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®

Michael F. Altschul
Senior Vice President, General Counsel

David Diggs
Vice President, Wireless Internet Development

John Marinho
Vice President, Technology and Cybersecurity

Debbie Matties
Vice President, Privacy

CTIA-THE WIRELESS ASSOCIATION®
1400 16th Street, NW, Suite 600
Washington, DC 20036
(202) 785-0081

June 1, 2013

TABLE OF CONTENTS

EXECUTIVE SUMMARY

CTIA's members develop and deliver a host of products and services that are part of the Internet of Things – a rapidly growing ecosystem of connected devices that collect and transmit data between and among themselves. The Internet of Things promises to improve the quality of life by automating personal tasks and industrial and agricultural operations and by revolutionizing medical, scientific, and commercial research through "big data" analytics.

The Federal Trade Commission's workshop on the privacy and security implications of the Internet of Things is an opportunity to learn from CTIA's members and other relevant stakeholders. The FTC should consider including:

- Manufacturers, developers, and providers of devices and services;
- Consumers;
- Telecommunications providers; and
- Entities and individuals who use connected devices and the data they collect to improve public welfare.

A diverse group of workshop participants will ensure the Commission receives balanced input on both the privacy and security issues and the consumer and societal benefits attributable to the Internet of Things.

Indeed, the Internet of Things ecosystem involves a large number of players in the mobile space; a range of platforms, device formats, and services; and data of differing sensitivity. A privacy and security framework should reflect this diversity and should not vary depending on the type of device or technology used to collect or transmit data. In addition to being technology-neutral, any framework should be flexible enough to allow companies to innovate and grow.

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®

CTIA–The Wireless Association® ("CTIA") welcomes the opportunity to provide input to the Federal Trade Commission ("FTC" or "Commission") on the privacy and security implications of the "Internet of Things" in preparation for the Commission's upcoming workshop on this issue.[1]

I. INTRODUCTION

CTIA is an international nonprofit trade association that has represented the wireless communications industry since 1984. CTIA's members develop and deliver a host of products and services that are part of the rapidly developing ecosystem of connected devices. Until relatively recently, wireless services and devices, such as smartphones and tablets, primarily allowed *people* to connect with each other. Now, *things* – such as appliances, vehicles, machinery, and other mobile and stationary objects – are increasingly linked to each other and to individuals through sensors and both wireless and wireline connections, forging an interactive and automated world of connected devices. The Internet of Things describes our increasingly connected world where "virtually every physical thing…can also become a computer that is

[1] *See* FTC News Release, *FTC Seeks Input on Privacy and Security Implications of the Internet of Things* (April 17, 2013), *available at* http://www.ftc.gov/opa/2013/04/internetthings.shtm.

connected to the Internet."[2] Indeed, the number of wireless connections in the United States has grown by 70 million over the last five years, and now exceeds the nation's population,[3] due in large part to the proliferation of wirelessly connected devices in the developing Internet of Things.

The Internet of Things is growing at a staggering rate and without any fixed boundaries. Its ecosystem evolves continually through a virtuous cycle of innovation and investment resulting from the efforts of service providers, infrastructure vendors, device manufacturers, operating systems developers, and applications developers. Thus, as each of these different sectors develops and introduces new technologies, the other sectors are spurred to further innovation, and consumers and businesses enjoy the benefits of an ever more connected life.

The FTC's upcoming workshop on the privacy and security implications of the Internet of Things is an opportunity to learn from all of the relevant stakeholders in this multifaceted ecosystem. These stakeholders include companies that manufacture products and services that are part of the Internet of Things, consumers who use connected devices, providers of various technologies that enable connectivity, companies that manufacture security solutions for the Internet of Things, and entities and individuals who use data from connected devices to improve public welfare. A diverse group of workshop participants will ensure that the Commission receives balanced input on both the privacy and security issues and the consumer and societal benefits attributable to the Internet of Things.

---

[2] Elgar Fleisch, *What is the Internet of Things? An Economic Perspective*, Auto-ID Labs White Paper WP-Bizapp-053 at 3 (Jan. 2010), *available at* http://www.autoidlabs.org/uploads/media/AUTOIDLABS-WP-BIZAPP-53.pdf.

[3] *See* CTIA, *Wireless Quick Facts*, http://www.ctia.org/media/industry_info/index.cfm/AID/10323.

