TIA White Paper

Realizing the Potential of the Internet of Things:

Recommendations to Policy Makers

2015

ADVANCING GLOBAL COMMUNICATIONS

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
tiaonline.org

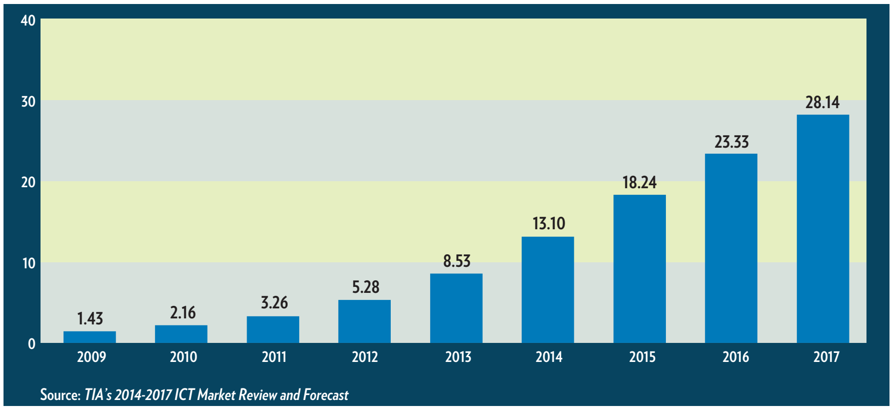
Realizing the Potential of The Internet of Things:
Recommendations to Policy Makers

The future for telecommunications and the world economy lies with the Internet of Things (IoT). At its most basic, the "Internet of Things" is a label for an increasingly connected future in which regular, everyday items – from household appliances to cars to medical devices – are outfitted with sensors and connected to the Internet to share their data. Viewed more broadly, the Internet of Things will give rise to an entire ecosystem for interconnected devices, objects, systems, and data all working together. In this new world, most communications will be machine-to-machine (M2M), and there will be a continuous exchange of information between devices, sensors, computers, and networks.

The rapid rise of the Internet of Things has been driven by several factors, including the widespread penetration of broadband Internet, faster mobile connections, and the use of advanced computing capability, which allows for the development of smaller and cheaper devices. In recent years, a key element driving growth has been the ability to install inexpensive sensors in machines and devices. This has been made possible by advances in sensor technology that have dramatically reduced costs, while also capitalizing on geo-location or other technology advancements. Once these devices are connected to a network, consumers and businesses will have the ability to collect and analyze significant amounts of machine-generated data in real-time, allowing people to make decisions that maximize efficiencies in time and cost.

Aside from driving transformative societal effects, the economic potential of the IoT is enormous. In 2012, an estimated 8.7 billion "things" were connected worldwide, and projections show that this could grow to 50 billion

MACHINE-TO-MACHINE SERVICES SPENDING
IN THE UNITED STATES ($ BILLIONS)



Source: *TIA's 2014-2017 ICT Market Review and Forecast*

by the year 2020[1] – generating global revenues of $8.9 *trillion* in the process[2]. In direct terms, this represents an enormous market for information and communications technology (ICT) manufacturers, vendors, and suppliers. Ultimately, however, there will be enormous secondary economic effects as the Internet of Things emerges and gradually transforms daily life worldwide.

> **The Internet of Things holds the potential for major disruptive effects across a wide variety of market sectors... [m]eanwhile, there are a number of important horizontal policy issues that affect the Internet of Things across markets and use cases.**

Not surprisingly, policymakers are taking a much greater interest in the Internet of Things, and are attempting to craft forward-looking laws and regulations that keep pace with innovation – or at least do not hinder it. This white paper begins by offering a general framework for such policy discussions. The recommendations that follow are applicable across market sectors, and will help ensure that the full economic, societal, and technological potential of the Internet of Things is ultimately realized.

