Before the
FEDERAL TRADE COMMISSION
Washington, DC 20580

In the Matter of	)
	)
Privacy and Security Implications of the Internet of Things	)
	)
	)
	)

COMMENTS OF CTIA—THE WIRELESS ASSOCIATION®

Debbie Matties
Vice President, Privacy

John Marinho
Vice President, Technology and Cybersecurity

CTIA—THE WIRELESS ASSOCIATION®
1400 16th Street, NW, Suite 600
Washington, DC 20036
(202) 736-3680

January 10, 2014

TABLE OF CONTENTS

EXECUTIVE SUMMARY

As the panelists at the FTC's recent workshop on the privacy and security implications of the Internet of Things ("IoT") discussed, the IoT holds tremendous promise and potential to improve economic productivity, individual health and well-being, and energy efficiency. And although it is developing quickly, the IoT is still in its infancy.

As the IoT unfolds, voluntary industry guidelines and market forces will protect consumers' privacy and encourage the creation of innovative security solutions. In addition, existing government policy guidelines will also provide guidance to companies as the IoT develops.

Many possible applications of the IoT have been conceived, but they will not be realized until cohesive interoperability standards have been developed to allow the IoT to grow to scale and reach its full potential. This process could take five or more years to complete. Because the data flows and associated privacy and security implications cannot be known until standards enable true interoperability, new regulation or new best practices at this time would be premature and could impede innovation. Until then, emerging connected devices will continue to present the same privacy and security issues that consumers, industry, and regulators face today.

CTIA therefore encourages the FTC to continue to use its enforcement tools and apply existing policy guidelines in a technology-neutral manner, as it has done effectively thus far to protect consumers who use connected devices. This approach will complement voluntary industry guidelines and codes of conduct, as well as the market incentives that companies already have to protect the privacy and security of consumers' data in the burgeoning IoT.

CTIA—The Wireless Association® ("CTIA") welcomes the opportunity to provide input to the Federal Trade Commission ("FTC" or "Commission") on the issues raised at the FTC's recent workshop on the privacy and security implications of the "Internet of Things" ("IoT").[1] These comments supplement comments CTIA submitted on June 1, 2013, in preparation for the workshop.

I. INTRODUCTION

CTIA is an international nonprofit trade association that has represented the wireless communications industry since 1984. Its members develop and deliver a host of products and services that are part of the rapidly developing ecosystem of connected devices. CTIA commends the Commission for hosting a balanced and informative workshop on this issue.

As the panelists at the workshop discussed, the IoT holds tremendous promise and potential to improve economic productivity, individual health and well-being, and energy efficiency. Although it is developing quickly, the IoT is still in its infancy. Indeed, as FTC Chairwoman Edith Ramirez noted in her keynote address, we are "at the dawn of the Internet of Things."[2] And just as few could fully anticipate a mere two decades ago the role the Internet would play in the lives of Americans, we do not know how innovation in the IoT will unfold and what the applications and ramifications of this transformative technology will be.[3]

---

[1] *See* FTC News Release, *FTC Seeks Comment on Issues Raised at Internet of Things Workshop* (Dec. 11, 2013), *available at* http://www.ftc.gov/news-events/press-releases/2013/12/ftc-seeks-comment-issues-raised-internetthings-workshop.

[2] Keynote Address of FTC Chairwoman Edith Ramirez, FTC Workshop: Privacy and Security Implications of the Internet of Things, Nov. 19, 2013 ("FTC IoT Workshop").

[3] *See* Paul Taylor, *CES 2014: Cisco Boss Hails 'Internet of Everything'*, Financial Times, Jan. 7, 2014 (noting Cisco CEO John Chambers believes that the IoT "will be the next and biggest wave of the internet"), *available at* http://www.ft.com/intl/cms/s/0/576d2f4c-7709-11e3-807e-00144feabdc0.html#axzz2puir5iGi**;** Adam Thierer, *Can We Adapt to the Internet of Things?*, IAPP Privacy Perspectives, June 19, 2013 (stating that the IoT "will rival the first wave of Internet innovation"), *available at* https://www.privacyassociation.org/privacy_perspectives/post/can_we_adapt_to_the_internet_of_things.

CTIA therefore encourages the FTC to take a cautious approach as it wisely did in the 1990's when the commercial Internet began to take hold. CTIA members value and have programs in place to protect the privacy of their customers' data across their platforms and services and have made efforts and will continue to devote significant resources to secure both their networks and their customers' data. CTIA members' existing compliance programs and voluntary industry guidelines can be tailored to companies' business practices and technologies, and they can be drafted and modified, as necessary, to account for the varying roles and responsibilities of different participants in the IoT ecosystem. Existing policy guidelines, including the White House Privacy Blueprint[4] and the FTC's 2012 Privacy Report,[5] will also provide guidance to companies as the IoT develops. The guidance should be interpreted in a technology-neutral way to reflect the diversity of the IoT ecosystem. These policy guidelines, operating in tandem with self-regulatory regimes and policymaker oversight, will enable appropriate information sharing so that companies can both protect the privacy and security of consumer data and bring consumers these innovative products and services that will improve quality of life, increase efficiency, and grow the economy.

Market forces also will provide incentives for companies to protect consumers' privacy and create innovative security solutions. CTIA members recognize that consumers will not embrace the IoT if they do not trust companies to safeguard the privacy and security of their data. Therefore, like all companies in the ecosystem, providers have every incentive to act in

[4] The White House, *Consumer Data Privacy in a Networked World* (Feb. 2012), *available at available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[5] *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policy Makers* (Mar. 2012) ("FTC Privacy Report"), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

consumers' interests to secure and protect the privacy of the data they collect. Indeed, CTIA's members have a long track record of protecting the privacy and security of consumer data.

