Opening Remarks of FTC Chairwoman Edith Ramirez
The Internet of Things: Privacy and Security in a Connected World
Washington, DC
November 19, 2013

I. Introduction

Good morning, everyone, and welcome to the FTC's workshop on the Internet of Things. I want to begin by thanking the FTC staff who organized this program. I also want to thank the many speakers who have assembled here today for contributing their time and expertise.

The Internet of Things has already entered the daily lives of many consumers. We can now rely on home security systems that show us who is at the front door on a screen on our tablets, even if we are across the country. We wear wireless medical and fitness devices that share our blood glucose readings with our doctors or tweet our race time to our followers. And sensors on our plants can send a message to our smartphones to remind us they need watering.

But we are at the cusp of tremendous change. Today's workshop examines the next technological leap when most everyday physical objects will be able to communicate with other objects, as well as with us. Almost anything to which a sensor can be attached can become a node in a ubiquitous network, continuously transmitting data in real time. It is estimated that there are already 3.5 billion such sensors,[1] and some experts expect that number to increase to trillions within the next decade.[2]

---

[1] *See* TSensors Summit™ for Trillion Sensor Roadmap, *available at* http://tsensorssummit.org/Resources/Why%20TSensors%20Roadmap.pdf.

[2] *See id*.

It is still early when it comes to the Internet of Things but it is clear that change is afoot. Five years ago, for the first time, more "things" than people connected to the Internet.[3] By 2020, an estimated 90 percent of consumer cars will have some sort of vehicle platform, up from 10 percent today.[4] And it is estimated that by 2015, there will be 25 billion things hooked up to the Internet.[5] By 2020, we are told the number will rise to 50 billion.[6]

The Internet of Things is poised to transform manufacturing, business, and agriculture. Much of this can occur without collecting data about individuals. In the consumer market, smart devices will track our health, help us remotely monitor an aging family member, reduce our monthly utility bills, and even alert us that we are out of milk. The benefits to consumers will no doubt be great. But these benefits come with undeniable privacy risks. The very technology that allows you to stream your favorite movie or send for help when your car breaks down can also collect, transmit, and compile information about your actions.

II. Challenges Associated with Connected Devices

As I see it, the expansion of the Internet of Things presents three main challenges to consumer privacy: first, it facilitates the collection of vastly greater amounts of consumer data; second, it opens that data to uses that may be unexpected by consumers; and third, it puts the

---

[3] *See* Cisco Internet Business Solutions Group, *The Internet of Things How the Next Evolution of the Internet Is Changing Everything* 3 (Apr. 2011), *available at* http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

[4] *See* Telefonica, Connected Car Industry Report 2013 9 (2013), *available at* http://websrvc.net/2013/telefonica/Telefonica%20Digital_Connected_Car2013_Full_Report_English.pdf.

[5] *See* Cisco Internet Business Solutions Group, *The Internet of Things How the Next Evolution of the Internet Is Changing Everything* 3 (Apr. 2011), *available at* http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

[6] *See id*.

security of that data at greater risk. I'd like to give you my perspective on each of these challenges, and I look forward to others addressing them throughout the day.

A. Ubiquitous Collection

Let me turn first to the ubiquitous collection of consumer data that the Internet of Things will enable. We are told to expect that in the not too distant future, many, if not most, aspects of our everyday lives will be digitally observed and stored. The enormous data trove that will result will contain a wealth of revealing bits of information that, when patched together, may present a deeply personal and startlingly complete picture of each of us – our health, our religious preferences, our financial circumstances, and our family and friends. Our personal profiles will be parsed, augmented, and shared as they travel through an interconnected mosaic of commerce.

As one tech writer has explained in highly technical terms, "The 'Internet of things' will mean really, really big data."[7] With big data comes big responsibility. It is up to the companies that take part in this ecosystem to embrace their role as stewards of the consumer data they collect and use. That means adherence to the three core best practices espoused by the FTC: privacy by design, simplified consumer choice, and transparency.

First, privacy by design. Companies developing new products should build in consumer privacy protections from the outset. Privacy should be integral to the innovation process, with privacy hard-coded in. Companies should also consider how to shift the burden of privacy protection off the shoulders of consumers. For example, are there defaults or other design features that can help prevent consumers from sharing personal data in an unwanted manner? Privacy tools and settings should be as easy to use as the underlying product or service.

