

**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

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 than people connected to the Internet.<sup>3</sup> By 2020, an estimated 90 percent of consumer cars will have some sort of vehicle platform, up from 10 percent today.<sup>4</sup> And it is estimated that by 2015, there will be 25 billion things hooked up to the Internet.<sup>5</sup> By 2020, we are told the number will rise to 50 billion.<sup>6</sup>

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

security of that data at greater risk. 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,

<sup>7</sup> 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

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.

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?

## **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 \_\_\_\_\_ 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 \_\_\_\_\_

connected security cameras enabled a hacker to get his hands on the live feeds from 700 cameras and make them available on the Internet.<sup>8</sup>

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 er