New regulation or new recommended best practices at this time would be premature and could impede innovation, inhibiting the IoT's ability to reach its full potential to deliver benefits to consumers. The IoT is nascent. Its full promise depends on the development of interoperability standards that will enable seamless connectivity between devices and platforms. Standards development for the IoT has been uniquely complex, and it will take three to five years before the IoT ecosystem can support true interoperability.

Government interference at this stage, through promulgation of new regulations or new recommended best practices, could interfere with the development of standards that enable the real-time sharing of data that is critical to the proper functioning of the IoT. While the lack of standards has limited corporate investment in some aspects of the IoT, it also has encouraged innovation. In contrast, the mere announcement of plans by the government to develop regulations or recommended best practices for the IoT could chill further investment and standards development, creating uncertainty that would discourage companies from moving forward while they await the rules the government might impose. Furthermore, the data flows and the associated policy issues will not be understood until multiple players in the IoT ecosystem have adopted these standards. Until the IoT marketplace is closer to full adoption, the privacy and data security issues for connected devices will continue to be those that companies and consumers face today.

II. INDUSTRY GUIDELINES, EXISTING GOVERNMENT POLICY DOCUMENTS, AND FTC ENFORCEMENT CAN PROVIDE A FRAMEWORK TO PROTECT PRIVACY AND SECURITY AS THIS TECHNOLOGY EMERGES

Voluntary industry guidelines and codes of conduct, including those developed through a consensus-driven multi-stakeholder processes, will provide a framework to protect consumer privacy and security for new kinds of connected devices. This approach has several advantages: *First*, voluntary industry guidelines and codes of conduct allow companies to implement best practices in a manner appropriate to each company's technology and business model and in a way that protects consumers as they begin using the newest connected devices. *Second*, voluntary industry guidelines and codes of conduct are more likely to identify and address real harms while simultaneously accounting for the varying roles and responsibilities of different participants in the ecosystem. This is important because not all participants in the IoT ecosystem will have control over the data that transits the networks.[6] In addition, the IoT ecosystem involves a large number of players and data of varying sensitivity, some of which may raise few, if any, privacy issues. Industry guidelines and codes of conduct can reflect these differences and allocate responsibilities accordingly. *Third*, industry self-regulation can move at Internet speeds to adapt to the IoT.[7] Proactive industry self-regulation is better positioned to respond more quickly and effectively to consumer demands and marketplace evolution regarding consumer

[6] *See* Helen Rebecca Schindler, *et al.*, *Europe's Policy Options for a dynamic and trustworthy development of the Internet of Things*, RAND Europe, SMART 2012/0053 ("RAND Europe"), at xviii (stating that "because the 'things' of the Internet of Things act autonomously and as part of a densely linked ecosystem, sole control of the Internet of Things cannot be assumed to lie with the owners of devices or with providers of essential infrastructure services"), *available at* http://www.rand.org/content/dam/rand/pubs/research_reports/RR300/RR356/RAND_RR356.pdf.

[7] *See* Monroe Edwin Price and Stefaan G. Verhulst, *Self-Regulation and the Internet*, Kluwer Law International (The Hague, 2005), at 21 (stating that "[s]elf regulation has a greater capacity to adapt to rapid technical progress"); *see also infra* note 10.

privacy protections in the Internet Age than government regulation or new government guidance on best practices.[8]

The FTC's Privacy Report and the White House Privacy Blueprint are also sources of guidance for companies to use to develop best practices and codes of conduct at this stage of the IoT's development. As explained in more detail below, the IoT marketplace is currently fragmented and vendors are working in technology silos, which do not scale to allow the connectivity and ubiquitous computing necessary for a full-fledged IoT. The privacy issues these vendors must consider as they develop their products and services are the same as those that vendors of other products and services face today. Therefore, existing privacy policy documents provide good guidance for machine-to-machine ("M2M") vendors because they recommend incorporating privacy protections into new technology and enabling consumers to make informed decisions about how their personal data is used.

III. COMPANIES HAVE MARKET INCENTIVES TO PROTECT PRIVACY AND SECURITY

CTIA members have a long track record of protecting the privacy and security of consumer data that they collect and use. They recognize that protecting customer data not only is the right thing to do, but is a good business practice that helps them earn consumer trust and loyalty. CTIA members know that consumers will adopt the IoT only if they trust companies to protect the privacy and security of their data. Companies and consumers therefore have "aligned incentives" regarding the protection of personal information in the IoT.

[8] *See* Rolf Weber and Romana Weber, *Internet of Things: Legal Perspectives*, Springer-Verlag (2010), at 90 (stating that "continued self-regulation, for example in the form of voluntary codes of conduct, seems to be the most effective means of protecting privacy while fostering innovation").

