Before the
FEDERAL TRADE COMMISSION

)
)
)
Workshop to Explore Privacy and Security)
Implications of the Internet of Things)
)
)

COMMENTS OF AT&T

Theodore R. Kingsley
Keith M. Krom
Peggy Garber
AT&T Inc.
1120 20th Street, NW
Washington, DC 20036
(2020) 457-2055

Counsel for AT&T Inc.

May 31, 2013

Before the
FEDERAL TRADE COMMISSION

	)
	)
	)
Workshop to Explore Privacy and Security	**)**
Implications of the Internet of Things	**)**
	)
	)

TABLE OF CONTENTS

Before the

FEDERAL TRADE COMMISSION

	)
	)
	)
Workshop to Explore Privacy and Security	**)**
Implications of the Internet of Things	**)**
	)
	)

COMMENTS OF AT&T INC.

AT&T Inc. ("AT&T"), on behalf of itself and its affiliates, submits these comments in response to the press release dated April 17, 2013 ("Press Release") issued by the staff of the Federal Trade Commission ("Staff") , which invites comments on the growing connectivity of consumer devices and related privacy and security issues.

I. INTRODUCTION AND SUMMARY

AT&T is a global communications provider that provides voice, video and data connectivity between devices and people throughout the world. AT&T and a diverse range of companies and individuals are working creatively and cooperatively to develop and deliver an ever increasing variety of "intelligent systems" or "smart communications" which are enabled by a wide range of technologies and services provisioned in the context of a global market and ecosystem. The participants in this ecosystem have developed, and continue to develop, individual and collaborative measures to enhance security and safeguard the privacy of consumer information. The upcoming workshop provides Staff with an opportunity to highlight these multi-stakeholder approaches to privacy and security and establish the primacy of these approaches in the context of the ever-evolving Internet of Things (IOT).

In these comments, AT&T responds to the Staff's request for information concerning the technologies that enable the IOT, as well as some examples of intelligent system service offerings and applications (chiefly involving networked "things," or "machine-to-machine" (M2M) systems. AT&T highlights the Future of Privacy Forum's work in the context of Smart Grid technology as an example of how the participants in the ecosystem can work together to develop and implement privacy and security standards for the Internet of Things. Appropriately safeguarded, data collected and used in the provisioning IOT systems and solutions have the potential for a myriad of socially beneficial uses, such as health care and energy efficiency. AT&T concludes these comments with a discussion of the privacy and security principles appropriate to the IOT.

II. THERE IS AN EVER-INCREASING DIVERSITY OF INTELLIGENT NETWORKS AND SYSTEMS

The IOT encompasses an ever-growing suite of services, enabled by a wide range of technologies. At its core, the IOT is provisioned over evolving and expanding terrestrial and wireless communications networks and infrastructures that are used to manage and transport signaling and content data between electronic devices. AT&T is a global provider of wireline and wireless data and communications services, provisioning wireless data and communications services primarily over licensed radio frequency spectrum bands. In collaboration with other ecosystem innovators, AT&T uses its licensed commercial mobile radio service spectrum to deliver a range of M2M offerings, as described in more detail below.

AT&T and others also utilize a range of complementary connectivity technologies in the context of the IOT. For example, WiFi, Near Field Communications (NFC) and Bluetooth wireless technologies all may be used to provide a component of the communications networks used to deliver IOT services. AT&T works with a large and growing array of innovative companies to deliver IOT solutions, including device manufacturers, software providers and app developers. As with the market for mobile services generally, the IOT is a complex ecosystem comprised of innovative companies that are developing new services and capabilities for the benefit of consumers.

As Staff note, IOT technologies enable everyday devices to communicate with each other and such M2M systems are becoming more prevalent.[1] Across the country, utilities are installing smart meters on residential and commercial buildings. Each day consumers are adopting web-enabled home monitoring and security services and benefitting from medical-monitoring and health-and-wellness applications rely on smart communications technologies. Commercial and governmental delivery systems rely on smart tracking technologies and fleet- and route-management applications. Cities and towns are learning how to do more with less by adopting smart technologies for citizen engagement and the delivery of municipal services. At each turn, these technologies are improving the quality of peoples' lives, helping to keep populations healthier, increase security, reduce transportation costs, curtail greenhouse gas emissions, cut utility bills, and facilitate more efficient travel.

