U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE

March 20, 2015

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

From: Committee Majority Staff

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

I. INTRODUCTION

On Tuesday, March 24, 2015, at 11:00 a.m. in 2123 Rayburn House Office Building, the Subcommittee on Commerce, Manufacturing, and Trade will hold a hearing entitled "The Internet of Things: Exploring the Next Technology Frontier." This hearing will give Members of the Subcommittee an opportunity to hear about the emerging Internet of Things (IoT) marketplace and its role in strengthening the U.S. economy and improving the quality of life for consumers. In addition to examining the benefits of Internet-connected products and services, the hearing will explore how security and privacy are being addressed by the makers of these products. The hearing also will explore what companies are doing to protect increased consumer information flowing on networks as the IoT gains more exposure, acceptance, and use among consumers.

II. 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; and,
- Brad Morehead, Chief Executive Officer, LiveWatch Security, LLC.

III. BACKGROUND

A. Overview: The Internet of Things

The Internet of Things (IoT) defines an environment in which devices, services, and objects are Internet-enabled or connected. These things are networked, sensing, automated, and collecting and transmitting information and data in real-time to operate and perform according to

consumer preferences.[1] Sometimes referred to as "smart" devices, these objects are more than just phones and tablets, but also include appliances and machines that consumers use every day, such as refrigerators, thermostats, cars, lights, and even wearable technology like watches and clothes.[2] These connected devices offer consumers a wide range of benefits from increased productivity and efficiency, to greater information and knowledge, and more control and management over their environment.

The Internet of Things is making its mark on several sectors of the U.S. economy.[3] This is demonstrated in industries including health, energy, education, transportation, agriculture, and many others. In the health sector, connected devices are enabling health care providers to monitor, treat, and diagnose patients in different locations. In the energy sector, Internet connectivity is allowing individuals to control their household thermostats remotely through apps on their smartphones or tablets, saving on energy costs. In the transportation sector, networked cars are notifying drivers of upcoming safety hazards, helping drivers take corrective action to avoid a crash or other potential harm. This market of networked machines can result in improved health, safety, and productivity and reduced costs.[4]

These types of benefits across all sectors of the economy portend massive growth for the Internet of Things.[5] In 2010, over 12.5 billion devices were estimated to be connected to the Internet.[6] By 2015, it is predicted that over 25 billion devices will be connected, and by 2020, it is projected that 50 billion devices will be connected to the Internet.[7] As more consumers adopt these products that are becoming increasingly personalized and accessible and "opening new frontiers for improving processes,"[8] it has the potential to break down barriers to mass consumer acceptance and use.[9] The rapid growth of the IoT market in combination with the breadth and scope of its reach and potential value in every economic sector could revolutionize the world we understand and experience today.

B. Manufacturing Impact

In addition to networked consumer-facing devices, Internet connectivity is being integrated into workforce processes, infrastructure, machines, and other production and supply chain elements within the manufacturing industry.[10] The emerging connectivity in this industry -

---

[1] Adam Thierer."The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation." Mercatus Center, George Mason University. November 2014. Available at: http://mercatus.org/sites/default/files/Thierer-Wearable-Tech.pdf
[2] *Id.*
[3] *Thierer*, Mercatus Center, George Mason University
[4] Comments of The Consumer Electronics Association to the Federal Trade Commission in the Matter of Privacy and Security Implications of the Internet of Things. June 10, 2013. Available at http://www.ftc.gov/sites/default/files/documents/public_comments/2013/07/00027-86193.pdf
[5] *Id*.
[6] Cisco's Internet Business Solutions Group. The Internet of Things Graphic. Available at http://share.cisco.com/internet-of-things.html
[7] *Id.*
[8] Internet of Things, McKinsey Quarterly at 6
[9] *Id*.
[10] Markus Loffler and Andreas Tschiesner. "The Internet of Things and the Future of Manufacturing." McKinsey & Company. June 2013. Available at: http://www.mckinsey.com/insights/business_technology/the_internet_of_things_and_the_future_of_manufacturing

sometimes referred to as the Industrial Internet of Things[11]- promises to have a transformational impact in terms of increased productivity and revenue, more efficient business models, and meaningful resource savings.[12] The Internet offers the potential for networks to link data to, from, or in between products, company assets, and the surrounding operating environment.[13] The connectivity generates better information and analysis about transport times, manufacturing steps, and inventory costs significantly enhancing and optimizing decision-making.[14] The IoT is helping manufacturing companies "drive inefficiencies out of their systems, manage workforce skills gaps, and uncover new business opportunities."[15] All of these possibilities are driven by Internet connectivity and could have a profound effect on the manufacturing industry's production processes, value chain, and possibly serve as the foundation for a new industrial revolution.[16]