A. CTIA MEMBERS HAVE A TRACK RECORD OF PROACTIVELY PROTECTING THE PRIVACY OF CONSUMERS' INFORMATION

CTIA members have long realized that protecting consumers' privacy is essential to maintaining consumers' trust and loyalty, and they have a strong track record of proactively protecting the privacy of information that they collect. For instance, carriers take seriously their duty to protect customer proprietary network information ("CPNI") obtained through the carrier-customer relationship and provision of telecommunications services, and they have compliance programs in place to ensure those obligations are met. In addition, in 2008, as mobile computing began to proliferate and companies began to offer location-based services ("LBS"), CTIA members recognized that consumers would use LBS only if they trusted companies to protect sensitive location information. Therefore, CTIA and members of the wireless industry developed a set of industry "Best Practices and Guidelines for Location-Based Services" ("LBS Guidelines" or "Guidelines") to promote and protect the privacy of wireless customers' location information.[9] While developing the LBS Guidelines, CTIA reached out to privacy experts from more than 90 entities, including telecommunications companies, non-profit privacy groups, and government agencies, and examined numerous privacy policies from LBS companies.

Although CTIA and its members developed the LBS Guidelines before the FTC issued its Privacy Report, the Guidelines and the Privacy Report are in agreement, which is not surprising since the Fair Information Practice Principles provide the basis for both. The Guidelines direct entities that provide LBS to inform consumers how their location information will be used and

[9] The LBS Guidelines are available at http://www.ctia.org/business_resources/wic/index.cfm/AID/11300. As CTIA noted in the comments it submitted to the FTC in this proceeding on June 1, 2013, other associations similarly have developed best practices that ensure wireless providers protect consumer privacy, keep data secure, and foster innovation and competition. *See, e.g.*, Mobile Marketing Association's Global Code of Conduct for Mobile Marketing (July 15, 2008), *available at* http://mmaglobal.com/codeofconduct.pdf.

disclosed and require that companies obtain consent before they use or disclose such information to others. In addition, the LBS Guidelines instruct companies to give consumers the ability to revoke such authorization at any time and the ability to decide when or whether their location information may be disclosed to third parties. The Guidelines also include provisions requiring proper technical, administrative and physical safeguards to protect data, as appropriate, as well as recommended limits on data retention. The LBS Guidelines are designed to be expansive in scope and can apply to *all* LBS providers in the ecosystem, including application developers, platform providers, and equipment manufacturers, in addition to wireless carriers. CTIA's LBS Guidelines are a good example of how a self-regulatory approach to privacy protection can respond to consumers' needs rapidly and effectively.[10]

B. CTIA MEMBERS WORK HARD TO ENSURE THE SECURITY OF THEIR NETWORKS

Security is a top priority for the mobile industry, which invests significant resources in security solutions and advanced technologies to protect its networks.[11] As a result, the U.S. has one of the lowest mobile malware infection rates in the world at less than two percent, compared to other countries that are in excess of 40 percent.[12] CTIA members play an important role in the development of network security solutions by participating in many public-private initiatives to

[10] A little more than a year after CTIA published the LBS Guidelines, the proliferation of smartphones and advances in LBS technologies and services converged, allowing consumers to download a growing range of mobile apps and LBS services onto their handsets, without the wireless carriers' knowledge or involvement. These new apps and services potentially affected *all* mobile device users, and not just the wireless account holders to whom the LBS Guidelines originally had been limited. In response, CTIA proactively initiated efforts to update the Guidelines to expand their protections. By March 2010, CTIA had released updated LBS Guidelines that included new requirements to ensure protections for account holders and device users alike.

[11] CTIA Cybersafety and Cybersecurity White Papers, *available at* http://www.ctia.org/policy-initiatives/policy-topics/cybersafety-and-cybersecurity.

[12] *Id.*

advance security across the industry.[13] In addition, CTIA established the CTIA Cybersecurity Working Group, a private initiative where CTIA members are building network security solutions across the wireless and telecommunications industries. By bringing together players from across the ecosystem, the industry can make sure that different kinds of companies take on security responsibilities for what they can control, including by providing consumer advisories and education to help consumers understand their role as well.

The mobile industry is now leveraging the comprehensive security solutions from the traditional wireless market to the developing IoT. The mobile industry manages M2M cybersecurity through a variety of network security management processes, including 24/7 monitoring and threat assessment, design and testing, encryption, and vulnerability management. The mobile industry continues to improve these network security management processes through advances in the following areas:

- *Monitoring and vulnerability scans* that assess and anticipate threats in real time and stop problems before they happen;
- Advances in the *monitoring of specific cyber threat profiles*, which enable companies to mount quick and effective defenses and countermeasures;
- Advanced *security technology standards*, ranging from general guidelines to specific directives, which together create a suite of security standards that can continually evolve in response to the threat environment; and

[13] The current domestic and global security initiatives working on M2M in which CTIA participates include the following: (1) oneM2M, which is a partnership of seven global/regional standards bodies working to address fragmentation in M2M standards development; (2) ATIS – The Alliance for Telecommunications Industry Solutions, which is a technical and operations standards-setting body for the entire information and communications technology industry working on critical security and interoperability issues related to M2M connections; (3) 3GPP – The Third Generation Partnership Project, which adopts standards for mobile communications and is looking into standards for M2M wireless communications; and (4) TIA – The Telecommunications Industry Association, which recently released TIA-4950, "Smart Device Communications (M2M) Reference Architecture," and is working with the OPC Foundation to support new standards for interoperability.

- *Enhancements to security policies and risk management*, which are developed by a specialty field within the security profession and which improve definitions, documentation, and processes, and provide security assessments based on ongoing scans of the threat environment.

In addition to these activities happening throughout the industry, the CTIA Cybersecurity Working Group is engaged in several ongoing efforts to adapt and leverage network security techniques and tools from today's mobile communication ecosystem for use in the M2M wireless context, including security audits, authentication, encryption, virtual private networks, immutable root-of-trust, enhanced security protocols, and multiple interface security.

