FRED UPTON, MICHIGAN
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS

Congress of the United States
House of Representatives

COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115

Majority (202) 225-2927
Minority (202) 225-3641

MEMORANDUM

March 20, 2015

To: Subcommittee on Commerce, Manufacturing, and Trade Democratic Members and Staff

Fr: Committee on Energy and Commerce Democratic Staff

Re: Hearing on "The Internet of Things: Exploring the Next Technology Frontier"

On Tuesday, March 24, 2015, at 11:00 a.m. in room 2218 of the Rayburn House Office Building, the Subcommittee on Commerce, Manufacturing, and Trade will hold a hearing titled, "The Internet of Things: Exploring the Next Technology Frontier." This hearing immediately follows an Internet of Things (IoT) Showcase in the Rayburn foyer, held from 9 a.m. to 11 a.m.

I. BACKGROUND

IoT generally refers to the ability of everyday objects to connect to the Internet and to send and receive data.[1] Examples of IoT products are home automation devices that allow you to control the lights and temperature in your house from a smart phone, an Internet-connected jet engine that signals when maintenance is needed, and a bracelet that measures your heartrate and tracks your location while transmitting the information to a website. Not included in the definition of IoT are devices used for accessing the Internet such as computers, smartphones, or tablets—rather IoT includes consumer products that incorporate Internet into how they connect, communicate, and transmit information.

The expansion of IoT products and technology is occurring at a rapid rate. Six years ago, the number of "things" connected to the Internet surpassed the number of people.[2] As of this

[1] Federal Trade Commission, *Internet of Things: Privacy & Security in a Commercial World*, FTC Staff Report (Jan. 27, 2015).

[2] *The Internet of Things: How the Next Evolution of the Internet is Changing Everything*, Cisco Internet Bus. Solutions Grp. (Apr. 2011) (online at www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf).

year, there will be 25 billion connected products and it is expected that by 2020 there will be 50 billion connected products.[3] The rapid expansion of this technology poses significant opportunities for innovation, but also poses a number of risks for consumers. Previously "dumb" products will now have technology imbedded in them that will collect, transmit, store, and potentially share vast amounts of consumer data, including highly personal information.

The benefits associated with IoT are numerous. It can help in the development of smarter manufacturing where sensors are imbedded in equipment and wirelessly communicate notification that maintenance is needed before the machine ever breaks down.[4] Connected medical devices can allow patients with medical conditions to have their physicians remotely monitor their conditions—expanding access to care while also lowering costs.[5] Smart meters can enable energy providers and consumers to monitor and analyze the consumers' energy use so they can be more efficient.

II. SELECTED ISSUES

A. Cyber Security

A primary concern with IoT technology is that the information collected through the product is vulnerable to being hacked. The risks associated with hackings are compounded with IoT objects since cyber attackers can exploit weaknesses using the Internet and affect the product's functioning. For instance, many cars have microcontrollers that govern the car's engine, brakes and other instruments. Researchers have shown that it is possible to hack into a car's system and take over control of the car.[6]

These risks extend to medical devices as well. At the 2011 "Black Hat Briefing—a cyber-security conference—a presenter was able to demonstrate how he could hack into an insulin pump and induce an overdose.[7] The Food and Drug Administration (FDA) has issued non-binding guidance to assist industry in identifying cybersecurity risks and to provide

---

[3] *Id*.

[4] *Building Smarter Manufacturing With the Internet of Things (IoT)*, Lopez Research (Jan. 2014) (online at www.cisco.com/web/solutions/trends/iot/iot_in_manufacturing_january .pdf).

[5] *Improving Health Care Through Mobile Medical Devices and Sensors*, Center for Technology Innovation, Brookings Institute (Oct. 2013) (online at www.brookings.edu/~/ media/research/files/papers/2013/10/22-mobile-medical-devices-west/west_mobile-medical-devices_v06.pdf).

[6] *The Internet of Things: Home, Hacked Home*, The Economist (July 12, 2014) (online at www.economist.com/news/special-report/21606420-perils-connected-devices-home-hacked-home).

[7] *Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System* (online at media.blackhat.com/bh-us-11/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_ Devices_WP.pdf) (accessed on Mar. 19, 2014).

recommendations that manufacturers should follow to ensure functionality and safety in light of these risks.[8]

B. Data Privacy

Another concern in the IoT space is how product manufacturers use the data they collect, whether they sell it to third-parties, and how third-parties could then use that data. For instance, data collected from fitness tracking sensors can be used to infer a user's stress levels, gender, age, smoking habits, and overall well-being.[9] This data could then be used by the product manufacturer or sold to a third-party such as a health insurance company, which might then use this information to adjust health insurance rates.[10]

For a company that wants to notify consumers about their information collection and use practices, attaining their consent may be difficult, if not impossible. For example, providing such notice where the IoT product does not have a screen or interface. This raises questions about how and under what circumstances a manufacturer can effectively secure a consumer's informed consent to its privacy policy or terms of service agreement. There are also additional questions of when a company can use a product to begin collecting new types of information, or if a company can use the information it collects in new ways without getting additional consent or allowing the consumer to opt-out.

