and appliances in the supply-chain, IoT technologies are able to provide data analysis to maximize production, improve functionality, and minimize waste. As a result services provided using these technologies are more dynamic and effective, and they are substantially beneficial to the global economy overall.

The IoT is an enabler of data-driven innovation that will play a major role in the future of the global economy. 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.[1]

This white paper focuses specifically on the new IoT technologies and services that will fundamentally improve the way business is done and the way people live. This type of data processing applied to the information flows from the IoT will make many sectors of the economy more efficient and productive, including energy, agriculture, manufacturing, and healthcare.

This paper offers an overview of the transformative benefits of the IoT, and it presents a series of public policy recommendations to enable these benefits while ensuring that the IoT meets the needs of citizens, businesses and governments around the world.

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

Transformative Benefits of the Internet of Things

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 different levels of utility, but all will benefit greatly from IoT advances.

The economic benefits of the IoT are substantial. A June 2015 report by McKinsey & Co. estimates that the economic benefit from the Internet of Things ranges anywhere from $4 trillion to $11 trillion from now until the year 2025.[2] This estimate is based on projected technological development, rate of adoption, and economic and demographic trends over the next ten years. Much publicity and emphasis is placed on consumer application of the IoT as a significant portion of the value gained from IoT technology will stem from consumer end utilization. However, economic impact will also be felt through the industrial sector, where business-to-business applications will account for a majority of the value stemming from the IoT.

Industrial & Manufacturing

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. Smart meters can account for parts that need maintenance or replacement and connect production facilities so that real-time analytics can be used to assess this data to cut costs and eliminate waste.

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]

"Economic benefit from the IoT ranges from $4 trillion to $11 trillion from now until 2025."

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, it can help manage smart grids, and allow systems to balance loads and decrease equipment wear and tear. Sensors

[2] McKinsey & Company. "Unlocking the Potential of the Internet of Things." June 2015.
[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.

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 utilizing smart devices to accomplish their goals.

The Internet of Things 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 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.

Consumer Products and Services

Opportunities for consumers already abound, including the early stages of development in wearables, smart homes, autos and other connected consumer products. These technologies serve to cut consumer costs, allow for greater convenience, and improve efficiency. It is estimated that this sector will grow from $10 billion in 2013, to somewhere between $19-40 billion in 2019.[9] In the home, consumers can benefit from monitoring sources of energy output to minimize utility costs of water, electricity, and climate control. IoT technologies can help consumers use these means in a more practical way. For example, smart refrigerators can keep track of food storage and expiration dates, and sensors can automatically turn water on and off so only the necessary amount of water is used at a given time.

Wearables are also a major element of the IoT. Health and fitness monitoring devices, and smart watches help monitor nutrition and physical activity. Downloadable apps made for wearable devices can also be used for a wide variety of purposes and provide for greater efficiency. An example of wearable technology is a device with synchronized data from public transportation services to show the most efficient commuting routes, or a device that monitors health and wellbeing and transmits information to doctors to provide better information to medical professionals for improved care.

[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.

[8] Wladawsky-Berger, Irving. "Measuring the Economic Potential of the Internet of Things." *Wall Street Journal*. 17 July 2015.

[9] Thierer, Adam. Castillo, Andrea. "Projecting the Growth and Economic Impact of the Internet of Things." Mercatus Center. 15 June 2015.

Finally, autonomous cars made for consumer use exemplify the great potential of the IoT. Several companies, including Google, Tesla, Chrysler, and Samsung have been developing the technology for driverless cars to operate safely on the road. Automation promises to reduce the number of accidents that occur on the roads and provide greater safety when a crash does occur.[10] Although completely autonomous vehicles are still only in the pilot phase, accident-predicting technologies are already being applied in non-autonomous or semi-autonomous cars. This technology can be seen in vehicles that have the ability to automatically apply the brakes when sensors detect that the car is within proximity of something directly in front of or behind it.