Competitors in the IoT marketplace have at least as much incentive to differentiate their products through robust security on their networks as do providers in the traditional wireless environment. Although the IoT is nascent, the industry has already adapted and integrated many network security solutions into newly-released M2M technologies and services, including the following:

- AT&T's M2M home monitoring and security solutions called Digital Life, which allows users to remotely lock and unlock doors, turn appliances and lights off and on, and control home thermostats;

- Sprint's M2M-enabled health and fitness monitoring services, which are offered through partnership with a health and wellness provider;

- A joint service offered by Visa, Inc., MasterCard Inc. and American Express Co. that uses digital tokens instead of account numbers to process online and mobile purchases. Combined with EMV-chip technology, which has been widely adopted in the European Union and elsewhere, digital tokens improve authentication and overall security;[14] and

- Telefónica UK's smart grid services, for which Telefónica UK was awarded £11 billion in contracts to roll out 53 million smart meters across the United Kingdom by 2020 (the industry's largest M2M contract to-date). This project is expected to

[14] EMV, which stands for Europay, MasterCard, and Visa, is a global standard for authenticating credit and debit card transactions. *See A Guide to EMV*, EMVCo (May 2011), at 6, *available at* https://www.emvco.com/download_agreement.aspx?id=599.

result in £6.7 billion in reduced energy consumption and more efficient management and deployment of electricity services across the UK.

As the IoT grows, so too will the demand for security solutions, the market for which, by some estimates, is expected to reach nearly $1 billion annually by 2018.[15] Not only do these security investments protect consumer data, they are part of the virtuous cycle of innovation and investment that has led to the growth of mobile technology generally and that will lead to the expansion of the IoT.

C. COMPANIES CAN MEET CONSUMER EXPECTATIONS FOR DATA PRIVACY AND SECURITY IN THE IOT

Consumer trust in companies' ability to protect data privacy and security will be critical to the growth of the IoT. As Chairwoman Ramirez said at the workshop, "consumers will enthusiastically invite the Internet of Things into their homes, cars, and workplaces only if they're confident that they remain in control over their data."[16] Carolyn Nguyen, Director of Microsoft's Technology Policy Group, echoed this sentiment when she explained in her keynote address that the successful companies in the IoT will be those that are capable of earning consumers' trust.[17] Indeed, it is widely understood that even "perceived abuse" by industry "could lead to a societal rejection of" the IoT.[18]

Companies and consumers therefore have what Nguyen called "aligned incentives," which will ensure that companies continue to be proactive in protecting privacy and security in the new era of M2M communications. For instance, many M2M products and services will

---

[15] *Worldwide Internet of Things (IoT) 2013-2020 Forecast: Billions of Things, Trillions of Dollars*, International Data Corporation (Oct. 1, 2013), *available at* http://www.marketresearch.com/IDC-v2477/Worldwide-Internet-Things-IoT-Forecast-7854102/.

[16] Keynote Address of FTC Chairwoman Edith Ramirez, FTC IoT Workshop.

[17] Keynote Address of Carolyn Nguyen, Director, Microsoft Technology Policy Group, FTC IoT Workshop.

[18] *See* RAND Europe at 43.

involve ongoing relationships with consumers throughout the life of the product or service. Companies will want to ensure consumer loyalty by providing M2M products and services with appropriate security updates to prevent and address problems, if and when they are discovered. In addition, because there is every reason to expect robust competition in the marketplace for IoT products and services, companies likely will want to win consumer trust and loyalty by offering strong data privacy and security protections.[19]

IV. IT IS TOO EARLY FOR THE FTC TO RECOMMEND NEW PRIVACY AND SECURITY GUIDELINES OR BEST PRACTICES FOR THE IOT

Global corporations continue to support the development of open standards that will allow the IoT to grow to scale, and companies will make more significant investments in the IoT after interoperability standards have been established. Although standards bodies have initial efforts underway, they face a variety of complexities. It will take years before standards support true interoperability for the IoT. In the meantime, premature legal, regulatory, and policy roadblocks could slow this process and prevent the nascent IoT from reaching its full potential.[20]

A. CURRENTLY, PROPRIETARY M2M SYSTEMS OPERATE IN ISOLATION FROM ONE ANOTHER, AND IT WILL BE MANY YEARS BEFORE STANDARDS ALLOW TRUE INTEROPERABILITY AND COMPLETED VALUE CHAINS

As explained in *Standards Development in the Internet of Things* (*see* Appendix),[21] the establishment of common standards and platforms for the IoT is a predicate for significant

[19] *See e.g.*, Presentation of Kenneth Wayne Powell, General Manager and Senior Executive Engineer of Electrical System, Toyota Technical Center, FTC IoT Workshop (explaining how Toyota has incorporated "security by design" in its connected cars to segregate internal operating systems from connected systems that communicate with the outside world).

[20] *See* Paul Kominers, *Interoperability Case Study—Internet of Things*, Berkman Center for Internet & Society Publication No. 2012-10 (Apr. 2012), at 10-12 ("Interoperability Case Study—IoT") (stating that "legal inhibitions," including "data protection" requirements, are among the potential impediments to systemic interoperability in the IoT), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2046984.