A Horizontal Framework for IoT Policy

The Internet of Things holds the potential for major disruptive effects across a wide variety of market sectors. Vertical markets that will be affected include, for example:

- ***Health Care.*** Health care applications include the potential for remote patient monitoring using smart electronic devices, allowing patients and their doctors to obtain real-time access to health data. This is expected to lead to vast improvements in the quality of care, better health outcomes, and significantly lower costs.
- ***Transportation.*** Transportation applications will include not just the rapidly emerging self-driving and connected vehicles, but also the ability to develop "intelligent" transportation infrastructure from roads to airports to parking garages.
- ***Energy.*** Applications include smart metering, other "smart grid" technologies, and the ability to drive greater efficiencies in both energy production and consumption.
- ***Manufacturing.*** Sensor networks and smart devices will drive major improvements throughout the manufacturing process based on process improvements such as increased visibility into manufacturing processes that better inform decision-making, improved automation, augmented energy management, increased ability for proactive maintenance, and a better-connected supply chain.
- ***Government.*** The Internet of Things will have a major impact in the public sector, from defense and emergency service applications to driving improvements in service delivery and responsiveness to constituent needs.

With the Internet of Things holding the potential to achieve the real-world advances described above, much of the initial policy interest has developed vertically, i.e., with respect to a specific market. Market-specific regulators have started considering IoT-related policy actions for several of the markets above, although often never actually using the term "Internet of Things."

Meanwhile, there are a number of important horizontal policy issues that affect the Internet of Things across markets and use cases. These include, for example:

[1] http://share.cisco.com/internet-of-things2.html

[2] http://www.idc.com/getdoc.jsp?containerId=prUS24366813

- ***Interoperability.*** Enabling devices and systems to connect with each other on a technical level, typically through reliance on common standards or protocols.
- ***Privacy.*** The ability of consumers and businesses to safeguard their own personal or business data in a world of machine-to-machine transmissions.
- ***Security.*** Ensuring that devices, networks, and applications are secured from threats by malicious actors.
- ***Data Storage.*** Where, how, and when the vast amounts of data generated from individual sensors and devices will be stored.
- ***Spectrum and Bandwidth.*** Ensuring that sensor-enabled and network-aware devices are able to transmit their data in a manner that uses constrained resources efficiently.

IoT policy discussions should begin with a common horizontal framework whenever possible, followed by tailoring for specific vertical applications only as necessary.

With these common threads running across IoT applications and use cases, a significant danger exists that vertical regulations imposed in one market will be inappropriate for another. This could lead to a balkanized regulatory approach that stifles innovation and delays or degrades the economic and social potential of the IoT.

To avoid this scenario, ***IoT policy discussions should begin with a common horizontal framework whenever possible, followed by tailoring for specific vertical applications only as necessary***. Of course, achieving complete regulatory uniformity across different vertical markets may be both difficult and inadvisable. However, maximizing commonalities across sectors holds the potential for achieving both greater efficiencies as well as synergies across markets, increasing the potential for innovation. The IoT will effectively impact all aspects of society, and will grow existing – and create new – circular interdependencies among networks and devices used in the commercial enterprise, commercial consumer, public utility, and public safety segments, among many others. For example, the need for adequate consideration and management of risks to ensure the security and integrity of data (addressed later in this white paper) rests across all IoT applications.

The recommendations that follow in this white paper address many of the cross-cutting horizontal issues described above. As such, they are generally applicable across applications, use cases, and market sectors.

Recommendation: Policymakers' Approach to the Internet of Things Should Adhere to Competition- and Technology-Neutrality Principles

As ICT manufacturers and vendors work to meet the needs of their customers, competition will ultimately determine which products and services succeed or fail in the market, thereby fueling further innovation. As businesses increasingly make investments in the IoT, an utmost concern for policymakers should be to take a competition- and technology-neutral approach that respects the need for specific sectors to utilize creative solutions, and for innovators to address the needs of market segments. Policy makers should be wary of taking any action that locks the market to a limited set of solutions when new innovations, some of which cannot be predicted, are constantly being rolled out. No industry illustrates the need for flexibility and technology neutrality more than the dynamic ICT industry.

Policymakers should also avoid any situation that would put a government actor in a position to determine the future design and development of technology. To do otherwise would set a precedent of interference with the core innovation engine of the ICT sector, negatively impacting the interoperability and standards needed for IoT proliferation. Should a well-developed public policy case based on the consensus of stakeholders find that regulatory action is needed, we strongly encourage policymakers to promote the competitive dynamic by adopting regulations that are outcome-based, allowing innovation to thrive while still achieving the regulatory requirement.

Recommendation: Policymakers Should Encourage and Leverage Voluntary, Open, and Consensus-Based Standards

A major driver of the IoT will be the development of open, voluntary, and consensus-based standards.

