KEYNOTE REMARKS OF COMMISSIONER TERRELL MCSWEENY[1]
The 4th Annual Internet of Things Global Summit
Washington Marriott Georgetown, Washington, DC
October 7, 2016

Good morning, everyone, and thank you, Jonathan, for that very nice introduction. It's wonderful to be here today and have the opportunity to talk to so many critical stakeholders about the FTC's view of the challenges and opportunities posed by the ever-increasing Internet of Things.

As many of you know, the FTC is the nation's primary federal law enforcer with regard to consumer privacy and data security. The FTC is more than 100 years old and we've been doing this work for decades. We have used our general Section 5 enforcement authority under the FTC Act to protect consumers against deceptive and unfair practices to hold firms accountable for their promises about consumer privacy and to ensure that they take reasonable steps to safeguard personal information. We've applied these general principles to brick and mortar stores, to online business, to mobile apps, and even to the Internet of Things.

Almost three years ago – in November 2013 – the FTC hosted a workshop on the privacy and security implications of the growing Internet of Things, a concept that at the time was not in the common vernacular. In January 2015, we published a staff report highlighting the benefits and risks of having more everyday objects connected to the internet and set forth recommended practices for IoT device manufacturers. And now as we look back on that report of almost two years ago, I think we can say that possibilities of the IoT have probably exceeded our expectations – in ways both good and bad.

On the positive side of the ledger, of course consumers enjoy many increased conveniences and functionalities from devices connected to the Internet. There are obvious benefits and efficiencies from sensors that tell consumers where to find an empty parking space or optimize traffic signals, devices that send diagnostic information about malfunctions to the manufacturer or can install security patches over the air, wristbands that track a wearer's physical activity, medical devices that can be monitored and operated remotely, and footage from security cameras that can be viewed from afar. One might question whether there is anything too trivial to connect to the internet, because now even socks, tea-kettles, water bottles and toothbrushes are becoming part of the Internet of Things.

However, at the same time, consumers are already beginning to experience and react to some of the security and privacy risks associated with insecure IoT products – from high-profile hacks of vehicles to insecure routers that put home networks at risk.

It is no surprise, therefore, that consumer faith in their data security and privacy is relatively low. In a recent survey of more than 41,000 US households, one in five reported

[1] The views expressed in this speech are my own and do not necessarily reflect those of the Commission or any other Commissioner.

being the victim of a security breach and 84 percent cited concerns about online privacy and security.[2]

Consumer trust appears to be a growing issue – one that may be affecting IoT adoption.[3] That consumers are identifying security as a top barrier to purchasing connected devices suggests to me that we enforcers have an important job to do – and that it is necessary to strengthen US privacy and data security laws.

Certainly, in many cases, aspects of cost-benefit analysis for consumers regarding privacy and data security risks can be quite clear. For instance, if an employer offers a discount on health insurance premiums to employees who wear a fitness tracker, employees can find out what information the tracker collects and decide if they think it's worth it to share that information to save money.

But the real challenge in protecting consumers in the era of connected everything is that many of the tradeoffs these devices require are not transparent to consumers, thereby depriving them of the ability to make an educated decision about whether or not they believe using the device is worth the risk. And I think we have to frankly acknowledge as a baseline matter that putting any device that transmits data online, whether it's to the cloud, or to another device via Bluetooth or wi-fi, injects an additional element of risk.

Through decades of experience with home computers and more recently with smartphones, I think that many consumers are aware of the fact that they can play an active role in maintaining good security hygiene on their personal computers and smartphones. Consumers generally know the basics - that they should have current anti-virus software, not click on unknown links, and not open suspicious attachments. But do they know what proactive measures they need to take to secure their internet-connected coffee maker or pet feeder?

Perhaps a consumer thinks to herself, "what do I care if someone hacks into my connected toaster and finds out that I use the bagel setting on Sundays – what difference does it make?" The problem is that these billions of devices that are coming on line and into our homes are connected to wi-fi and home networks. This means that they can serve as a conduit to a bad actor to commit serious damage, even though the risk might not be obvious or visible to the device owner. And the fact that many IoT devices do not have screens or obvious ways to receive security updates only exacerbates the problem.

A consumer who buys a connected toaster may very well treat it the way she treats her analog toaster – plugging it in and forgetting about it. And here it's critically important for manufacturers to do a better job communicating to consumers about expectations and security risks. Any device that is connected to the internet through a consumer's home network needs to have security measures reasonably designed to protect information transmitted from that device

---

[2] Rafi Goldberg, Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities, NTIA (May 13, 2016), available at https://www.ntia.doc.gov/print/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities

[3] Accenture, *Igniting Growth in Consumer Technology*, January 5, 2016, *https://www.accenture.com/_acnmedia/PDF-3/Accenture-Igniting-Growth-in-Consumer-Technology.pdf*

and from other devices on the same network. Manufacturers need to implement "Security by Design," meaning that from the moment in the design cycle someone makes the decision to connect a device to the internet, someone needs to be closely assessing security risks and vulnerabilities and how to address them. And just as important, this job doesn't stop the moment that the merchandise is purchased by a user and shipped from the warehouse. Reasonable security entails keeping up with emerging threats and new vulnerabilities and providing consumers with notice of such risks and software updates to address them.