[21] Charles Bokath, *Standards Development in the Internet of Things*, (Jan. 2014) ("Bokath White Paper") (attached as Appendix).

investment and growth in the IoT. The "value chain" that will allow the IoT to reach its full promise requires standards that will enable interoperability between many devices, networks, providers, and services, and that will simplify application development.[22]

The standard-setting process has gotten underway but is expected to take years to complete. Scores of organizations have an interest in M2M standardization.[23] Participants in the standardization process are working to accommodate a diverse set of players that represent different industry sectors with competing requests and goals.[24] IoT devices are often constrained in memory, processing capacity, and size, and they vary in capacity depending on their vertical application.[25] As a result, IoT standard setting is uniquely more time consuming than other standard-setting processes, and standards and middleware (the inter-standards "glue") each will require years to establish.[26]

Companies are devoting significant resources to setting standards and developing middleware so that they can create vertical and horizontal value chains to connect devices, networks, delivery platforms, applications, and users across multiple industry sectors. Though it will take three to five years to work through the complexities, their efforts will result in

---

[22] *See* Bokath White Paper at 2; *see also* Interoperability Case Study—IoT at 4 (stating that "[a]t its core, achieving such point-to-point communications fundamentally relies on interoperability"); Liat Ben-Zur, *Connecting Things to the Internet Does Not an Internet of Things Make*, Wall Street Journal, All Things D (May 8, 2013) (stating that the IoT, which has not arrived yet, requires "openness and flexibility" and the "ability to work across heterogeneous networks and heterogeneous devices"), *available at* http://allthingsd.com/20130508/connecting-things-to-the-internet-does-not-an-internet-of-things-make.

[23] Bokath White Paper at 3.

[24] *Id.*

[25] *Id.*

[26] *Id.* at 3-4*; see also* Don Clark, *'Internet of Things' in Reach*, Wall Street Journal, Jan. 5, 2014 (noting that "agreements on key communications technologies may be five to 10 years away"), *available at* http://online.wsj.com/news/articles/SB10001424052702303640604579296580892973264; Kevin Fitchard, *why we need a standard for the Internet of things*, GigaOM, July 12, 2012 (stating that the "issue of fragmentation among bands and technologies [that would connect M2M systems] isn't going to get worked out any time soon"), *available at* http://gigaom.com/2012/07/12/internet-of-things-standard.

connections that will enable true end-to-end M2M solutions that will work together to deliver immense new benefits to consumers and society.[27]

B. PREMATURE FTC ACTION COULD DELAY IOT INTEROPERABILITY AND WOULD ADDRESS SPECULATIVE, NOT KNOWN, PRIVACY AND SECURITY RISKS

Standards bodies' processes are designed to consider broad industry requirements, including security and "privacy by design." As the multiple players in the ecosystem develop and adopt interoperability standards, they can identify and address new privacy and security risks associated with new data flows. Thus, new best practices (or even a rigid application of the Fair Information Practice Principles) are premature because it is not known yet how the data flows will affect consumers.[28] As the Chartered Institute for IT and the Oxford Internet Institute noted in their recent report about the IoT, "too many of the properties of complex Internet of Things systems are emerging properties … that can only be fully understood after development."[29]

---

[27] Bokath White Paper at 5; *see also* Don Clark, *'Internet of Things' in Reach*, *supra* note 26 (stating that the "much-ballyhooed Internet of Things still is largely a collection of possibilities" because of "a number of stumbling blocks that could slow investment," such as "conflicting wireless-communications standards"), *available at* http://online.wsj.com/news/articles/SB10001424052702303640604579296580892973264; Tony Danova, *An Important Piece To 'The Internet Of Things' Puzzle Is Still Missing*, Business Insider, Dec. 18, 2013, (stating that before the IoT "can happen, a standard for storing data and connecting each of these devices needs to be created" and "[w]ithout it, these devices may not ever function to their full potential"), *available at* http://www.businessinsider.com/an-important-piece-to-the-internet-of-things-puzzle-is-missing-2013-12; Christopher Mims, *Here's the one thing someone needs to invent before the internet of things can take off*, Quartz, Dec. 17, 2013 (explaining that "a critical piece of the internet of things puzzle remains to be solved" because "many objects on the internet of things [still] can't share data with one another"), *available at* http://qz.com/158782/heres-the-one-thing-someone-needs-to-invent-before-the-internet-of-things-can-take-off; Pierre-Marie Mateo, *Internet of Things Needs Standards in Order to Make Headway*, L'Atelier Trends, Nov. 27, 2013 (noting that "a lack of standards and systems integration means that the data is for the most part being produced in silos"); *available at* http://www.atelier.net/en/trends/articles/internet-things-needs-standards-order-make-headway_425738.

[28] *See* RAND Europe at 58; *see also* Presentation of Marc Rogers, Principal Security Researcher, Lookout, Inc., FTC IoT Workshop (stating that regulation is premature, as we do not even understand yet all of the questions that the IoT raises).

[29] *The Societal Impact of the Internet of Things*, BCS – The Chartered Institute for IT/Oxford Internet Institute Forum Report (Mar. 2013) ("Chartered Institute/Oxford Internet Institute Forum Report"), at 8. The Chartered Institute for IT/Oxford Internet Institute Forum Report also notes that it is still not clear at

Because we have not yet seen problems necessitating an IoT-specific regime, the FTC will be in a better position to determine whether additional best practices are necessary after industry develops interoperability and security standards. At that time, the FTC will be able to identify and address real, known risks, instead of speculative ones.[30] Until then, because of a lack of interoperability between devices and the siloed nature of the IoT, privacy and data security issues for connected devices will continue to be those that companies and consumers face today.