A major driver of the IoT will be the development of open, voluntary, and consensus-based standards. Ongoing and future standardization efforts that enable the success of the IoT will cut across market segments, and will range from overarching guidelines to specific technical criteria, ensuring increasing interoperability as well as backwards-compatibility. Importantly, these standards are able to dynamically adapt to needed changes based on the expertise of their stakeholders. These standards also reduce costs, because manufacturers and software developers can produce for multiple applications and multiple end uses, allowing the benefits of economies of scale. TIA expects the development of IoT to be driven by a global – not regional – approach based on the development of open, voluntary, and consensus-driven standards.

Numerous existing standardization efforts, as well as future efforts, to address industry-consensus needs will define and contribute to the development of an interoperable IoT. TIA broadly supports the "multiple paths" approach to the development of international standards whereby healthy competition among the different efforts will result in market-driven solutions that provide customers with the best options. TIA houses this type of standardization efforts, such as in its Engineering Committee TR-50 M2M (Smart Device Communications).[3] Other examples of such standardization activities include:

- oneM2M, an international partnership working to develop technical specifications which address the need for a common M2M Service Layer that can be readily embedded within various hardware and software.[4]
- Open Interconnect Consortium (OIC), a group of industry leaders working together to deliver a specification and to promote an open source implementation to improve interoperability among the billions of devices making up the IoT.[5]

[3] Engineering Committee TR-50 M2M (Smart Device Communications) is responsible for the development and maintenance of access-agnostic interface standards for the monitoring and bi-directional communication of events and information between machine-to-machine (M2M) systems and smart devices, applications or networks. These standards development efforts pertain to but are not limited to the functional areas as noted: Reference Architecture, Informational Models and Standard Objects, Protocol Aspects, Software Aspects, Conformance and Testing, and Security.

[4] http://www.onem2m.org/

[5] http://openinterconnect.org/

Standardization is a form of economic self-regulation that can relieve the government of the responsibility for developing detailed technical specifications while ensuring that voluntary, consensus standards serve the public interest, saving resources that can be used to serve the public interest in other ways. TIA urges policymakers to defer to these standards as they are developed and come to define the IoT. By taking this approach, policymakers can use these standards as valuable sources of scientific and technical information developed with the assistance of private sector experts, allowing agencies to use standards as a resource for advanced technical information without first-hand independent knowledge of research in the area.

Standardization is a form of economic self-regulation that can relieve the government of the responsibility for developing detailed technical specifications while ensuring that voluntary, consensus standards serve the public interest, saving resources that can be used to serve the public interest in other ways.

At the same time, Government can help encourage the development of industry standards by funding research in cross-cutting areas such as cybersecurity and M2M interoperability for advanced communications technologies. Continued research is needed to prevent systemic attacks on IoT systems. This may provide an opportunity to create university-based cybersecurity "centers of excellence" or Federal lab-based research such as the National Cybersecurity Center of Excellence (NCCoE) at NIST. Interoperable mobility enables public safety and law enforcement officials to use the various public safety and cellular mobile networks while avoiding the necessity of carrying multiple mobile devices. It promotes coordinated communications among various public service agencies and allows higher-priority use of scarce spectrum services market and is critical for the common good. Also, bringing commercial technologies and emergency services technologies closer together will result in lower costs and more advanced features for critical emergency services.[6]

Policymakers should avoid any approach that would redefine "open standards" in a way that equates patented technology with "free" (as in without payment) or "free to use freely" (as in without payment and without any restrictions). This kind of redefinition would undermine the rights of those who have invested in the development of standardized technologies that enable the functioning of countless sectors of the economy. Technological capabilities and innovations most often result from substantial investments in research and development. Thus, if patent holders in standards-setting activities are expected to give away or waive their patent rights, there are likely to be significant adverse results, including that technology leaders will reduce or cease participation in voluntary standards-related activities; or that individuals and organizations will not invest in the development of next-generation technology in the technical areas subject to standardization, creating innovation "dead zones" in those areas.