---

[7] Bob Violino, *The 'Internet of things' will mean really, really big data*, InfoWorld, July 29, 2013, *available at* http://www.infoworld.com/d/big-data/the-internet-of-things-will-mean-really-really-big-data-223314.

The second central principle is simplified consumer choice: Taking context into account, the companies that take part in the Internet of Things should give consumers control over their data. Often, this will mean just-in-time choice.

And that brings me to the third, and related, principle, which runs through all the FTC's privacy recommendations: transparency. Transparency is crucial. As more and more of our devices become smarter and smarter, it is essential we know as much about them as they know about us – that we understand what information the devices are collecting and how it is being used or shared.

I do not pretend these privacy best practices are a panacea, or that they will always be easy to implement. Privacy on the World Wide Web and on mobile devices is already challenging. Even on a website on their desktop computer, consumers still often lack effective mechanisms to understand and control how their data is collected and used. On a smartphone, the smaller screen exacerbates this challenge. And the difficulties will be exponentially greater with the advent of the Internet of Things, as the boundaries between the virtual and physical worlds disappear. Will consumers understand that previously inert everyday objects are now collecting and sharing data about them? How can these objects provide just-in-time notice and choice if there is no user interface at all? And will we be asking consumers to make an unreasonable number of decisions about the collection and use of their data?

The answers to these and other questions may not be simple. But in my mind the question is not *whether* the core principles of privacy by design, simplified choice, and transparency should apply to the Internet of Things. The question is *how* to adapt them to the Internet of Things.

B. Unexpected Uses of Data

The ubiquitous collection of data in our wired world inevitably gives rise to concerns about *how* all this personal information is used. Is the data used solely to provide service to the consumer? Or will the information flowing in from our smart cars, smart devices, and smart cities just swell the ocean of "big data" – allowing the creation of profiles about consumers and inferences and predictions about their behavior?

Connected cars may direct emergency responders to an accident, but will the data transmitted be shared with your insurer who may raise your rate or cancel your policy? Your smart TV may track whether you watch Masterpiece Theatre or the Kardashians, but will your TV-viewing habits be shared with prospective employers or schools? Or to data brokers, who will put that nugget together with information collected by your parking lot security gate, your heart monitor, and your smart phone, and paint a picture of you that you won't see but that others will – people who might make decisions about whether you are shown ads for organic food or junk food, what sale offers you receive, and where your call to customer service is routed.

C. Security

Finally, let me move to security. Any device connected to the Internet is potentially vulnerable to hijack, and companies need to build security into their products, no exceptions. In the Internet of Things, data security will take on new importance as it may affect the safety of our cars, medical devices, and homes.

Companies that don't pay attention to their security practices may find that the FTC will, as a company called TRENDnet recently learned. In the FTC's first enforcement foray into the Internet of Things, we alleged that TRENDnet's lax software design and testing of its IP-

connected security cameras enabled a hacker to get his hands on the live feeds from 700 cameras and make them available on the Internet.[8]

The FTC is particularly vigilant when it comes to safeguarding sensitive consumer data, such as health information. I highlight the importance the FTC places on health information because of the numerous devices gathering health data – from wearable fitness devices that help us track and record exercise or sleep or blood pressure to "smart pills" that tell doctors whether we're taking our medicine. These devices are poised to revolutionize healthcare. But we must also take special care to prevent sensitive health information from falling into the wrong hands. This is among the crucial subjects to be discussed during today's program.

III. Conclusion

So, in closing, let me end where I began. We are at the dawn of the Internet of Things. And like all dawns, the first light of the new day both illuminates and casts shadows. We see the promise of improved safety, health, and efficiency as the items of our everyday life come alive. But we are alert to the challenge of protecting consumer privacy in a cyber environment that breathes our personal data like oxygen.

Consumers will enthusiastically invite the Internet of Things into their homes, cars, and workplaces only if they are confident that they remain in control over their data. I know that we can find a way to reap the rewards from our connected future while mitigating the privacy and security challenges that it brings. The purpose of today's program is to figure out how. Thank you for joining us in that endeavor.

---

[8] *TRENDnet, Inc.*, File No. 122 3090 (F.T.C. Sept. 4, 2013) (complaint and proposed consent order), *available at* http://www.ftc.gov/os/caselist/1223090/index.shtm.