Benefits By Sector		
Sector	**Value** **(Tens of Billions of Dollars)**	**By Year**
Consumer	1.9 – 4	2019
Energy	2.2 – 1,400	2020 – 2030
Agriculture	10	2025
Manufacturing	90 – 230	2025
Healthcare	110 – 250	2025
Total	**400 – 1,100**	**2025**

Table 1

Government Services

Governments will also benefit significantly from IoT technologies. Real-time statistics can allow for better information collection on how government services are addressing certain challenges. An example of what the IoT can do for government services is in policing. Utilization of body-cams can better monitor police behavior, and connected firearms can track when a firearm is detached from its holster to dispatch backup if it is ever fired.[11] Not only do these technologies provide benefit in times of emergency, but sensors and cameras can also be applied to study officer behavior and generally improve policing practices.

Another example of how government services can benefit from the internet of things is in smart cities. In September of 2015, the Obama Administration announced it will invest $160 million in a new smart cities initiative to better manage city infrastructure and serve as a testing ground for new IoT technologies in a joint public-private effort.[12] Smart cities provide real-time analysis and maintenance of city functions through the use of sensors for traffic control, energy utilization, highway maintenance, emergency services, and other uses such as environmental sensors to monitor air and water quality.

Developing Economies

Developing countries offer perhaps the greatest opportunity for immediate realization of profound benefits from IoT technologies. Estimates show that by 2025, approx. 38 percent of the annual

[10] Koslowski, Thilo. "Forget the Internet of Things: Here Comes the 'Internet of Cars.'" *Wired.* 4 January 2013.
[11] Eggers, William D. "Redesigning Government Work for the Internet of Things." *NextGov.* 2 September 2015.
[12] The White House: Office of the Press Secretary. "FACT SHEET: Administration Announces New "Smart Cities" Initiative to Help Communities Tackle Local Challenges and Improve City Services." 14 September 2015.

growth of the IoT will come from the developing world.[13] Access to mobile technology is growing dramatically in developing countries. Combined with the IoT, this growth in mobile broadband means citizens in developing countries will have greater access to necessities they would not normally have access to. For example, knowledge of water sources, agrarian aid to maximize production and minimize waste, and access to financial services become readily available when utilizing IoT technology in this manner.[14] The possibilities can cover energy, water availability, industrialization, healthcare and disease control, infrastructure, and resource management. IoT implementation can help with UN Sustainable Development Goals.[15]

"By 2025, 38% of the annual growth of the IoT will come from the developing world."

IoT interventions have already led to benefits for developing regions.[16] Equipment has been tagged with sensors to monitor temperature and location, and cold changes. Such information is helpful to agriculture and food production. Data accrued from these sensors also helps facilitate the transportation and distribution of vaccines and makes this equipment more secure. In East Africa, for example, hand pumps tagged with sensors to monitor water flow are deployed to help to inform local communities of water using and decrease the downtime of a malfunctioning pump.

In developing economies, urban planning provides an opportunity to take full advantage of IoT technologies. Sensors that monitor rainfall enable cities and municipalities to prepare for potentially damaging floods. As many developing cities also experience water shortages, IoT technologies also allow for more effective water conservation techniques regarding rainwater storage. Additionally, sensors placed along roads and in transit systems provide for the monitoring of environmental conditions and to identify places where maintenance is needed.[17] These sensors also enable transit services to detect the fastest, safest, and best possible routes which is an enormous benefit for emergency service providers.

Agriculturally, developing economies can also take advantage of IoT technologies for irrigation and farming. Digital farming through sensors that can track livestock, manage pumps and fencing, and account for soil moisture.[18] John Deere is already working to make farm tractors data control centers capable of tracking production variables and functional activity. Monitoring farms in this way can improve food production in developing economies where the food gap is high compared to the United States as larger amounts of people are consuming more meat which requires more grain. Information gleaned through IoT technologies can produce a higher yield and much lower waste.[19]

Ensuring the full potential of IoT technologies in these areas is exceptionally important as global economic focus is shifting to the developing world.[20] Of course, connecting mobile devices to the Internet often presents a challenge in the developing world, particularly in parts of Africa and Asia.

[13] Internet Society. "The Internet of Things: An Overview." October 2015.

[14] Brookings Institution. "How the 'Internet of Things' is transforming the global economy." 21 October 2015.

[15] United Nations. Sustainable Development Goals. Sustainable Development Knowledge Platform.

[16] Internet Society. "The Internet of Things: An Overview." October 2015.