Premature promulgation of new best practices also could further complicate the creation of standards that enable the real-time sharing of data, which will be the lifeblood of IoT development. Data flows are the key to innovation and the "foundation for a new economy."[31] The technical and operational data that connected devices generate will be essential to the proper functioning of the IoT.[32] Much of this data, even when aggregated with other data, will not be personally identifiable and will not raise the privacy concerns associated with personal information.[33] If the FTC acts at this early stage of the IoT's development before anyone has had a chance to understand how the IoT actually will function, it risks imposing a regime that unnecessarily restricts data flows that pose no risk to privacy, but that will be essential to

---

this stage of the IoT what would be "suitable privacy models that [could] support sharing of personal identifiable information in an ecosystem of private and commercial entities, and that at the same time [could] satisfy end users' preferences." *Id.*

[30] But even then, because the IoT is a concept representing an ecosystem of diverse industries, vendors, applications, types of data, and use-cases, it does not lend itself to the kind of targeted guidance that the FTC has issued for other discrete technologies, such as mobile applications and facial recognition technology.

[31] Keynote Address of Carolyn Nguyen, Director, Microsoft Technology Policy Group, FTC IoT Workshop; *see also* RAND Europe at 7 (stating that connected devices in the IoT will produce "data, the collection, storage, combined processing and ubiquitous availability of which will become increasingly important").

[32] Presentation of Marc Rogers, Principal Security Researcher, Lookout, Inc., FTC IoT Workshop.

[33] *Id.*

realizing the benefits of the IoT. Furthermore, if the FTC issues new best practices that would require consumers to take action frequently in order to facilitate data flows between connected devices (by giving frequent and numerous consents, reading too many notices, or entering security codes, for instance), consumers may not use connected devices or fully reap the benefits this technology may offer.[34] If the FTC waits until standards have been developed and adopted to consider whether new best practices for the IoT are necessary, it will enable the IoT to grow and can ensure that it identifies and addresses real privacy and security risks that consumers may face in the future.

V. CONCLUSION

The IoT promises to bring great economic and societal benefits and improve quality of life for consumers. But the IoT is still in its infancy. Although many possible applications of the IoT have been conceived, they will not be realized until cohesive interoperability standards have been developed to allow the IoT to grow to scale and reach its full potential. This process could take five or more years to complete. Because the data flows and associated privacy and security implications cannot be known until standards enable true interoperability, new regulation or new best practices at this time would be premature and could impede innovation. Until then, emerging connected devices will continue to present the same privacy and security issues that consumers, industry, and regulators face today.

CTIA therefore encourages the FTC to continue to use its enforcement tools and apply existing policy guidelines in a technology-neutral manner, as it has done effectively thus far to protect consumers who use connected devices.[35] The White House Privacy Blueprint and the

[34] Presentation of Anand Iyer, President and COO, WellDoc Communications, Inc., FTC IoT Workshop.
[35] *See In the Matter of TRENDnet, Inc.*, F.T.C. File No. 122-3090 (Sept. 4, 2013) (Complaint), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/09/130903trendnetcmpt.pdf.

FTC Privacy Report, coupled with the FTC's enforcement authority under Section 5, will complement voluntary industry guidelines and codes of conduct, as well as the market incentives that companies already have to protect the privacy and security of consumers' data in the burgeoning IoT. This approach will allow companies to innovate and develop the IoT and ensure that informed consumers can reap the benefits of the IoT while knowing that their privacy is protected and their data is secure.

CTIA looks forward to working with the Commission as it continues to monitor the development of the IoT and examine the issues that it raises.

Respectfully submitted,

/s/

Debbie Matties
Vice President, Privacy

John Marinho
Vice President, Technology and Cybersecurity

CTIA—THE WIRELESS ASSOCIATION®
1400 16th Street, NW, Suite 600
Washington, DC 20036
(202) 736-3680

January 10, 2014

Standards Development in the Internet of Things

Chuck Bokath

January 10 2014

Introduction

While the Internet of Things (IoT) does not have a single, widely-accepted definition, it can be described as a growing set of objects, or "things," that might include tags, sensors, and a variety of devices that interact with each other and with distributed software applications. IoT is the application domain of Machine to Machine (M2M) communications, which provides the plumbing that enables the IoT ecosystem.[1] The IoT will comprise tens to hundreds of billions of heterogeneous and pervasive objects.[2] These objects will have limited capacity, be uniquely addressable, and become increasingly intelligent and autonomous.

Today's IoT industry is in its infancy, with proprietary vertical silos using multiple communication stacks that are tightly coupled and embedded along with nonstandard constrained devices.[3] This currently prevents devices and objects in the IoT from communicating with one another across multiple and diverse platforms. Industry Standards groups are working to provide a cohesive set of standards to enable global M2M interoperability for the IoT. De facto standards will encourage companies to make more significant investments in the IoT and will spur its growth. Until then, for several years, M2M applications will remain limited to proprietary implementations with incomplete value chains and will lack interoperable cross-market applications. Over the next three to five years, standards development and adoption will lead toward industry evolution and maturity.

---

[1] Eric N. Barnhart, P.E. and Charles A. Bokath, "Considerations for Machine-to-Machine Communications Architecture and Security Standardization", http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6156367 (2012).

[2] Constantine A. Valhouli, "The Internet of things: Networked objects and smart devices", The Hammersmith Group, http://thehammersmithgroup.com/images/reports/networked_objects.pdf, (2010).