In order to protect consumers and realize the benefits of connected devices, any privacy and security framework must be technology-neutral so that it can accommodate a range of technologies and marketplace participants. It must also be flexible enough to enable the free flow of data that is the lifeblood of the Internet of Things. A combination of industry best practices, regulatory policy guidelines, and multi-stakeholder and industry-led efforts will enable the wireless industry to both protect the privacy and security of consumer data and bring consumers these innovative products and services that improve quality of life, increase efficiency, and grow the economy.

II. CTIA MEMBERS DEVELOP PRODUCTS AND SERVICES THAT ARE PART OF THE INTERNET OF THINGS

Although some devices may be connected by wires, wired connections are often impractical, too costly, or both. Moreover, wired connections are limited to devices at fixed locations where wireline access is cost effective. Wirelessly connected devices can be mobile, while others may be at fixed locations where wireline access is scarce or nonexistent, such as along a riverbed or a highway. Wireless connectivity is therefore critical to the Internet of Things.[4] CTIA's carrier members provide the wide-area wireless networks that connect both mobile and fixed devices and make them part of the Internet of Things. CTIA's supplier members develop and build the infrastructure, both hardware and software elements, that allows these wireless networks to deliver nearly ubiquitous connectivity, as well as the connected devices and applications that make up the endpoints of the Internet of Things.

[4] ABI Research, *Over 30 Billion Wireless Connected Devices to be Part of the IOE in 2020* (May 2013), *available at* https://www.abiresearch.com/research/product/1016390-over-30-billion-wireless-connected-devices/ ("ABI Research") (stating that "[a]lthough wired solutions play a part in the [Internet of Things] market, it is the wireless solutions that will be the major enablers").

Although still in its infancy, the Internet of Things is projected to comprise between 30 *billion*[5] and 50 *billion* machine-to-machine ("M2M") devices worldwide by 2020,[6] compared to an estimate of about 80 *million* M2M wireless devices in 2010.[7] Some analysts estimate that there will be 1 *trillion* connected devices in the combined consumer and industrial sectors by 2025.[8]

CTIA members have engaged in extensive M2M development projects. For example, Verizon Wireless facilitates transportation asset tracking, remote monitoring of bike-shares, management of municipal fleets, smart metering, and automotive telematics.[9] Another CTIA carrier member, AT&T Mobility, features a program for monitoring patients' heart data as well as other medical conditions,[10] and is "embedding wireless capabilities into . . . eReaders, dog collars, pill caps, photo frames, car ignition switches, smart meters, and more."[11] AT&T also offers an automated home service, Digital Life, which allows customers to "turn down their thermostats from the office, lock the doors remotely, check on pets or loved ones, or monitor for

---

[5] *Id.*

[6] *See* OECD, *Machine-to-Machine Communications: Connecting Billions of Devices*, OECD Digital Economy Papers, No. 192, at 7, 8 (Jan. 2012) ("OECD Report"), *available at* http://dx.doi.org/10.1787/5k9gsh2gp043-en (*citing* Ericsson, *Annual Report 2010*, at 18 (2010), *available at* http://www.ericsson.com/thecompany/investors/financial_reports/2010/annual10/sites/default/files/Ericsson_AR_2010_EN.pdf); *accord* Dave Evans, Cisco, *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything*, at 3 (Apr. 2011), *available at* http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf; *see also* Ericsson White Paper, *More than 50 Billion Connected Devices* (Feb. 2011), *available at* http://www.ericsson.com/res/docs/whitepapers/wp-50-billions.pdf.

[7] *See* OECD Report at 8 (citing an estimate by Berg Insight).

[8] Bill Wasik, *Welcome to the Programmable World*, WIRED, at 142 (June 2013).

[9] *See* Verizon, *Connected Machines, Unlocked Potential*, *available at* http://www.verizonenterprise.com/solutions/connected-machines/.

[10] *See* AT&T, *Machine-to-Machine (M2M)*, *available at* http://www.business.att.com/enterprise/Family/mobility-services/machine-to-machine/.

[11] *See* AT&T, *AT&T M2M (Machine to Machine) Communications Snapshot*, *available at* http://www.att.com/Common/about_us/files/pdf/M2M_Snapshot.pdf.

intruders."[12] In addition, Snaptracs, a subsidiary of CTIA member Qualcomm, offers Tagg, a GPS-enabled dog collar that allows pet owners to monitor their pets' locations and activities.

III. FTC'S WORKSHOP SHOULD INCLUDE A FULL RANGE OF INTERESTED PARTIES

The FTC's workshop is an opportunity to learn from all relevant stakeholders, including companies that do not manufacture consumer-facing products and entities and individuals who can explain the societal benefits of the Internet of Things.