C. Protecting Personal Information

Interconnectivity of the Internet of Things has brought attention to security and privacy. With the IoT market still in its very early stages of development, the challenge will be to understand the promise and implications of these new technologies and how to balance security and privacy in a manner that allows for continued competition in the marketplace and does not foreclose innovation.

D. Federal Trade Commission Activity

In September 2013, the Federal Trade Commission (FTC) initiated its first enforcement action related to an Internet of Things device.[17] In this case, the FTC alleged that TRENDnet, a marketer of an Internet-connected home security video camera called SecurView, failed to use reasonable security to protect consumers' privacy, even though it claimed in product descriptions that the device was secure.[18] The FTC was alerted to this security vulnerability after a hacker breached SecurView's software and publicized almost 700 private camera feeds on the Internet.[19] The FTC reached a settlement with TRENDnet in which the company agreed to establish a comprehensive information security program, notify customers about future security issues with the cameras, provide free technical support for 2 years, and obtain third-party assessments of its security programs every 2 years for the next 20 years.[20]

On November 19, 2013, the FTC conducted a workshop on the Internet of Things where it sought input from stakeholders about the privacy and security implications of the Internet of

---

[11] See http://www.accenture.com/us-en/technology/technology-labs/Pages/insight-industrial-internet-of-things.aspx
[12] *Id.*
[13] *Manufacturing*, McKinsey & Company
[14] Michael Chui, Markus Loffler, and Roger Roberts. "The Internet of Things. McKinsey Quarterly. March 2010. Available at: http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_internet_of_things
[15] See http://www.forbes.com/sites/ptc/2014/07/01/how-the-internet-of-things-is-transforming-manufacturing/
[16] *Manufacturing*, McKinsey & Company
[17] See http://www.informationintersection.com/2014/03/the-internet-of-things-has-the-ftcs-attention-so-it-should-also-have-yours/
[18] See http://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles
[19] *Id.*
[20] *Id.*

Things.[21] On January 21, 2015, the FTC released a Staff Report summarizing the discussions of the workshop and proposing recommendations in this area.[22] In the Report, FTC staff acknowledged that the IoT offers many benefits, such as more efficient and less expensive health care, conveniences in the home, and greater safety on the roadways.[23] FTC staff also acknowledged the privacy and security risks of the technology, recommending that industries develop self-regulatory programs and adopt "privacy-and security-sensitive practices."[24] The Report determined that specific legislation addressing the IoT was premature at this time, but staff did call for Federal data security and privacy legislation.[25]

The Commission vote to issue the Report was 4-1, with Commissioner Maureen Ohlhausen issuing a concurring statement and Commissioner Wright voting no and issuing a dissenting statement.[26] In Commissioner Ohlhausen's concurring statement, she identified 2 recommendations in the report that she did not support: 1) the recommendation for baseline privacy legislation, and 2) the recommendation for data minimization.[27] Commissioner Wright issued a dissent because FTC staff recommendations on best practices and broad-based privacy legislation were offered without analytical support showing that they would improve consumer welfare.[28]

IV. ISSUES

The following issues may be examined at the hearing:

- The wide breadth and scope of the IoT across industries in the U.S. economy.
- The IoT's transformative impact on the manufacturing industry.
- Consumer implications of the IoT and the protection of personal information.

V. STAFF CONTACTS

If you have any questions regarding this markup, please contact Paul Nagle or Olivia Trusty of the Committee staff at (202) 225-2927.

---

[21] See https://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world
[22] FTC Staff Report. Internet of Things: Privacy and Security in a Connected World. January 21, 2015. Available at: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf
[23] *Id.*
[24] *Id. at vii*
[25] *Id. at 48-50*
[26] See https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices
[27] See https://www.ftc.gov/system/files/documents/public_statements/620691/150127iotmkostmt.pdf
[28] See https://www.ftc.gov/system/files/documents/public_statements/620701/150127iotjdwstmt.pdf