[17] Adler, Laura. "The Urban Internet of Things." *Data-Smart City Solutions*. Harvard University. 31 August 2015.

[18] "Digital Farm Set for Internet's Next Wave." *The Guardian*. 21 September 2015.

[19] Lohr, Steve. "The Internet of Things and the Future of Farming." *The New York Times.* 3 August 2015.

[20] Internet Society. "The Internet of Things: An Overview." October 2015.

Public and private entities alike are working to change this.[21] Technology-based solutions are currently seeking to overcome these challenges, such as Google's Project Loon which aims to provide wireless internet access to rural and lower income areas around the world.[22]

[21] Alliance for Affordable Internet. "Vision and Strategy."

[22] "What Is Project Loon?" Project Loon. Google.

Securing the Internet of Things

The IoT presents an exciting faze of Internet-based innovation which has also brought about some new challenges. For instance, the need to maintain adequate security has been a fundamental pillar of electronic commerce 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.[23] 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 personal harm 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.[24]

"When it comes to IoT security, risk assessment is critical."

Fortunately, along with the opportunity to provide enormous benefits, there is also an opportunity 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 system, 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 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.[25]

As with the physical comparison, there is no such thing as perfect security. Often, door and window locks are sufficient to keep out intruders. However, other houses may have bars on the windows, reinforced deadbolt locks, and possibly an alarm system that detects break-ins and alerts the police.

Ultimately, when it comes to IoT security, risk assessment is critical. Companies need to embrace security by design, beginning with risk assessment as part of the design process, testing security

[23] Greenberg, Andy. "Hackers Remotely Kill a Jeep on the Highway – With Me In It." *Wired*. 21 July 2015.
[24] Fleishman, Glenn. "An Internet of Treacherous Things." MIT Technology Review. 13 January 2015.
[25] Zeichick, Alan. "ISP opportunity: Protect the Internet of Things in the home." Network World. 23 June 2015.

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.

While many 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.

An IoT without adequate security would be an IoT of little benefit. [26] Therefore, IoT security challenges must be adequately addressed. 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.

[26] Brookings Institution. "How the 'Internet of Things' is transforming the global economy." 21 October 2015.

Fostering the Internet of Things: Public Policy Recommendations

From the early days of electronic commerce, to the rise of “cloud computing,” “big data” analytics, and now the “Internet of Things,” we have seen continued evolution of information technology tied to enhanced Internet capabilities. The IoT is merely the newest phase of this evolution, where the number and scope of internet-connected devices has dramatically increased, along with the increasing capabilities for devices to interact not only with people, but with other systems and directly with one another.

SIIA offers the following recommendations for policymakers seeking to assess the opportunities and challenges presented by the IoT, and to encourage policies capable of enabling the IoT to transform the way we work, learn, communicate and live our lives.

1. Do Not Seek an Overarching IoT Policy Framework.

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. 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 business-to-consumer context might be inappropriate when applied in a business-to-business context. Similarly, internet-connected light bulbs are very different than “wearables,” which are also different from items such as connected appliances and automobiles.

In general, existing laws have continued to function quite effectively and provide substantial consumer protection, even in light of rapid technological innovation over the last decade. 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 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.

> **“Existing laws have continued to function quite effectively and provide substantial consumer protection, even in light of rapid technological innovation over the last decade.”**

In 2014, the FTC settled their 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. The FTC can and should continue to aggressively 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.

2. Privacy Rights for the IoT Should Be Based on Risk and Societal Benefits.

As technologies evolve, 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, FIPPs have provided guidelines for policymakers and data stewards regarding responsible information management practices."**

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."[27] Another report released by the Administration concluded that the notice and choice framework is

[27] Big Data: Seizing Opportunities, Preserving Values. Executive Office of the President. May 2014.

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.”[28]

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 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 to 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.[29]

3. Encourage Best Practices for Privacy and Cybersecurity

While history over the last two decades has demonstrated the challenge to continually update public policies to keep pace with technology, this is likely to be even more so in the years ahead. The IoT will continue to rapidly evolve over the next couple decades, leading to what many have termed, the “Internet of Everything,” where Internet connectivity is ubiquitous and devices will regularly communicate with each other as part of their basic functionality.