A full catalogue of current M2M communications is beyond the scope of these comments, but a few examples may help to frame discussion at the upcoming Staff workshop:

[1] http://www.ftc.gov/opa/2013/04/internetthings.shtm (last accessed May 23, 2013).

Asset tracking: Increasingly, Radio Frequency Identification (RFID) technology, barcodes and other devices allow the pinpoint tracking of a multitude of physical assets. Hospitals keep track of medical equipment inventory, ensuring that devices large and small, simple and complex, are deployed where needed. Retailers have a similar real-time window into inventory levels and the location of their goods. Package delivery services inform consumers of the location of their packages at any time in transit, and advise when items are delivered to their final destination. Motor vehicle-sharing services provide car location information and determine whether they should be repositioned to optimize their availability for the next use.

Smart meters and home energy management services: The communications-enabled smart meter is the center of an ecosystem of M2M devices that electric utilities use to deliver services. These meters form the end points of a web of M2M devices throughout the utility's network that gives operators a real-time view of the state of the distribution network. Utilities can pinpoint damaged network assets, divert current flow around damaged assets to keep power flowing to more customers, arrange for repairs more quickly, even turn a subscriber's power on and off immediately and from a remote location. The M2M communications capabilities in electrical networks allow the integration of renewable generation capabilities like solar and wind power. They allow utilities to automatically ask that subscribers curtail energy usage during peak periods to reduce the need for new, power plants that are necessary only a few days out of the year.

The energy usage data flowing from smart meters allows consumers to run their homes more efficiently. Energy consumers can route their energy usage information to the energy management service provider of their choice. The service provider can, in turn, analyze the data flow and offer myriad tips for conserving energy – identifying a major appliance that needs service or replacement, notifying a subscriber if equipment like a pool pump is running when it should not be, even alerting homeowners if their insulation seems inadequate compared to that of their neighbors.

Smart homes: M2M communications also enable services that help automate and increase the security of homes. Residents who subscribe to smart-home services can turn lights and appliances on and off, lock and unlock doors, and monitor the security of their homes using a smart phone or other web-enabled device from virtually anywhere in the world.

Healthcare: Healthcare stands out as the sector of the economy that will probably be transformed more than any other by M2M technologies in the coming years, and the transformation is already well under way. M2M healthcare technologies have the potential to improve health outcomes, reduce health expenditures and facilitate the offering of care in more patient-friendly ways.

Wireless, body-worn sensors will increasingly allow the healthcare industry to free patients from the tangle of wires that can accompany a hospital stay and in many cases restrict patient mobility. Similar technologies are migrating into homes, allowing the remote and continuous monitoring of patients' blood-pressure, respiration rate and a variety of other biometric information. This information typically flows across a short, unlicensed wireless link to a monitoring hub in the patient's home, which then passes the information to the broadband network, routing it to the cloud where analytics continuously monitor a patient's status, notifying a healthcare provider in case of anomalies. These applications allow patients to be monitored in the comfort of their own homes.

There is a profusion of newly developed applications in the health and wellness area that pairs communications-enabled devices of some sort with smart-phone apps. For example, mobile devices can transmit an individual's daily weight information to a smart phone carrying an app that monitors trends and, potentially, offer diet or exercise suggestions in response. Similarly, fitness applications help individuals keep track of daily miles walked, calories burned, and monitor pulse and respiration rates over the course of time.

Within AT&T specifically, AT&T and eCardio Diagnostics combined mobile technology with cardiac care support services in order to provide monitoring solutions for heart patients. eCardio provides cardiac event monitors. AT&T is providing eCardio with M2M wireless data and mobile connectivity for near real-time, remote monitoring of cardiac patients. eCardio's monitoring solution on cardiac devices allows heart patients to recover at home rather than spend additional time in the hospital.

This integrated solution allows doctors to have critical patient information sent to them near real-time, as circumstances occur, helping them improve response times to urgent medical issues. Clinical productivity is improved by timely access to accurate patient information from any Internet-enabled computer. Not only does the solution provide a better patient experience, it can also help hospitals, health insurance companies, pharmacies, drug retailers and research organizations lower their costs of treatment and ultimately pass these lower costs onto consumer patients.

Similarly, Vitality worked with AT&T to facilitate pharmaceutical adherence. Vitality invented a device called "GlowCap" which fits standard pill bottles. The GlowCap is Internet connected and reminds patients when to take their medication, is equipped with a button to push to renew prescriptions, and can send reminders and other communications to the home phone as well as to the care provider.