Now I realize that the costs of sensors has dropped dramatically which is why we're seeing what I alluded to earlier as the Internet of Trivial things. And here manufacturers might find a tension between maintaining the low costs of devices and the resources required to continually provide consumers with security updates and patches over time. After all, will a manufacturer commit to provide security updates to a $40 connected toaster for the many years of its expected lifetime? And how will it inform the owner of the availability of updates and how will the updates be delivered? Because connecting devices to the internet creates an element of potential risk – not just for that specific device, but to other devices connected to the same network – perhaps we should not be so cavalier about connecting everyday items to the internet just because we can and for the novelty value. Security risks and costs need to be taken into account during product development.

It's incumbent on manufacturers to communicate clearly to consumers up front what they can expect with their IoT devices. While many connected devices may not have screens that allow for clear disclosures – or they may only have very small screens not suitable for detailed communication – manufacturers need to find other means to communicate clearly and conspicuously the key features of IoT devices. What security protections are in place? What data are being collected and how long will they be retained? What data are being sold or shared, and with whom? How can consumers make sure that they keep apprised of security updates and patches? Is the manufacturer committing to update the product for only a set number of years?

I have serious concerns about internet-connected devices that are suddenly "bricked" and become useless after the manufacturer discovers security problems that it no longer wants to patch. The decision to effectively render IoT devices useless of key internet functionality can be not only contrary to reasonable consumer expectations, but extremely harmful to consumers, who purchased a device assuming that it would have the same serviceable lifetime as its non-connected counterpart. In the absence of clear and conspicuous disclosure and express consumer choice to the contrary, manufacturers need to conform to reasonable consumer expectations regarding functionality, data collection and security practices, and product lifetime in order to earn consumer trust of connected devices and promote continued growth of the IoT. Earlier this year when Nest abruptly stopped supporting the Revolv smart home hub, the FTC carefully examined a number of factors including the number of units sold, Nest's practice of providing full refunds after the Revolv system shutdown was announced and its notifications to consumers.[4]

[4] Letter from Mary K. Engle, Associate Director, Division of Advertising Practices, Fed. Trade Comm'n, to Richard J. Lutton, Jr, Head of Legal and Regulatory Affairs, Nest Labs, Inc., (July 7, 2016), https://www.ftc.gov/system/files/documents/closing_letters/nid/160707nestrevolvletter.pdf

In addition, everyone in this ecosystem – and I'm including the FTC in this group – needs to do a better job educating consumers about some of the unique risks to the IoT that may not be obvious. For instance, the FTC recently held a workshop on ransomware, which has become a growing threat on desktop computers. But it's only natural to think that ransomware attacks will migrate to the IoT. Does a consumer know what to do if her coffee maker stops working and she gets a demand for $10 to turn it back on? What if someone hacks into the telematics of her connected car and disables the ignition, demanding a ransom to turn control back to the owner? At the moment these problems may be hypothetical, but that shouldn't stop companies from developing plans to mitigate these kinds of attacks.

Finally, I want to mention a recent development we've seen when unsecured IoT devices, such as security cameras and DVRs, are being harnessed into massive bot armies to implement large-scale DDOS attacks – a security concern the FTC noted in its 2015 IoT report. I'm sure many of you are aware that security researcher Brian Krebs recently found himself the victim of a distributed denial of service of attack that reportedly was sending 620 gigabits per second of junk data to his website. The attack was one of the largest ever reported. A few days later French web hosting provider OVH reported being hit by an even larger DDOS attack, with combined peak traffic of over 1 terabits per second. And what made these attack possible? Security researchers report that the perpetrators harnessed the IoT, namely, security cameras and video recorders that were not adequately secured. Hackers often access such devices through previously infected or poorly protected wi-fi routers. As it happens, the FTC has brought enforcement actions against the manufacturer of internet-connected security cameras that were not secure, as well as against the manufacturer of insecure wi-fi routers that put the home network of thousands of consumers at risk.

There is an industrywide need to find effective solutions to secure the Internet of Things – and, I would argue, need for the next Congress to pass comprehensive data security legislation. The sheer number of connected devices can pose a grave threat that individual consumers may never personally see or appreciate. We need to make sure that these disruptive technologies and business models don't disrupt our daily lives and become obstacles for consumers and vectors for mischief.

So I look forward to continuing to discuss these issues and working together with all of you to make sure that we each do our part to help secure the Internet of Things. IoT security is an issue that requires thoughtful consideration from consumers, manufacturers, regulators and law enforcers, and advocates alike.