III. FEDERAL GOVERNMENT ROLE

A. Federal Trade Commission

The Federal Trade Commission (FTC) possesses broad jurisdiction under Section 5 of the FTC Act to prohibit "unfair or deceptive acts or practices in or affecting commerce" by a wide variety of individuals and entities.[11]

---

[8] Food and Drug Administration, *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, Guidance for Industry and Food and Drug Administration Staff* (Oct. 2, 2014) (online at www.fda.gov/downloads/medicaldevices/deviceregulationand guidance/guidancedocuments/ucm356190.pdf).

[9] Scott Peppet, *Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security & Consent*, 93 Tex. L. Rev. 85 (Mar. 1, 2014). The Patient Protection and Affordable Care Act prohibits setting insurance rates based on certain factors such as gender, race, and general health status, while insurance companies retain the ability to use certain ratings such as smoking rating and age rating. 42 U.S.C. 300gg-4, 18116.

[10] *Big Doctor Is Watching: How Your Fitness Tracker Could Increase Your Health Insurance Costs Someday*, Slate (Feb. 27, 2015) (online at www.slate.com/articles/technology/ future_tense/2015/02/how_data_from_fitness_trackers_medical_devices_could_affect_health_in surance.html).

[11] 15 U.S.C. 45(a).

In January 2015, the FTC released a staff report entitled, "Internet of Things: Privacy & Security in a Connected World."[12] The report summarized information presented at a FTC sponsored workshop and provided staff recommendations for ensuring consumer protection in the IoT sphere. Staff recommendations in the report included:

- Implement reasonable security.
- Build-in security as part of the design of a product—not consider privacy or security risks after the fact.
- Ensure personnel practices promote good security—provide training on security practices, only give access to consumers' personal data to personnel that need it, and designate personnel at an appropriate level within the company responsible for security.
- Retain service providers that are capable of maintaining reasonable security.
- Implement a "defense-in-depth" approach with multiple levels of security, such as encrypting data.
- Implement reasonable access control measures to limit the ability of unauthorized persons from access a consumer's product—such as limiting its ability to connect with certain other products.
- Monitor products throughout their life cycle.[13]

While the FTC report did not recommend legislation specific to IoT, it did recommend that Congress enact baseline privacy legislation to increase consumer choice, require transparency, and mandate some level of privacy by design.[14]

B. Federal Communication Commission

The Federal Communications Commission (FCC) has authority over spectrum allocation and assignment for non-federal government entities. Spectrum, or the wireless airspace on which devices communicate, can be either licensed by the FCC or unlicensed so that anyone can use that particular band of spectrum. IoT devices communicate using spectrum and the FCC's Technological Advisory Council expects unlicensed spectrum to be the primary wireless platform for IoT technologies.[15]

[12] *See* note 1.

[13] *Id.*

[14] *Id.*

[15] Federal Communications Commission Technological Advisory Council Meeting Presentation (Dec. 4, 2014) (online at transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting12414/TAC-12-4-14-Full-Presentation-Final.pdf).

C. White House Consumer Privacy Bill of Rights

In February 2012, the White House released a framework for protecting consumer privacy, which included a proposal for a Consumer Privacy Bill of Rights.[16] Incorporated into the proposal were the Fair Information Practice Principles (FIPPs) of notice, choice, access, accuracy, data minimization, security, and accountability.

In February 2015, the White House released a discussion draft of legislation called the Consumer Privacy Bill of Rights Act of 2015.[17] This proposed legislation, widely criticized by members of Congress, the FTC, and consumer advocacy groups, would allow industries to develop their own codes of conduct on the handling of consumer information. It would also charge the FTC with making sure those codes of conduct satisfy certain requirements, including providing consumers with clear notices about how their personal information will be collected, used and shared.

IV. WITNESSES

Daniel Castro
Vice President
Information Technology and Innovation Foundation

Brian van Harlingen
Chief Technology Officer
Belkin International, Inc.

Rose Schooler
Vice President, Internet of Things Group and
GM, IoT Strategy and Technology Office
Intel Corporation

R. Brad Morehead
Chief Executive Officer
LiveWatch Security, LLC

[16] The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 2012) (online at www.whitehouse.gov/sites/default/files/privacy-final.pdf).

[17] The White House, *Consumer Privacy Bill of Rights Act of 2015 Discussion Draft* (online at www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf) (accessed on Mar. 19, 2014).