Recommendation: Policymakers Should Employ Regulatory Approval Approaches that are Globally Harmonized, Transparent, and Streamlined

The ICT industry is one of the most far-reaching and competitive segments of the global economy. Across jurisdictions, the varying requirements of ICT present unique challenges to ensuring that governments, consumers, and other stakeholders in a diverse marketplace have the ability to determine readily whether a device has been properly certified, and to obtain additional information about a device as efficiently as possible. With the drastic increase in the number of connected things in the IoT, it will be very important for policymakers to ensure that regula-

[6] http://www.tiaonline.org/gov_affairs/fcc_filings/documents/TIA%20U.S.%20ICT%20R&D%20Policy%20Report.pdf

tory approval processes are transparent and efficient. We urge policymakers to examine their regulatory device approval mechanisms methodically to ensure that these systems are as globally-harmonized, predictable, transparent, and reliable as possible. This will promote the "build once, sell anywhere" principle, which drastically reduces regulatory costs, time-to-market, and cost to end users throughout the business and consumer markets.

The IoT will rely significantly upon maximizing continuity of connectivity. With the world rapidly becoming wireless, establishing an appropriate spectrum policy is essential to ensure that the IoT will be successful.

For example, to streamline the process ICT manufacturers must go through to get products to market, policymakers are strongly urged to consider permitting the use of Supplier Declarations of Conformity (SDoCs) for trusted classes of products as an alternative means by which an ICT manufacturer may demonstrate compliance with regulatory rules. The benefits of such an allowance include flexibility and objective treatment for manufacturers in where to have their products tested, high compliance levels, and lower administrative costs. The appropriate allowance of SDoCs would also support mutual recognition agreements (MRAs) among trading partners and widespread recognition of another country's conformity assessments, further reducing associated costs. Based on a long-standing record of compliance, many technologies have proven that very low risk exists for violating the technical rules, primarily because they are built to meet consensus technical standards, allowing policymakers to be assured that they can take this step to allow for more rapid availability of products into the marketplace at reduced cost to stakeholders, including consumers.

As a further example, the use of physical markings or labels has played a key role in providing important information about devices, but the continuous evolution of industrial design and multiple regulatory environments has led to increased costs and difficulty in ensuring that all relevant markings or labels are affixed in an efficient and convenient manner for the user of the device. An effective solution to this problem is the non-exclusive use of electronic labeling, which allows consumers and other users access to easily readable and prominently displayed information about each device. This information should include required regulatory markings and other important information, including proper device care, electronic recycling programs, and warranties. Already, through closely working with TIA, several key jurisdictions have allowed this approach.

Recommendation: Utilize a Spectrum Policy that Maximizes a Continuity of Connectivity

The IoT will rely significantly upon maximizing *continuity of connectivity*. With the world rapidly becoming wireless, establishing an appropriate spectrum policy is essential to ensure that the IoT will be successful. In commercial communications networks, mobile data use is exploding as consumers embrace smartphones, tablets and other devices. Wireless connectivity is becoming the way in which consumers access the Internet through technologies such as LTE, Wi-Fi, and satellite. Governments worldwide also have a significant dependency on spectrum for both communications and non-communications purposes.

Meanwhile, radio technologies themselves are changing, placing new demands on spectrum allocations and raising new operational and regulatory challenges. There are currently several new or emerging technologies that are competing in the marketplace to serve the Internet of Things. These include Near Field Communication (NFC), a standards-based short-range wireless technology widely linked with mobile payments. More recently, Bluetooth Low Energy (Bluetooth LE or BLE) has been built specifically to consume small amounts of energy; it is also viewed as a good candidate for small data packets sent from wearable computing devices such as smart watches and fitness trackers. Traditional Wi-Fi is also expected to play a key role, due to its low cost and ubiquity in the marketplace. Indeed, the future Internet of Things will likely be based on *heterogeneous networks* whereby devices can sequentially or simultaneously use different network technologies.