Manufacturers, Developers, and Providers of Devices and Services

The Commission can get an overview of the range of devices and services that comprise the Internet of Things from the following entities:

- Manufacturers of smartphones, tablets, and the other "hub" devices from which consumers can control their interaction with connected devices;
- Manufacturers of connected vehicles, such as trucks, trains, aircraft, and boats;
- Makers of connected devices and appliances that monitor health and fitness (sometimes called mHealth or connected health);
- Manufacturers of "smart" appliances for automated home systems (*e.g.*, thermostats, alarm systems, HVAC systems, and Internet-connected appliances);
- Developers of "smart" enterprise solutions, such as automated and connected systems for industrial equipment and technology used for inventory management;
- Cloud-based service providers that will store and process the data that connected devices collect and use; and

[12] Brad Smith, *CTIA Day 1: The Future is Now for Connected Homes*, Wireless Week, May 21, 2013, *available at* http://www.wirelessweek.com/news/2013/05/ctia-day-1-future-now-connected-homes.

- Developers of applications ("apps") that run on connected devices, as well as apps that run on "hub" devices, which allow users to interact with and control connected devices.

Consumers

The Commission also should hear from consumers, who can describe their expectations for the Internet of Things. This will help the Commission identify consumers' responsibilities and develop an appropriate consumer education program.

Telecommunications Providers

Because a variety of communications technologies enables connectivity, each of which presents different privacy and security issues, the workshop should include a range of providers, including wireless (terrestrial and satellite) and wireline carriers that support wide area networks; WiFi and other unlicensed service providers that connect local area networks; and providers of Near Field Communication, Bluetooth, RFID, and other technologies that enable personal area networks. In addition, companies that manufacture security solutions for the Internet of Things should participate and discuss the solutions they have developed to secure devices, platforms, and networks while still allowing the free flow of data between and among devices and across networks.

Entities and Individuals Who Use Connected Devices to Improve Public Welfare

Finally, the Commission also should consider including the following entities and individuals who use data from connected devices to improve public welfare:

- Government officials who can explain how they use connected devices and data analysis to improve public works and enhance city planning;

- Emergency first responders and law enforcement officials who can discuss how connected devices enable them to discover and respond to emergencies;
- Transportation officials who can describe how they use M2M communication to regulate traffic flow and ease congestion;
- Medical professionals who can explain how the Internet of Things will improve public health and allow personal health monitoring; and
- Environmental professionals who can describe how connected devices allow greater conservation of energy and natural resources.

IV. INDIVIDUALS AND SOCIETY BENEFIT FROM CONNECTED DEVICES

The Internet of Things promises to improve the quality of life by automating personal tasks and industrial and agricultural operations and by revolutionizing medical, scientific, and commercial research through "big data" analytics. The benefits to individuals and to the public depend on the unimpeded flow of data, some of which is personally identifiable and some of which identifies a particular object or location, but not an individual.

A. INDIVIDUALS WHO USE CONNECTED DEVICES BENEFIT FROM INFORMATION PERSONAL TO THEM AND THAT IDENTIFIES THEM

Individuals can use connected devices to make their lives easier, healthier, and more productive. Some of these benefits require individuals to allow devices to collect and share their personal information.

For instance, patients can use wearable devices that enable doctors to monitor their medical conditions remotely and continuously. These devices can alert doctors to physiological changes that require immediate medical attention or adjustment of medication. Wearable devices can also help elderly patients with limited mobility, allowing self-monitoring or remote monitoring of their condition and location. These devices enable elderly individuals to live

independently or with minimum assistance, thereby decreasing medical costs and improving quality of life.[13]

Likewise, individuals can use wearable devices to monitor their own health and fitness. For example, Fitbit offers a variety of devices that monitor a user's weight, calories burned and consumed, and sleep cycles. These devices communicate with the user's device and allow the user or a healthcare professional to analyze the data online.[14]

Consumers also can use M2M wireless technology to remotely control and access data from appliances in their homes. Connected thermostats and home security systems allow consumers to control and conserve energy in their homes and monitor for intruders. Connected refrigerators may facilitate the automatic creation of shopping lists, or even (at the consumer's option) automatically order groceries.

Companies that provide these products and services should be transparent about their data privacy and security practices so that consumers can make informed decisions. The Internet of Things is not a monolith, however. Many M2M communications will not involve the transmission of personal information and therefore will not raise the same privacy issues.