With such a dynamic technological environment, new regulations run the risk of stifling burgeoning innovation that holds the promise of transforming the way we work, communicate, learn and live our lives. Instead, industry best practices and self-regulatory codes of conduct can provide more flexibility to evolve and adapt over time with technology and user preferences and expectations. For instance, voluntary but enforceable codes can be used to establish frameworks that enable individuals to associate usage preferences with connected devices, indicating to other devices how information collected from individuals’ devices may be used. Well-behaved companies will typically inform users of their devices regarding the information collected by the device and how it is used.

“New regulations run the risk of stifling burgeoning innovation that holds the promise of transforming the way we work, communicate, learn and live our lives.”

[28] Big Data and Privacy: A Technological Perspective. Executive Office of the President, President’s Council of Advisors on Science and Technology. May 2014.

[29] Fred H. Cate and Viktor Mayer-Schonberger. Notice and Consent in a World of Big Data. November 2012.

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.

Privacy and security "by design," or the practice of building privacy and security into devices early in the design cycle of a technology rather than as an afterthought, are critical elements to the IoT. Security risk assessments, continuous monitoring, the use of strong encryption for sensitive information or where there is considerable security risk, security defaults and security testing prior to product launches are all elements that should be considered in a security-by-design approach, and these can be used as the basis for codes of conduct to guide various IoT industry segments.

Similarly, privacy by design practices should include 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).[30] As many have noted, 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.

However, these concepts cannot be broadly defined or applied consistently across all implementations of IoT technology, because they present different sets of responsibilities in different contexts, evolving along with technology and user demands and expectations. Therefore, policymakers should consider ways to incent the combination of 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.

4. Promote Technology Neutrality and Avoid Technology Mandates.

"Further, mandating types of encryption or approaches to de-identification might seem like good approaches for enhancing privacy and data security, but such approaches continue to prove incapable of keeping up with technological evolution."

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

[30] Cavoukian, Ann, and Jeff Jonas. Privacy by Design in the Age of Big Data. June 2012.

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 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).” 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.

Further, mandating types of encryption or approaches to de-identification might seem like good approaches for enhancing privacy and data security, but such approaches continue to prove incapable of keeping up with technological evolution. There is almost always a better way to accomplish a given purpose waiting around the corner. Policies must continue to encourage innovation to find faster, better, and less expensive ways to protect privacy and security.

For instance, while technology that designs protection in the concept and engineering phases—e.g. privacy and security by design—provides the most efficient way to provide for data privacy and security, government policies requiring specific technological solutions have consistently proven to be ineffective.

5. IoT Standards Should Be Open and Industry-led

The ability of devices to increasingly communicate with each other, and with people, is integral to the Internet of Things, as is the ability to integrate multiple data sources 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 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.

> **“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.

6. Policies for Embedded Software Should Provide for Product Integrity

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.

"It is important to remember that the IoT is developing healthily in the presence of many well-understood legal doctrines that protect health, safety and property rights."

Nonetheless, as these kinds of connected devices are becoming more common, policymakers are exploring the need to update current laws and regulations in this area.   For example, in response to a Congressional request, the U.S. Copyright Office is studying the law surrounding "embedded software."   This study could review the circumstances under which software embedded in IoT devices is licensed to the user, in contrast to the circumstances in which the owner of the device is also the owner of the copy of the embedded software.   The Office's recent experience in dealing with these issues also raised some controversial public policy questions involving public safety, health and the environment.

The issues surrounding the IoT are just beginning to be framed for public debate, and it is important to remember that the IoT is developing healthily in the presence of many well-understood legal doctrines that protect health, safety and property rights. 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 policy makers to engage in careful study before disturbing these statutory regimes.

The Software & Information Industry Association (SIIA) is an umbrella association representing 800+ technology, data, and media companies globally. Industry leaders work through SIIA’s divisions to address issues and challenges that impact their industry segments with the goal of driving innovation and growth for the industry and each member company. This is accomplished through in-person and online business development opportunities, peer networking, corporate education, intellectual property protection, and government relations.
For more information, visit siia.net.

SIIA Public Policy
Software & Information Industry Association
1090 Vermont Avenue NW
Sixth Floor
Washington, DC 20005