The Internet of Things: When Things Talk Among Themselves
Remarks of Commissioner Maureen K. Ohlhausen
FTC Internet of Things Workshop
November 19, 2013

I am delighted to have the opportunity to set the stage for the afternoon sessions of the Internet of Things workshop. Given my particular focus on technology policy, I am very interested in the evolution of the Internet from its start as basically a one-way conversation, where websites provided information to users; to the rise of social media, where users not only talked back to webs
medicine, and transportation, as today's panelists have and will continue to discuss. These new capabilities clearly will offer great benefits to consumers in their day-to-day lives but we must also be sensitive to the fact that the ability to collect large amounts of information and, in some cases, to act on that information also raises important consumer privacy and data security issues, as our last panel will address. I am pleased that the FTC is holding this workshop to get a better understanding of how to achieve the benefits of the Internet of Things while reducing risks to consumers' privacy.

I consider the Commission's interest in the Internet of Things to be another chapter in our work on consumer privacy and data security issues. It is a particularly interesting chapter to me, however, because it also draws together several hot issues in this space, such as data security, mobile privacy, and big data. On a more philosophical level, it also raises the question of what is the best approach for a government agency like the FTC to take with regard to technological and business innovation. The success of the Internet has in large part been driven by the freedom to experiment with different business models, the best of which have survived and thrived, even in the face of initial unfamiliarity and un

structures, including any self-regulation; market dynamics; and the nature and extent of likely consumer and competitive benefits and risks. Second, we should use this learning to educate consumers and businesses on how to avoid or minimize any risks that we may identify. Providing consumer tips and suggesting best practices for business is one of the FTC's most valuable and cost-effective activities. Of course, the FTC is also an enforcement agency and it can and should use its traditional deception and unfairness authority to stop consumer harms that may arise from particular Internet-connected devices. This not only helps consumers but also benefits the companies involved in the Internet of Things by policing actors that may tarnish the technology itself. Likewise, the FTC should use its flexible and fact-intensive approach to antitrust enforcement to investigate and, where appropriate, challenge competitive harms occurring in the Internet sphere.

For the remainder of my remarks, I will touch briefly on some specific issues—data security, mobile privacy, and big data—that have particular relevance to the development of the Internet of Things.

Data Security

As you know, the FTC, as part of its broad focus on consumer privacy, has an active data security program. The importance of this program will only continue to grow with the Internet of Things, which will sometimes involve the transmission of sensitive data such as a consumer's health status or private activities within the home. You may have heard about a recent FTC case that exemplifies the kinds of data security risks that the Internet of Things may present. In September, the FTC settled a case against TRENDnet, which sold its Internet-connected SecurView cameras for purposes ranging from home security to baby monitoring.[1] Although the company claimed that the cameras were secure, they actually had faulty software that allowed unfettered online viewing by anyone with a camera's Internet address. As a result, hackers posted live feeds of nearly 700 consumer cameras on the Internet, showing activities such as babies asleep in their cribs and children playing in their homes.

The type of consumer harm we saw in the TRENDnet case—surveillance in the home by unauthorized viewers—feeds concerns about the Internet of Things overall. It is thus crucial that companies offering these technologies take the necessary steps to safeguard the privacy of users to avoid giving the technology a bad namem0 .4(tobab(eras (i)-1.505 0)8.3(e-.08 TTD5.6h soinf.4(y spheings.)Tj/TT-14)T

billion in 2010 to 6.8 billion at the end of 2012.[2] Mobile devices play an important role in the Internet of Things as they collect, analyze, and share information about users' actions and their environments, from their current location, travel patterns, and speeds to their surrounding noise levels. This raises questions of how businesses should convey on the small phone screen information about what data, sometimes of a sensitive nature, that these devices and apps collect, use, and share.

The Commission is devoting significant resources to addressing the mobile phenomenon. In addition to setting up a dedicated Mobile Technology Unit of tech-savvy folks, we have held workshops, issued reports, conducted research, and developed extensive consumer and business education materials.[3]

The Commission has also been very active on the enforcement front in the mobile space. One case that has implications for the Internet of Things involved an app that collected information from consumers' address books on their mobile phones without the consumers' knowledge or consent. The FTC settled a complaint against Path, a social networking company, for this activity, as well as for alleged violations of the Children's Online Privacy Protection Act.[4] As this case suggests, the collection of personal information from a consumer's mobile phone without disclosure or permission may be a deceptive or unfair practice under the FTC Act. This has obvious implications for other Internet-connected devices that collect pe

In response to these kinds of concerns, the Commission recently began a formal study of the data broker industry. We sent out formal requests for information to nine large data brokers to learn more about their practices, including how they use, share, and secure consumer data.[6] It is vital that we have a good understanding of how data brokers operate because appropriate use of data can greatly benefit consumers through better services and convenience while inappropriate use or insecure maintenance of data could cause significant harm to consumers. We will carefully analyze the submissions from the companies and use the information to decide how to proceed in this area.

* * *

The Internet has evolved in one generation from a network of electronically interlinked research facilities in the United States to one of the most dynamic forces in the global economy, in the process reshaping entire industries and even changing the way we interact on a personal level. And the Internet of Things offers the promise of even greater things ahead for consumers and competition.

The FTC's approach of doing policy R&D to get a good understanding of the technology, educating consumers and businesses about how to maximize its benefits and reduce its risks, and using our traditional enforcement tools to challenge any harms that do arise offers, in my opinion, the best approach. This type of informed action will allow free markets and technological innovation to serve the greatest good, while still maintaining a federal role in protecting consumers and ensuring a level playing field for competitors.

Thank you for your attention.

---

[6] Press Release, Fed. Trade Comm'n, FTC to Study Data Broker Industry's Collection and Use of Consumer Data (Dec. 18, 2012), *available at* http://ftc.gov/opa/2012/12/databrokers.shtm.