B. INDIVIDUALS AND ENTITIES CAN BENEFIT FROM INFORMATION RELAYED BY CONNECTED DEVICES THAT CONTAIN INDIVIDUALIZED BUT NON-PERSONAL INFORMATION

There are many examples of connected devices that transmit data that identifies a particular object or a location, but that does not constitute personally-identifiable information.

---

[13] *See* Wearable Technologies, *WT for an Aging Population*, (June 5, 2011), *available at* http://www.wearable-technologies.com/2011/06/wt-for-an-aging-population/ (citing activity monitors, fall sensors, emergency buttons, wearable cameras, bracelets that sound an alarm if an Alzheimer's patient walks outside a preset safe zone, and glucose/blood pressure/weight monitors).

[14] *See* Fitbit website, http://www.fitbit.com.

Examples include

- A public trash can or recycling bin that can signal when collection is needed;[15]
- Buoys with GPS sensors and wireless connections that can be used to provide location-specific information about marine currents and conditions;[16]
- Buses and trains that can provide real-time information to dynamically optimize routing and avoid congestion;[17] and
- Vehicles that can communicate in real time to avoid collisions.[18]

These services require connected devices to share particularized information, but not information that identifies a particular individual. For instance, intelligent transportation systems need to share the location, direction, and speed of a car, but not the identity of the car's owner or driver. These types of M2M communications therefore do not create the same privacy considerations as other uses of the Internet of Things.

C. "BIG DATA" CAN BE ANALYZED TO PRODUCE TREMENDOUS ECONOMIC AND SOCIAL BENEFITS

Analysis of the vast amounts of sensor-generated data could transform scientific, medical, and commercial research and produce tremendous economic and social benefits. The

---

[15] *See, e.g.*, BigBelly Solar, *Telit Magazine: "Smart Grid" for Waste and Recycling: M2M Transforms Public-Space Trash Collection Operations, available at* http://www.bigbelly.com/telit-mag-smartgrid-for-waste-recycling-m2m-transforms-public-space-trash-collection-ops/.

[16] *See, e.g.*, GeoBorders, *IRIDIUM SBD MT3300 Oceanografic Drifter Buoy, available at* https://geoborders.com/en/p/870; GeoBorders, *iSPHERE Oil Spill and Current Tracking Buoy, available at* https://geoborders.com/en/p/733.

[17] *See, e.g.*, Andrew Nusca, ZDNet, *GE Unwraps 'Industrial Internet': M2M for Planes, Trains, Manufacturing* (Nov. 29, 2012), *available at* http://www.zdnet.com/ge-unwraps-industrial-internet-m2m-for-planes-trains-manufacturing-7000008097/; Frost & Sullivan, *Using Wireless Technology to Manage and Optimize Government Fleets: Saving Money, Generating Revenues, and Increasing Safety, available at* http://shop.sprint.com/global/pdf/services_solutions/white_paper_govt_fleet_mgmt.pdf; T-Mobile, *M2M Public Sector*, http://m2m.telekom.com/industry/public-sector.

[18] *See, e.g.*, U.S. Department of Transportation, Research and Innovative Technology Administration, *Intelligent Transportation Systems Joint Program Office, available at* http://www.its.dot.gov.

key to data-driven innovation "is the ability to capture, commingle, store, verify and analyze relevant data, and then integrate the results into established processes to derive innovative practical outcomes."[19] Aggregation and analysis of personally identifiable information collected from multiple sources can pose privacy risks, however. Companies therefore should adopt best practices that ensure transparency, data security and integrity, and, where appropriate, de-identification of data.[20] This approach would build consumer trust and safeguard individual privacy while allowing consumers to realize the benefits of "big data" analytics, which could be tremendous.

For instance, "big data" analysis of de-identified information about individuals' healthcare and lifestyle choices has the potential to improve medical care, lower healthcare costs, and enhance medical and epidemiological research. According to McKinsey Global Institute

> If US healthcare were to use big data creatively and effectively to drive efficiency and quality, the sector could create more than $300 billion in value every year. Two-thirds of that would be in the form of reducing US healthcare expenditure by about 8 percent.[21]

In addition, researchers can gain greater insight into personal health risks by combining information from electronic medical records with information about lifestyle choices deduced from sensor-generated data about grocery store purchases and physical activity.[22] Researchers

---

[19] Software and Information Industry Association White Paper, *Data-Driven Innovation*, at 10 (2013), *available at* https://www.siia.net/index.php?option=com_docman&task=doc_download&gid=4279&Itemid=318.

