Opening Remarks of FTC Chairwoman Edith Ramirez
Privacy and the IoT: Navigating Policy Issues
International Consumer Electronics Show
Las Vegas, Nevada
January 6, 2015

Good afternoon. I would like to thank the Consumer Electronics Association for inviting me to lead off today's discussion on protecting privacy in the emerging era of the Internet of Things.

I was delighted to have the opportunity to tour the CES "show floor" this morning – the exhibits showcasing new connected products, services, and technologies certainly confirm that the IoT has arrived. Whether it is a remote valet parking assistant, which allows drivers to get out of their cars and remotely guide their empty car to a parking spot; a new fashionable bracelet that allows consumers to check their texts and see reviews of nearby restaurants; or smart glucose meters, which make glucose readings accessible both to those afflicted with diabetes and their doctors, the IoT has the potential to transform our daily lives. Just looking around this room, I can see smart health bands everywhere, tracking our steps and movements in the hopes of fulfilling our New Year's resolutions.

As we embark on a new year, observers have made a number of predictions for the IoT. We are told that, in 2015, the world will have 25 billion connected devices;[1] the number of smart home devices will reach nearly 25 million;[2] and IoT software platforms will "become the

[1] DAVE EVANS, CISCO INTERNET BUS. SOLUTIONS GRP., THE INTERNET OF THINGS HOW THE NEXT EVOLUTION OF THE INTERNET IS CHANGING EVERYTHING 3 (2011), *available at* http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf. These estimates include all types of connected devices, not just those aimed at the consumer market.

[2] Press Release, Consumer Electronics Association, CEA and Parks Associates Find Twenty Percent of U.S. Broadband Households to Acquire One or More Smart Home Devices Within the Next Year (Oct. 16, 2014), *available at* http://www.ce.org/News/News-Releases/Press-Releases/2014/CEA-and-Parks-Associates-Find-Twenty-Percent-of-U.aspx.

rage."[3] But we have also been warned that 2015 will be the year we start hearing about smart-home hacking.[4]

These predictions highlight the complexity of the IoT – it has the potential to provide enormous benefits for consumers, but it also has significant privacy and security implications. The IoT could improve global health, modernize city infrastructures, and spur global economic growth. To be sure, these potential benefits are immense, but so too are the potential risks. Connected devices that provide increased convenience and improve health services are also collecting, transmitting, storing, and often sharing vast amounts of consumer data, some of it highly personal, thereby creating a number of privacy risks.

Today, I would like to focus on three key challenges that, in my view, the IoT poses to consumer privacy: (1) ubiquitous data collection; (2) the potential for unexpected uses of consumer data that could have adverse consequences; and (3) heightened security risks. These risks to privacy and security undermine consumer trust. And that trust is as important to the widespread consumer adoption of new IoT products and services as a network connection is to the functionality of an IoT device.

I believe there are three key steps that companies should take to enhance consumer privacy and security and thereby build consumer trust in IoT devices: (1) adopting "security by design"; (2) engaging in data minimization; and (3) increasing transparency and providing consumers with notice and choice for unexpected data uses. I believe these steps will be key to successful IoT business models and to the protection of consumer information.

[3] Frank Gillett, Internet of Things Software Platforms Will Become the Rage in 2015, Forrester (Nov. 13, 2014), http://blogs.forrester.com/frank_gillett/14-11-13-internet_of_things_software_platforms_will_become_the_rage_in_2015.

[4] John Shinal, *2015 Could Be Year of First Smart-Home Hacks*, USA TODAY, Dec. 30, 2014, *available at* http://www.usatoday.com/story/tech/columnist/shinal/2014/12/30/the-future-of-the-smart-connected-home/20763995/.

I. Privacy and Security Risks of Connected Devices

A. Ubiquitous Data Collection

Let me start by expanding on the three privacy challenges I identified. The first is the ubiquitous collection of personal information, habits, location, and physical condition over time. In the not too distant future, many, if not most, aspects of our everyday lives will leave a digital trail. That data trove will contain a wealth of revealing information that, when patched together, will present a deeply personal and startlingly complete picture of each of us – one that includes details about our financial circumstances, our health, our religious preferences, and our family and friends.

The introduction of sensors and devices into currently intimate spaces – like our homes, cars, and even our bodies – poses particular challenges and increases the sensitivity of the data that is being collected. Connected devices are effectively allowing companies to digitally monitor our otherwise private activities. Moreover, the sheer volume of granular data that a small number of devices can generate allows those with access to the data to perform analyses that would not be possible with less rich data sets, providing the ability to make additional sensitive inferences and compile even more detailed profiles of consumer behavior.

B. Unexpected Uses of Consumer Data

This pervasive collection of data inevitably gives rise to concerns about how all of this personal information will be used. Will the data be used solely to provide services to consumers? Or will the information flowing in from our smart cars, smart devices, and smart cities just swell the ocean of "big data," which could allow information to be used in ways that are inconsistent with consumers' expectations or relationship with a company?

Your smart TV and tablet may track whether you watch the history channel or reality television, but will your TV-viewing habits be shared with prospective employers or universities? Will they be shared with data brokers, who will put those nuggets together with information collected by your parking lot security gate, your heart monitor, and your smart phone? And will this information be used to paint a picture of you that you will not see but that others will – people who might make decisions about whether you are shown ads for organic food or junk food, where your call to customer service is routed, and what offers of credit and other products you receive?

And, as businesses use the vast troves of data generated by connected devices to segment consumers to determine what products are marketed to them, the prices they are charged, and the level of customer service they receive, will it exacerbate existing socio-economic disparities?

We cannot continue down the path toward pervasive data collection without thinking hard about all of these questions.