The field of telehealth also holds the promise of extending the reach of healthcare practitioners far into remote areas. Visiting nurses and other healthcare workers are already being equipped with tablet devices that synch wirelessly with medical peripherals (blood-pressure monitors, blood-glucose monitors, etc). These professionals can visit home-bound patients and monitor their conditions, including conferring where appropriate with remote doctors or nurses. This suite of telehealth services is now even offered to patients upon discharge from the hospital. Rather than returning for weekly follow-up visits after discharge, patients can allow the regular, remote measurement of their biometric data and confer as appropriate with their healthcare providers over secure video links enabled by a wireless tablet device.

Smart Cities: Local and municipal government operations are also benefitting from M2M communications. Fleet-management technologies allow municipalities to remotely monitor the repair status of their vehicle fleets, the safety habits of their drivers, even facilitate route planning to increase safety and reduce fuel consumption. M2M technologies built into public transportation vehicles not only allow more effective fleet management but can be opened to the commuting public to allow better information about the time of the next bus or train at a particular stop.

One example of an electronic fleet management solution for heavy equipment vehicles is provided by Zonar in collaboration with AT&T. Using RFID technology and on-board diagnostics Zonar can collect, report, and analyze data before, during, and after a vehicle trip. The electronic vehicle inspection report uses Zonar's handheld device to scan RFID tags attached to critical inspection zones on the vehicle. The device wirelessly transmits the report back to Zonar facilitating predictive maintenance and enhancing roadway safety for school buses, utility vehicles, transit buses, and waste and recycling vehicles. AT&T provides the M2M management platform as well as the wireless connectivity to communicate with vehicles.

Further, municipalities may procure smart trash receptacles that can signal when they need to be emptied, so sanitation fleets can work more efficiently, rather than emptying every can on their rounds. Smart technologies built into city parking systems can increase revenue, speed the enforcement process and reduce drivers' frustrations with paying for parking.

III. PRIVACY AND SECURITY ISSUES VARY DEPENDING ON THE M2M APPLICATION AND ARE BEING ADDRESSED COLLABORATIVELY BY THE ECOSYSTEM

Staff asks whether de-identified data from smart devices can and should be used for socially beneficial purposes.[2] The answer is yes: such data are and should continue to be used. Aggregated and de-identified data can be used to reveal otherwise indiscernible patterns and trends in a number of socially beneficial contexts, including medical and epidemiological research, energy conservation, multi-modal traffic management, and agricultural, industrial and commercial productivity and efficiency. Staff also seeks comment on privacy and security listings associated with smart technology and its data. These risks vary depending upon the specific M2M application and the degree of human interaction.

The degree of human intervention or interaction in M2M systems varies. The smart grid technology that allows a utility to monitor the functionality of its network assets typically involves relatively limited human interaction on a regular basis. As long as the monitored assets are working properly, no alarms go off and human interaction is largely unnecessary. On the other hand, telehealth applications inherently involve a significant degree of human interaction. As an example, if wireless monitors are employed to measure a patient's biometric data, the data

[2] *Id.*

are reviewed, and potentially acted on, by an on-premises healthcare worker or a medical professional on the other end of a communications link. While both scenarios involve M2M communications, the privacy and security implications of both scenarios are different.

A second important respect in which M2M systems vary concerns the communications media they use. M2M transmissions work over a range of technologies, including those described above; everything from very short-distance wireless links (in the case of some medical monitoring technologies), to Blue Tooth or other unlicensed-spectrum links that can work throughout the average American home. These may be carried on licensed wireless spectrum, as in the case of smart-phone apps that link to cloud platforms, and they may pass over wired broadband links as well.

One example of proactive, cooperative industry efforts on privacy issues is the recent development of a Smart Grid Privacy framework. In October 2012, the Future of Privacy Forum (FPF) announced a privacy seal program based upon a fundamental set of privacy principles incorporated in its Smart Grid Privacy Guidelines. Aware of the critical need for privacy and security protections for sensitive consumer energy information, industry members proactively engaged in collaborative, self-regulatory efforts. FPF convened a diverse group of companies, including AT&T, Comcast, Ecofactor, IBM, Intel, Motorola, Neustar, Opower, Tendril, Verizon, and TRUSTe to develop the privacy framework. FPF also requested input from utilities and utility regulators as interested stakeholders.