[20] *Id.* at 5. *See also* Future of Privacy Forum, *De-Identification*, *available at* http://www.futureofprivacy.org/de-identification/.

[21] James Manyika et al., *Big Data: The Next Frontier for Innovation, Competition, and Productivity*, (May 2011), *available at* http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation.

[22] *See, e.g.*, Kim Rose, *Big Data's Potential Drives Healthcare Spending for Epidemiology and Genomes* (Apr. 30, 2013), *available at* http://hortonworks.com/blog/big-datas-potential-drives-healthcare-spending-for-epidemiology-and-genomes/.

can also combine information about weather patterns and disease outbreaks to predict epidemics.[23]

De-identified datasets can also be used to promote energy conservation. For example, real estate managers can use "big data" about energy usage to project energy consumption at their properties and correlate cost savings and efficiency trends with building construction and operational parameters for planning future projects.[24]

Similarly, state and local governments can compile data from networks of highway sensors and cameras to manage traffic flow, respond to emergencies and changes in traffic patterns, and manage public transit services.[25]

Companies also are using "big data" to improve agricultural productivity. John Deere has added sensors to farming equipment, enabling connectivity between the equipment, owners, operators, dealers, and agricultural consultants. Data from these sensors is combined with historical and current data about weather, soil conditions, crops, and other factors and analyzed to improve productivity and efficiency and help farmers manage their equipment.[26]

---

[23] *See* Jacques Coetzee, *How Big Data Is Being Used to Record the Future* (Mar. 8, 2013), *available at* http://memeburn.com/2013/03/how-big-data-is-being-used-to-record-the-future/.

[24] *See* Michael Bendewald, *How Energy Managers Can Leverage Big Data Right Now* (Apr. 2013), *available at* http://www.facilitiesnet.com/energyefficiency/article/How-Energy-Managers-Can-Leverage-Big-Data-Right-Now--13976#; Bennett Fisher, *How Big Data Can Tackle Commercial Building Energy* Feb. 15, 2012), *available at* http://gigaom.com/2012/02/15/how-big-data-can-tackle-commercial-energy/.

[25] *See* Intel Case Study, *Improving Traffic Management with Big Data Analytics* (2013), *available at* http://www.intel.com/content/dam/www/public/us/en/documents/case-studies/big-data-xeon-e5-trustway-case-study.pdf; Jeff Bertolucci, *Dublin Points Big Data Tech at Traffic Jams* (May 20, 2013), *available at* http://www.informationweek.com/big-data/news/big-data-analytics/dublin-points-big-data-tech-at-traffic-j/240155213.

[26] BigData Startups, *John Deere is revolutionizing farming with big data* (2013), *available at* http://www.bigdata-startups.com/BigData-startup/john-deere-revolutionizing-farming-big-data/.

V. GOVERNMENT POLICY DOCUMENTS AND INDUSTRY GUIDELINES CAN FRAME PRIVACY AND CYBERSECURITY BEST PRACTICES

The Internet of Things ecosystem involves a large number of players in the mobile space; a range of platforms, device formats, and services; and data of varied sensitivity. A privacy and security framework should reflect this diversity and should not vary depending on the type of device or technology used to collect or transmit data. Instead, a framework should be technology neutral and apply "in a way that is proportional to the nature, sensitivity, and amount of data collected…."[27] In addition, any framework should be flexible. Rigid regulatory burdens could stifle technological innovation and discourage the development of the Internet of Things. Flexible industry best practices and regulatory policy guidelines, however, will enable the wireless industry to both protect the privacy and security of consumer data and bring consumers the innovative products and services that will improve quality of life, increase efficiency, and grow the economy.

The mobile industry has a strong track record of addressing privacy and security issues as technology evolves and the marketplace expands. For example, CTIA used the Fair Information Practice Principles to develop the CTIA Best Practices and Guidelines for Location Based Services ("LBS Guidelines"), which are designed to promote and protect consumer privacy as new location-based services ("LBS") are created and deployed.[28] The LBS Guidelines explain how LBS providers can implement strong notice and choice mechanisms to protect the privacy of consumers who use LBS services. CTIA designed the LBS Guidelines to be flexible enough to adapt to new LBS services, and they apply regardless of the technology or mobile device used

[27] FTC Report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 2012) at 9.