C. Security

Third, the IoT poses a number of security risks. Any device that is connected to the Internet is at risk of being hijacked. Like traditional computers and mobile devices, inadequate security on IoT devices could enable intruders to access and misuse personal information collected and transmitted by the device. And, as we purchase more smart devices, they increase the number of entry points an intruder could exploit to launch attacks on or from. Moreover, the risks that unauthorized access create intensify as we adopt more and more devices linked to our physical safety, such as our cars, medical care, and homes.

Data security is already challenging, as evidenced by the growing number of high profile breaches with which we are all familiar. But security in an IoT world is likely to present unique challenges. As an initial matter, some of the developers entering the IoT market, unlike hardware and software companies, have not spent decades thinking about how to secure their products and services from hackers.[5] And, the small size and limited processing power of many connected devices could inhibit encryption and other robust security measures.[6] Moreover, some connected devices are low-cost and essentially disposable. If a vulnerability is discovered on that type of device, it may be difficult to update the software or apply a patch – or even to get news of a fix to consumers.

II. Industry Solutions

A. Security by Design

Now that I have addressed the potential problems, let me turn to what I think should be done to address these risks. First, companies should prioritize security and build security into their devices from the outset. Specifically, companies should: (1) conduct a privacy or security risk assessment as part of the design process; (2) test security measures before products launch; (3) use smart defaults – such as requiring consumers to change default passwords in the set-up process; (4) consider encryption, particularly for the storage and transmission of sensitive information, such as health data; and (5) monitor products throughout their life cycle and, to the extent possible, patch known vulnerabilities.

In addition, companies should implement technical and administrative measures to ensure reasonable security, including designating people responsible for security in the organization, conducting security training for employees, and taking steps to ensure service providers protect

[5] Brian Fung, *Here's the Scariest Part of the Internet of Things*, WASH. POST, Nov. 19, 2013, *available at* http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/19/heres-the-scariest-part-about-the-internet-of-things/.

[6] Stacey Higginbotham, The Internet of Things Needs a New Security Model, Which One Will Win? GigaOm (Jan. 22, 2014), https://gigaom.com/2014/01/22/the-internet-of-things-needs-a-new-security-model-which-one-will-win/.

consumer data.

B. Data Minimization

Second, companies that collect personal information should follow the principle of data minimization. In other words, companies should collect only the data needed for a specific purpose and then safely dispose of it afterwards. Data minimization is a longstanding privacy principle, and for good reason: Data that has not been collected or that has already been destroyed cannot fall into the wrong hands. Collecting and retaining large amounts of data greatly increases the potential harm that could result from a data breach.

We often hear the argument that to realize the benefits of big data, businesses should not face limits on the collection and retention of data because the value lies in its unanticipated uses. But I question the notion that we must put sensitive consumer data at risk on the off-chance a company might someday discover a valuable use for the information.

I agree that we need more dialogue on acceptable and unacceptable uses of consumer data. But I continue to believe that reasonable limits on data collection and retention are a necessary first line of protection for consumers.

To the extent that companies collect information, they should de-identify consumer data where possible. Many of the beneficial big-data uses from the IoT could still be accomplished by using de-identified data. De-identification isn't perfect. There is always the possibility that ostensibly anonymized data can be re-identified. To address this issue, sound technical strategies for making data anonymous should be coupled with administrative safeguards. As the Federal Trade Commission has said, companies should publicly commit not to seek to re-identify data and they should, through contract, require the same of those with whom they share data.[7]

[7] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 21-22 (2012).

C. Notice and Choice for Unexpected Uses

Finally, companies should give consumers clear notice and provide simplified choices for unexpected collection or uses of their data. Consumers know, for instance, that a smart thermostat is gathering information about their heating habits, and that a fitness band is collecting data about their physical activity. But would they expect this information to be shared with data brokers or marketing firms? Probably not. In these and similar cases, consumers should be given clear and simple notice of the proposed uses of their data and a way to consent. This means notice and choice outside of lengthy privacy policies and terms of use.[8]

I recognize that providing notice and choice in an IoT world is easier said than done. Connected devices may have little or no interfaces that readily permit choices. And we risk inundating consumers with too many choices as connected devices and services proliferate. But in my mind, the question is not *whether* consumers should be given a say over unexpected uses of their data; rather, the question is *how* to provide simplified notice and choice.

I am confident that the same ingenuity, design acumen, and technical know-how that is bringing us the IoT can also provide innovative ways to give consumers easy-to-understand choices.

I believe steps like the ones I have described are critical to fostering consumer trust. And they are also good business.

***

[8] FTC staff recently completed a survey of roughly 150 mobile apps and found that nearly all had privacy policies with broad and vague statements regarding how they handled data, making it difficult to assess how the data would actually be used and with whom it would be shared. FED. TRADE COMM'N STAFF, WHAT'S THE DEAL? AN FTC STUDY ON MOBILE SHOPPING APPS 16-24 (2014), *available at* http://www.ftc.gov/reports/whats-deal-federal-trade-commission-study-mobile-shopping-apps-august-2014.

We are on the cusp of a new technological revolution. Some observers have argued that precisely because the IoT is in its early stages, we should wait to see how it evolves before addressing privacy and security issues. But I believe we have an important opportunity to ensure that new technologies with the potential to provide enormous benefits develop in a way that also protects consumer information.

As is evident here this week, companies are investing billions of dollars in this growing industry; they should also make appropriate investments in privacy and security. The stakes are too high to do otherwise. So, as we commit to New Year's resolutions, we should also resolve to take appropriate steps for the IoT to flourish and reach its full potential across our economy in a way that does not harm or sacrifice consumer privacy.

Thank you.