[3] Stuart Revell, "Machine to Machine Communications (M2M) Challenges and opportunities", https://connect.innovateuk.org/documents/3077922/3726367/IoT+Challenges,%20final+paper,%20April+2013.pdf/38cc8448-6f8f-4f54-b8fd-3babed877d1a, (2013)

Industry Investment in the Internet of Things

'C-level' executives eagerly anticipate getting a slice of the projected $14.4 trillion global market,[4] but often find M2M adoption challenging in the current landscape. According to executives, the greatest accelerant to IoT investments are broadly adopted interoperable standards that result in a well-connected value chain.[5] Without a well-connected value chain, companies are unable to produce sustainable business models that can support the forecasted revenue opportunities. Other considerations like competing interests across industry participants and protection of intellectual property also are complicating development of IoT. Additionally, thus far corporations have been unable to find within today's fragmented IoT market quick wins that might boost confidence in M2M platform solutions and spur more investment in IoT technologies. As a result, while global corporations' investments are spurring innovations in M2M and IoT, they have been limited while standards are being developed and the promises of savings and efficiencies may be far off. When companies invest, they need to convince several layers of management that an investment proposal makes sense, which has slowed sales cycles.[6]

Global Standardization for the Internet of Things

Standardization is the accelerant that lowers operating and capital expenses, speeds up time to market, and simplifies application development.[7] The IoT market requires strong industry standards to promote long-term technology investments.[8] Standards are the building blocks that allow different elements within the IoT to evolve and innovate while maintaining interoperability and service delivery.

In Standards Development Organizations (SDOs), typical development cycles have many steps, including Initiating, Mobilizing the Workgroup, Drafting the Standard, Balloting the Standard,

---

[4] Joseph Bradley, Joel Barbier, Doug Handler, "Embracing the Internet of Everything To Capture your share of $14.4 Trillion", http://www.cisco.com/web/about/ac79/docs/innov/IoE_Economy.pdf#page=1, 2013, Cisco.

[5] Value chains are the building block components within a vertical application that cohesively link devices, data networks, platforms and applications creating an end to end interoperable IoT solution.

[6] David Wood, "Breakthroughs with M2M: moving beyond the false starts", http://dw2blog.com/2013/05/18/breakthroughs-with-m2m-moving-beyond-the-false-starts, 2013.

[7] Eric Klein, "M2M and the Importance of Standards", http://www.vdcresearch.com/maw/13_EMOB_MAW_View_July_M2MStandards_EK_1.pdf, 2013, VDC Research.

[8] Emmanuel Darmoius and Omar Elloumi, "M2M Communications: A Systems Approach", (Wiley; 1 edition April 30, 2012) .

and Gaining Final Approval. Under ideal circumstances, this multi-step process takes approximately 12 to 18 months, though in a difficult standards cycle, it can take as long as 48 months.[9]

Devices in the IoT are often constrained in memory, processing capacity, and size. Just as important, IoT devices will vary in capacity depending on their vertical applications. These constraints and capacity variabilities generate more potential requirements and options for standards. SDOs must consider stakeholders' differing opinions on these requirements and options, which makes IoT standard-setting uniquely more time consuming than it is for other standards processes.[10]

Presently, many organizations have a direct or indirect interest in M2M standardization.[11] Participants in standardization review processes work very hard to accommodate different industry sectors' competing requests, agendas, and goals, but the industry is still currently fragmented.[12]

To address the fragmentation, seven global regional SDOs have partnered to create a unified global standards body, oneM2M, that is designed to drive global acceptance of the technology.[13] However, oneM2M is not slated to deliver a first release of a limited M2M technical specification until late 2014.[14]

---

[9] "Develop Standards", http://standards.ieee.org/develop/process.html, IEEE-SA

[10] For instance, working groups such as the Internet Engineering Task Force (IETF) are introducing new protocols that attempt to solve the constrained issue in networking. New companies, such as Jasper, are working on providing efficient data transit capabilities through AT&T's network. Software companies are creating platforms to interoperate with various networking technologies. Enhanced Service Delivery Platform (SDP) organizations, such as the ALLSEEN Alliance and M2M Industry Working Group, need to interoperate with the multitude of application protocols based on capabilities of the device.

[11] "GSC MSTF preliminary list of global organizations, groups, associations and other entities with a direct or indirect interest in machine-to-machine (M2M) standardization", http://www.tiaonline.org/standards/mstf/documents/Global_M2M_Standardization_Task_Force-M2M_Activity_Mapping_GSC-16_Report_Halifax_rev2_0.pdf, October, 2011.

[12] Mike Bushong, "More on Open: Standards", http://www.plexxi.com/2013/06/more-on-open-standards/#sthash.KGs995bL.dpbs, 2013, Plexxi Inc.

[13] Eric Klein, "M2M and the Importance of Standards", http://www.vdcresearch.com/maw/13_EMOB_MAW_View_July_M2MStandards_EK_1.pdf, 2013, VDC Research.

[14] "oneM2M WI-0003 Roles and Focus Areas", http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CC4QFjAA&url=ftp%3A%2F%2Fftp.onem2m.org%2FWork%2520Programme%2FWI0003%2FoneM2M-WI-0003-VocabPrinciples-

In addition to oneM2M, other SDOs,[15] industry working groups,[16] and government agencies[17] are working on and publishing their own updates on multiple proprietary architectures, security schemes, and communication protocols. Dozens of other organizations are creating new or adapting proposed standards based on their own interests or geographic technical or legal requirements.[18] Global industry has the resources and motivation to work through the complexities, but it will take time.