[28] The LBS Guidelines are available at http://www.ctia.org/business_resources/wic/index.cfm/AID/11300.

or the business model of the company that offers the LBS service. In addition, CTIA has issued the Consumer Code for Wireless Service, which, among other things, requires signatories to abide by a privacy policy that they must make available to the public. Moreover, CTIA's Cybersecurity Working Group ("CSWG"), which comprises a range of CTIA members, has developed cybersecurity solutions for industry and for consumers and enterprise customers. CTIA members make the CSWG's solutions available to customers throughout the mobile ecosystem.[29] Other associations similarly have developed best practices that ensure wireless providers protect consumer privacy, keep data secure, and foster innovation and competition.[30]

CTIA members recognize that strong privacy protection and cybersecurity are good business practices. Companies earn and maintain consumer trust and loyalty by protecting consumers' data and keeping devices and networks secure. CTIA members therefore have strong business incentives to develop and implement these best practices. CTIA recognizes that the wireless companies will face new challenges as the Internet of Things progresses, and it looks forward to input from the FTC and other regulators as it develops new best practices to address these issues.

In addition to industry guidelines, elements of the FTC's Privacy Report can also provide a privacy protection framework for the Internet of Things. Since issuing its Privacy Report in 2012, the FTC has successfully used its three-pronged privacy framework – (1) privacy by design, (2) simplified consumer choice, and (3) transparency – to provide guidance on privacy issues related to particular technologies. For instance, the FTC's recent staff report, *Mobile*

---

[29] CTIA—The Wireless Association, *Today's Mobile Cybersecurity: Protected, Secure and Unified* (October 2012), at 17-18, *available at* http://files.ctia.org/pdf/CTIA_TodaysMobileCybersecurity.pdf .

[30] *See, e.g.*, Mobile Marketing Association's Global Code of Conduct for Mobile Marketing (July 15, 2008), *available at* http://mmaglobal.com/codeofconduct.pdf.

Privacy Disclosures: Building Trust Through Transparency, recognized the roles of different industry participants in the mobile app ecosystem and provided effective guidance for collaboration and shared responsibility between and among all stakeholders.

The FTC may provide similar guidance to the nascent Internet of Things and, when necessary, use its enforcement authority to take appropriate action.[31] The FTC should maintain a flexible and technologically neutral approach, however. Like voluntary industry guidelines, flexible regulatory guidance will allow companies to implement best practices in a manner appropriate to each company's technology and the needs of consumers as they adopt new products and services in this rapidly evolving ecosystem.

The White House Privacy Blueprint provides another complementary approach to privacy protection through private sector participation in the development of voluntary enforceable codes of conduct. Because a consensus-driven, multi-stakeholder model can engage all interested parties, it is more likely to produce a framework that is flexible and able to adapt to new products and services as technology evolves.

The U.S. National Institute for Standards and Technology is taking a similar approach to cybersecurity. It is facilitating an industry-led process to develop a voluntary cybersecurity framework. CTIA members are actively involved in this process, and because mobile network operators have prioritized cybersecurity since they began building cellular networks, they already have a framework on which to build.[32]

---

[31] *See, e.g., In the Matter of TJX Companies, Inc.*, F.T.C. No. C-4227 (July 29, 2008) (Decision and Order) (upholding consent order to settle charges TJ Maxx failed to provide adequate security for customer information where the company had used insecure networks to transmit and store customers' personal information and the data had been stolen).

[32] The mobile industry has integrated all of the players in the mobile ecosystem – carriers, manufacturers, app developers, and operating system and platform providers – into its approach

VI. CONCLUSION

We are increasingly moving to a world of convergence where connectivity and intelligence is seamlessly embedded in all devices, whether mobile or stationary. The privacy and security implications of connected devices should be examined holistically, and privacy and security standards and practices should be tailored to the nature of data shared, not the type of technology or device used to transmit the data. A combination of open industry standards, flexible regulatory guidance, and multi-stakeholder and industry-led voluntary codes of conduct will protect the privacy and security of personal information. It also will allow the ubiquitous connectivity and sharing of data between and among both mobile and stationary devices that is essential to the proper functioning of the Internet of Things. This balanced approach will ensure that informed consumers and the public at large can reap the benefits of the Internet of Things while knowing that their privacy is protected and their data is secure.

CTIA looks forward to working with the Commission as it continues to examine these issues.

Respectfully submitted,

/s/

Debbie Matties
Vice President, Privacy

CTIA-THE WIRELESS ASSOCIATION®
1400 16th Street, NW, Suite 600
Washington, DC 20036
(202) 736-3654

June 1, 2013

---

to cybersecurity. Collectively, the mobile industry has spent hundreds of millions of dollars to secure the mobile ecosystem. *Today's Mobile Cybersecurity*, *supra* note 29, at 5.