As a result of these dynamic changes, spectrum allocations and uses that may have sufficed during the 20th century are increasingly under stress. Unfortunately, policymakers are no longer writing spectrum policy on a blank sheet of paper, and virtually all spectrum suitable for mobile service has been allocated. For that reason, TIA believes that any spectrum policy must reflect the following principles to allow the use of radio spectrum to evolve to meet changing demand and promote innovation:

- ***Predictability.*** Spectrum allocations need to be predictable. Identifying demand and changes in demand, understanding the pace of radio technology development by platform, and long term planning are all essential parts of a spectrum policy that can provide predictability for both commercial and government users.
- ***Flexibility.*** For commercial allocations, flexible use policies consistent with baseline technical rules that are technology-neutral have proven to be the best approach. Any government allocations of spectrum should be managed to ensure better usage of scarce spectrum resources for all users.
- ***Efficiency.*** Policies should encourage more efficient use of spectrum where technically and economically feasible. In particular, policies should prioritize *global harmonization* and coordination of spectrum allocations;[7] protection from harmful interference for licensed uses; adjacency to similar services; and allocations of wide, contiguous blocks of spectrum. Cleared, exclusively-licensed spectrum allows the most efficient and dependable use of spectrum for commercial mobile broadband deployment.
- ***Priority.*** In cases where spectrum sharing is technically and economically possible, policies must advance good engineering practice to best support an environment that protects those with superior spectrum rights from harmful interference.

Furthermore, spectrum sharing represents a means of increasing the efficient use of spectrum and of helping to alleviate challenges in spectrum scarcity. It could eventually prove critical in enabling the *continuity of connectivity* that is so critical for the Internet of Things. In addition to ongoing efforts underway to realize successful sharing regimes, other promising efforts include the deployment of Licensed Shared Access (LSA) approaches, a "third way" spectrum management system that combines elements of traditional "command and control" spectrum management with geolocation technology, e.g., by providing users with a "token" to use spectrum at certain times/places. LSA approaches show great promise, as they provide a means of ensuring the ongoing viability of incumbent uses by creating a policy environment that enables compatible operations with new uses while also providing secondary users a means of gaining access to spectrum that is already licensed to one or more primary users, but may be underutilized or capable of supporting multiple uses.

[7] **Globally harmonized spectrum is essential to ensure the economies of scale that will facilitate the large-scale deployments necessary** to utilize the promise of new technologies fully. Global harmonization also facilitates roaming, an important part of creating the "continuity of connectivity" required for the Internet of Things.

Recommendation: Promote Efforts to Modernize Wired Media for IoT Applications

IoT applications will continue to depend heavily on wired media for various industrial applications (the deployment of parking space sensors in a garage is a basic example). High-capacity, low-cost cabling solutions that allow the connection of a multitude of increasingly sophisticated individual sensors to the network will often be essential for quality-of-service or security reasons where wireless options do not make sense. For example, excessive errors in motion control systems could cause machinery shut-downs and a break in the manufacturing process and require a manual re-set of equipment, increasing manufacturers' costs.

IoT applications will continue to depend heavily on wired media for various industrial applications.

Moreover, wired solutions generally also avoid the spectrum bandwidth constraints associated with widespread deployment of individual sensors or devices. In addition, cabling can also potentially be used to provide electrical power to the individual sensors or devices, making it essential for applications where the use of individual device batteries may be difficult.

Ultimately, as the experience with conventional Ethernet has demonstrated, the use of cost competitive and high performance cabling can lead to economies of scale in network designs and deployments.

For these reasons, standards-making bodies are making progress toward the development of next-generation cabling standards for IoT applications. The IEEE 802.3 working group is looking at channel models, cable, and connectivity for Reduced Twisted Pair Gigabit Ethernet (RTGPE).[8] In particular, there are two efforts to devise performance models for supporting 100 Mbps and 1 Gbps data rates on a single twisted pair copper cable (as opposed to the four pairs normally required), as well as providing electrical power (Power over Ethernet – PoE). Products based on these and other wired standards represent potentially smarter and cheaper alternatives to today's low-voltage wiring applications, allowing network functionalities and intelligence to move closer to the edges of a network (e.g., smarter individual sensors) rather than in a centralized device controller.

Recommendation: Utilize a Voluntary, Flexible, and Collaborative Approach to Data Security Based on International Standards

With the IoT naturally involving an ever-increasing number of "things" connected throughout society, new and evolving security issues will emerge as challenges. The ICT industry already considers security issues throughout the design process, and this approach will continue to be employed to mitigate threats in the IoT. TIA urges policymakers to regard the IoT as an opportunity for greater security, since by using a network approach paired with proper risk management techniques, IoT devices can be made to work together to produce comprehensive, actionable security intelligence in near real time. These approaches and risk management techniques are by and large driven by market demand, typically manifested through industry-driven best practices and standards developed in open, voluntary, and consensus-based fora.