Development of Inter-Standards Middleware

Although the establishment of standards is necessary for market acceleration, true interoperability will be realized through middleware (inter-standards "glue") that fills the gaps between standards that do not fully meet the needs of the market.[19] After the standards have been defined, IoT platform vendors will need to develop middleware to create interoperability between each of the technologies defined by SDO-ratified standards. The development of middleware will add as much as 18 to 24 months to the standards development cycles.

V1_2.DOC&ei=n_LKUvamIZC_kQeTtIDACQ&usg=AFQjCNFk_UsX-DlvzLOShPQ339Tn-Kqxbg&sig2=gkYhkOFGp62N5nHqNaktQA&bvm=bv.58187178,d.eW0, 2013, oneM2M Work Programme.

[15] Examples include Internet Engineering Task Force; Association of Computing Machinery (ACM); Third Generation Partnership Project 2 (3GPP2); Inter-American Telecommunication Commission; Internet Protocol for smart object communications (IPSO); Organization for the Advancement of Structured Information Standards; Open DeviceNet Vendors Association; and Open Services Gateway Initiative (OSGi).

[16] Examples include M2M Industry Working Group (M2MIWG); ALLSEEN Alliance; Open Services Gateway Initiative (OSGi) Alliance; SIM Alliance; Zigbee Alliance; Continua Alliance; and Weightless Special Interest Group.

[17] Examples include U.S. National Institute of Standards and Technology (NIST); U.S. National Science Foundation (NSF); ICT Standards Advisory Council of Canada (ISACC); Administration of Quality Supervision, Inspection & Quarantine of the People's Republic of China (AQSIQ); and International Organization for Standardization (ISO).

[18] Examples of other organizations include International Telecommunications Union (ITU); M2M Standardization Task Force *(*MSTF); Internet Protocol for Smart Object Communications (IPSO); Telecommunications Industry Association (TIA); CDMA Development Group (CDG); GSM Association (GSMA); Open Mobile Alliance (OMA); Institute of Electrical and Electronics Engineers (IEEE); Association of Radio Industries and Businesses (ARIB); Alliance for Telecommunications Industry Solutions (ATIS); and China Communication Standardization Association (CCSA)

[19]Sean Horan "4 Reasons to Justify M2M Middleware Solutions", http://networkingexchangeblog.att.com/enterprise-business/4-reasons-to-justify-m2m-middleware-solutions/, 2012, AT&T.

Realization of Value Chains and the IoT Ecosystem

The creation of standards promotes the development of IoT value chains; value chains provide functional components or building blocks that when combined with middleware enable a cohesive, end-to-end M2M solution.[20] Five key segments of a value chain – devices, network, delivery platform, applications, and customers – provide critical services that need to interoperate across the segments' functional lines in a standard process.[21] Although standards provide the bedrock to interconnect the segments, cross-industry efforts will be needed to connect all the segments of a value chain and allow companies to support IoT and address every day, real-world scenarios. A connected value chain will enable vertical markets to grow and flourish. When the vertical markets are able to *interoperate* across industries' horizontal market segments, then a global IoT ecosystem can be established.[22]

Conclusion

Today's connected devices operate in proprietary technology silos. Development of standards and middleware will drive greater investment in the IoT. A realistic horizon for cross-sector interoperable standards and middleware in the global IoT ecosystem is three to five years.

[20] Emerson, Bob, "M2M: the Internet of 50 Billion Devices", http://m2m.com/servlet/JiveServlet/downloadBody/1043-102-1-1033/M2M_Magazine_The_internet_of_50_billion_devices.pdf#page=1, 2012, M2M Magazine.

[21] David Escandon , "A QNX Neutrino Primer of Embedded Designers, Part One" http://www.arrownac.com/solutions-applications/embedded/eblog/?q=node/58, 2013, Arrownac Inc.

[22] A vertical market is a set of services that are available to M2M applications within one industry segment that satisfy one or all the components of the IoT value chain. Two examples would be *Asset Tracking* and *Automotive Vehicle-Vehicle*, which are services that incorporate diagnostic, location and monitoring systems. A horizontal market is a coherent framework that is valid across a large variety of business domains, networks, and devices; it is a set of technologies, architectures, and processes that will interoperate across market segments.

ABOUT

Besides starting and operating Blind Tiger Communications, Chuck Bokath is a Senior Research Engineer at the Information and Communications Laboratory at the Georgia Tech Research Institute, working largely in the cyber-security and commercial wireless industries. Mr. Bokath has 25 years experience in the wireless telecom, forensics and security industries. Mr. Bokath has been interviewed and has spoken as a subject matter expert on privacy, exploitation, cyber-security within the commercial mobile wireless industry in numerous seminars, tradeshows, newspapers, and radio programs, including the New York Times, CBS Radio, and CNN.

Mr. Bokath is the Cyber-security Chair of the North American Standards Body, TIA, and has authored several standards for the Machine to Machine ecosystem within that organization. Mr. Bokath has entered security contributions to the oneM2M global standards development organizations, which are currently pending adoption. Additional standards work includes member of the North American TIA delegation to the Global Standards Delegation, member of the Georgia Tech M2M Delegation to ITU M2M Focus Group, and expert contributor for creation of the Java Wireless Messaging Standard (JSR-120).

Mr. Bokath founded Blind Tiger Communications to solve a problem in the majority of the nation's prisons: smuggling and use of illicit use of mobile devices to threaten, launder money, and continue operate unlawful businesses inside prison walls. Mr. Bokath has used his intimate knowledge in the cyber security and wireless industries to create Mobile Soap - a wireless managed access system to detect, defeat, and collect data from these illicit mobile devices.