The Guidelines are targeted to companies that use consumer information (for example, companies offering home energy management, remote home control or security, smart thermostats and other services) to provide smart grid services. Furthermore, the Smart Grid Privacy Guidelines are designed to help assure consumers that organizations using their information are employing best practices for security, privacy, and dispute resolution and are using consistent approaches to obtaining consent. In order to receive a seal endorsement, participating organizations must validate that they are following Smart Grid Privacy Guidelines. TRUSTe, the company that administers the seal, checks an organization's privacy policy, scans for potential privacy threats, reviews consumer consent processes, and conducts various business and technical assessments to verify compliance.

As the Smart Grid example suggests, self-regulatory initiatives can result in genuine progress toward a more comprehensive, consumer-centric approach to privacy. AT&T recommends continued collaboration between industry and policymakers to encourage the expanded use of the Smart Grid Privacy framework and the adoption of similar self-regulatory approaches. Such approaches should establish criteria and best practices to ensure the consistent, functional treatment of privacy and consistent user privacy experiences across the IOT ecosystem.

Ultimately, the most productive approach to ensuring robust privacy and security standards is voluntary compliance with broadly accepted industry guidelines. AT&T has participated in a number of industry efforts to develop privacy guidelines. For example, AT&T participated in the development of the CTIA Best Practices and Guidelines for Location-Based Services.[3] It also participated in discussions with the FPF and the Center for Democracy and Technology regarding the development of broader industry guidelines on privacy protections for location-based services.[4]

[3] http://files.ctia.org/pdf/CTIA_LBS_Best_Practices_Adopted_03_10.pdf (last accessed May 29, 2013)

[4] *See* Future of Privacy Forum Website, *Best Practices for Mobile Application Developers*, http://www.future ofprivacy.org/best-practices-for-mobile-app-developers/.

The industry is fully cognizant of the security issues around M2M. As more and more devices become connected it is logical to expect that any security risks are going to increase across the ecosystem. Threats can include interception of data transmissions, network and device denial of service attacks, malware infections and other forms of threats. M2M security is a necessary prerequisite and any service provider or M2M solution that fails to adequately address security from the outset will not be successful in the marketplace. For this reason, there are a wide variety of standards bodies working on security standards for M2M.

The "oneM2M" initiative is an example of a standards body that was established with the goal to develop technical specifications which address the need for a common M2M Service Layer that can be readily embedded within various hardware and software, and relied upon to connect the myriad of devices in the field with M2M application servers worldwide. oneM2M has over 250 member companies, including AT&T and most of the major U.S. carriers. The scope of their work includes technical specifications for security and privacy aspects of M2M (authentication, encryption, etc.) and involve liaison relationships with other standards bodies such as 3rd Generation Partnership Project (3GPP), Broadband Forum (BBF), Home Gateway Initiative (HGI) and the International Telecommunications Union-Telecommunications Standardization Sector (ITU-T). The Telecommunications Industry Association (TIA) and the Consumer Electronics Association (CEA) are also working on M2M standards. The Cloud Security Alliance (CSA) has published several recommendations for security in the cloud which are relevant to M2M applications that are being deployed in the cloud. More broadly, there is ongoing mobile security standards work at various industry organizations including 3GPP, Global System for Mobile Communications Association (GSMA), ATIS, Internet Engineering Task Force (IETF) and CTIA-The Wireless Association; industry is working with government in variety of venues on mobile security including at The National Institute of Standards and Technology (NIST), The Defense Information Systems Agency (DISA) and The Department of Homeland Security (DHS).

Any further standards effort should: build upon work that is already being done with respect to M2M security standards; be an industry-led rather than a top-down regulatory standards-based model; be flexible enough to allow room for innovation, and be ecosystem wide as opposed to being narrowly focused on specific sectors such as mobile carriers. A good start would be to take an inventory of best practices that are already under development.

CONCLUSION

AT&T encourages the Staff to recognize how fast the IOT is changing, and how many different technologies and stakeholders area part of the ecosystem. Industry stakeholders like AT&T have a track record of committing to meaningful, voluntary efforts to improve privacy and security —and will continue to do so. Industry-led efforts will continue to be the most effective way to protect privacy and security in the context of the "Internet of Things."

Respectfully submitted,

/s/
Theodore R. Kingsley
Keith M. Krom
Peggy Garber
AT&T Inc.
1120 20th Street, N.W.
Washington, D.C. 20036
(202) 457-2055

Counsel for AT&T Inc.

May 31, 2013