[8] IEEE has also recently formed the P2413 group for the purpose of aggregating technical standards from existing IEEE efforts (such as 802.3) that may be relevant for IoT applications. *See* http://standards.ieee.org/develop/project/2413.html

To support high levels of security and resilience in the IoT, TIA urges policymakers to be guided by the following principles:

- *Respect competitive differentiation and business continuity.* As ICT manufacturers and vendors work to meet the needs of their customers, less secure products that are more vulnerable to cyber attacks will naturally be less attractive in the market. Today, this drives ICT manufacturers and vendors to strive to make their products and services less susceptible to cyber attacks, and these efforts are expected to increase dramatically.[9] The degree to which an organization's performance goals are used to ensure its ability to provide essential services while managing cybersecurity risk will depend on the specific needs of its sector and organization. However, in the ICT sector, manufacturers work with the range of organizations they supply to ensure that performance goals of those organizations are reflected in the ICT they purchase. The flexibility to innovate and the use of voluntary, consensus-based standards are both key enablers of this capability. There is no "one size fits all" solution to securing the IoT. The reach of the IoT across segments of the economy with varied levels of risk illustrates this. Government does have a legitimate role in requiring technology providers to disclose cyber risks to users (for example, the FTC has adequate authority under Section 5 of the FTC Act,[10] to stop unfair or deceptive acts or practices on a case-by-case basis using a flexible standard of reasonable security).

There is no "one size fits all" solution to securing the IoT.

- *Rely on international standards.* Numerous standards, guidelines, best practices, and tools are used by ICT manufacturers and the owners and operators of telecommunications networks to understand, measure, and manage risk at the management, operational, and technical levels. TIA urges policymakers to ensure that their approach to the IoT reflects the priority of the development of internationally-used standards and best practices. The global nature of the ICT industry necessarily requires a global approach to address cybersecurity concerns, and a global supply chain can be secured only through an industry-driven adoption of best practices and global standards. Country-specific standards should be avoided, as they would ignore the benefits of global harmonization, restricting trade in telecommunications equipment imported to or exported from other countries that are part of the global trading system. While there are legitimate public safety or security concerns, Government's role should be limited to setting performance requirements that can be flexibly addressed in standards and technical specifications – not to pick or mandate specific technologies or process methodologies. Such an approach is consistent with the United States' Department of Commerce National Institute of Standards and Technology's (NIST) *Cybersecurity Framework*,[11] which is voluntary, risk-based, and technology neutral, and relies on a variety of existing standards and other best practices to enable critical infrastructure providers to achieve resilience to cyber-based threats.

- *Utilize the successful public-private partnership model.* Public-private partnerships are an effective tool for collaboration on addressing current and emerging threats, and will serve as a key incentive encouraging businesses to make investments in cybersecurity that are appropriate for the risks they face. The voluntary, public-private model is also able to evolve in response to changes in threats and the risk environment. As both the complexity and number of attacks grow, it will be critical that policymakers leverage and augment, or create where necessary, public-private partnerships. Where industry collaboration is lacking or is not mov-

[9] http://www.gartner.com/newsroom/id/2828722

[10] *See* 15 U.S.C. § 45

[11] *See* NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0 (Feb. 12, 2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

ing forward at a pace able to address significant national needs, the Government can use its convening power to bring stakeholders together and encourage cross-sector development. Such an approach is reflected in the President's National Security Telecommunications Advisory Committee (NSTAC) report on the IoT and its impact tonational security and emergency preparedness,[12] which recommends the close collaboration of Government and industry to "coordinate, collaborate and leverage the various industry IoT consortia to develop, update, and maintain IoT deployment guidelines to manage cybersecurity implications and risks."

- *Increase end-user education.* This is a crucial aspect of improving cybersecurity in the IoT, as many cyber vulnerabilities are already known, and related attacks are relatively easy to prevent. Policymakers should lend focus to the common use of key terms and definitions related to the IoT, as well as to efforts that inform end users across the business and consumer communities of proper steps to take to ensure that proper cyber "hygiene" is impressed.

Recommendation: Ensure Flexibility and Feasibility in Addressing Data Privacy

While the IoT will bring significant societal benefits, increased connectivity also gives rise to new risks and vulnerabilities. The ICT industry recognizes privacy as a priority in the success of the IoT and understands the wide range of related concerns held by policymakers. Industry believes that IoT services must adopt principles similar to those that have worked successfully on the Internet to enable informed consumer choice: transparency about what data will be collected, how it will be used, and who will have access. We urge regulators not to adopt privacy regulations that would make it impossible for IoT systems to flourish, as full consumer benefits will require that data be retained and used in ways not currently contemplated, even by IoT innovators themselves. Instead, industry should be allowed to adopt best practices that can be responsive to fast-paced developments and that allow individual users to manage their level of data sharing. Policymakers are encouraged to ensure that their activities do not impose barriers that discourage the use of existing and developing voluntary efforts that are developed through standardization, best practice activities, and public-private partnerships to address privacy concerns. Internationally, policymakers should work towards interoperable privacy systems to avoid unnecessary impediments to the cross-border flow of information, which will be critical to the growth and functionality of the IoT.

…industry should be allowed to adopt best practices that can be responsive to fast-paced developments and that allow individual users to manage their level of data sharing. Policymakers are encouraged to ensure that their activities do not impose barriers that discourage the use of the use of existing and developing voluntary efforts that are developed through standardization, best practice activities, and public-private partnerships to address privacy concerns.

Policymakers should avoid implementing privacy obligations that are ambiguous, overly burdensome, or technically infeasible. The effect of adopting such policies would be to decrease industry's incentive to invest in IoT opportunities due to resulting regulatory uncertainty and unnecessarily higher risk. Industry members exploring IoT opportunities should have certainty and the ability to determine the most appropriate method to meet any regulatory requirements. This approach would best promote the development of the IoT, as it is a fluid and quickly evolving market opportunity. TIA believes that any Government actions should be focused in areas where the circumstances in fact raise significant privacy and security issues. For example, if data is de-identified or aggregated it does not present the same level of security or privacy concerns as other types of data.

[12] See NSTAC, NSTAC Report to the President on the Internet of Things (Feb. 19, 2014), available at *http://www.dhs.gov/sites/default/files/publications/Final%20NSTAC%20Industrial%20Internet%20Scoping%20Report_0.pdf*.

Further, Government guidance about the collection, use, and processing of data should be flexible to enable a range of possible technological means.

In addition, policymakers may serve an important role in ensuring IoT data privacy through public awareness efforts. Through “cyber hygiene” education efforts, many breaches that would result in a loss of data privacy can be avoided. In addition, a more informed end-user is less likely to make voluntary decisions with IoT devices and services that allow data usage beyond their individual comfort.

Conclusion

The IoT represents an immense opportunity for the improvement of the lives of citizens around the globe, across use cases. By ensuring that the path taken forward is collaborative and pro-innovation, consistent with the above recommendations, TIA believes policymakers can help these benefits materialize rapidly.

ABOUT TIA

The Telecommunications Industry Association (TIA) represents manufacturers and suppliers of global communications networks through standards development, policy and advocacy, business opportunities, market intelligence, and events and networking. TIA enhances the business environment for broadband, mobile wireless, information technology, networks, cable, satellite and unified communications. Members' products and services empower communications in every industry and market, including healthcare, education, security, public safety, transportation, government, the military, the environment, and entertainment. Visit tiaonline.org for more details.

TIA is accredited by the American National Standards Institute (ANSI) and is a proud sponsor of ANSI's Standards Boost Business campaign. Visit www.standardsboostbusiness.org for details.

TIA Policy Committees & Divisions

TIA conducts its policy and government affairs Innovation Agenda through membership committees. A TIA Board Member serves as TIA's Policy Chair and represents TIA's Government Affairs activities on the TIA Board of Directors.

TIA's Communications Research Division, User Premises Equipment Division, and Wireless Communications Division are also represented on the TIA Board of Directors. The Chairs and TIA Staff for each committee, working group and division can be found at http://www.tiaonline.org/policy/tia-policy-committees-divisions.

For more information on TIA's Government Affairs activities, please contact Danielle Coffey, VP of Government Affairs, at dcoffey@tiaonline.org.

Telecommunications Industry Association

Headquarters
1320 N. Courthouse Rd.
Suite 200
Arlington, VA 22201
USA
Phone: +1.703.907.7700
Fax: +1.703.907.7727

tiaonline.org

TIA®
ADVANCING GLOBAL COMMUNICATIONS