United States of America

Federal Trade Commission

The Internet of Things and The FTC:
Does Innovation Require Intervention?

Remarks of Maureen K. Ohlhausen*
Commissioner, Federal Trade Commission

U.S. Chamber of Commerce
Washington, D.C.

October 18, 2013

The Internet has been an enormously powerful driver of communication and commerce, connecting people around the world to each other, as well as to vast sources of information, products, and services. The paradigmatic consumer Internet experience began with a person sitting at a desktop computer typing in a website address in a browser or using a search engine. It then moved to mobile smart phones and tablets that allow people to access the Internet on the go through apps as well as through browsers and search engines. The next phase of Internet development is focusing on connecting devices and other objects to the Internet, without the active role of a live person, so that they can collect and communicate information on their own and, in many instances, take action based on the information they send and receive. This is often called the Internet of Things.

For some reason, the most cited example of the potential benefit of the Internet of Things is that your refrigerator will note that you have run out of milk and it will email or text you to remind you to buy milk. Maybe milk is a more important part of some people's lives

* The views expressed in this speech are my own and do not necessarily reflect the views of the Federal Trade Commission or any other Commissioner.

than it is of mine, but I am much more excited about the prospect that my car will automatically direct me to a route without a traffic jam or that a wearable health device will detect an impending medical crisis and alert me or my doctor. But maybe that's just me.

So what, exactly, is the Internet of Things? In my view, it means sensors and other types of telemetry embedded in physical objects, from cars to appliances to medical devices, that are linked through wired and wireless networks using the same Internet protocol that connects the Internet generally. These objects can record and measure the environment around them, from the apparently dreaded milk-less refrigerator to the irregularly beating heart, send that information to remote computers for recording and analysis, and, sometimes, take action in response to what they detect, such as suggesting a stop at the grocery store or delivering a life-saving intervention. These capabilities have the potential to revolutionize many fields, including manufacturing and logistics, medicine, transportation, and energy, just to name a few. They also clearly will offer great benefits to consumers in their day-to-day lives.

As someone who has focused on technology policy, I am very inspired by the transformative potential of the Internet of Things but am also 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. Thus, I am pleased that the FTC is holding a workshop on the Internet of Things on November 19 to get a better understanding of how to achieve its benefits while reducing risks to consumers' privacy.[1] I invite all of you to attend.

[1] Press Release, Fed. Trade Comm'n., FTC Seeks Input on Privacy and Security Implications of the Internet of Things (Apr. 17, 2013), *available at* http://www.ftc.gov/opa/2013/04/internetthings.shtm.

The workshop will examine a variety of issues, such as:

- What are the unique privacy and security concerns associated with smart technology and its data?
- What steps can companies take to prevent smart devices from becoming targets of or vectors for malware or adware?
- How should we weigh privacy risks against potential societal benefits, such as the ability to generate better data to improve health-care decision making or to promote energy efficiency?
- Can and should de-identified data from smart devices be used, and if so, under what circumstances?

In my view, the Commission's interest in the Internet of Things is 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, as well issues from the competition side of the house, such as net neutrality, in which I have long taken a leading role.

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 unease about the impact on consumers and competitors. It is thus vital that government officials, like myself, approach new technologies with a dose of regulatory humility, by working hard to educate ourselves and others about the innovation, understand its effects on consumers and the marketplace, identify benefits and likely harms, and, if harms do

arise, consider whether existing laws and regulations are sufficient to address them, before assuming that new rules are required.

For the FTC, I believe we can help ensure that the promise of innovations, like the Internet of Things, is realized by using our unique set of policy and enforcement tools. First and foremost, in a new technology or industry that is rapidly innovating, we should use our policy R&D function to get a better understanding of the technology itself; the new business models it may enable; any existing regulatory 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 the specific issues—data security, mobile privacy, big data, and net neutrality—that have the most 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. A recent FTC case exemplifies the kinds of data security risks that the Internet of Things may present. Last month, the FTC settled a case against TRENDnet, which sold its Internet-connected SecurView cameras for purposes ranging from home security to baby monitoring.[2] 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.

Our complaint alleged that TRENDnet failed to use reasonable security to design and test its software, including the setting for the cameras' password requirement. Our settlement prohibits TRENDnet from misrepresenting the security of its cameras or the security, privacy, confidentiality, or integrity of the information that its cameras or other devices transmit. The company must also notify customers about the cameras' security flaws and tell them how to correct them. Finally, the company is required to establish a comprehensive information security program.

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 name while it is still in its infancy.

Although the Commission can and does challenge poor data security practices under the FTC Act, as it did in TRENDnet and almost 50 other cases, I believe that federal data security and breach notification legislation would also be beneficial to industry and consumers.

[2] Press Release, Fed. Trade Comm'n, Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy (Sep. 4, 2013), *available at* http://www.ftc.gov/opa/2013/09/trendnet.shtm.

Currently, 47 states have data security laws requiring consumer notification if personal information has been compromised. Although some of the laws are similar, they are not identical and companies thus need to ensure compliance with dozens of statutes and provide varying consumer notifications. A single standard would let companies know what to do and consumers know what to expect when a breach occurs.

Mobile

Mobile has also been a highly disruptive technology that has brought great benefits to consumers and opportunities to businesses. The growth in the use of mobile devices is astronomical. According to the International Telecommunication Union, the number of mobile subscribers globally rose from 5.4 billion in 2010 to 6.8 billion at the end of 2012.[3] 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 relay 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 and issued reports on a variety of issues including Mobile Privacy Disclosures, Mobile Cramming, and Mobile Apps for Kids.[4] Last June, the FTC hosted a public forum

[3] INTERNATIONAL TELECOMMUNICATION UNION, THE WORLD IN 2010: ICT FACTS AND FIGURES 1 (2010), *available at* http://www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf; INTERNATIONAL TELECOMMUNICATION UNION, THE WORLD IN 2013: ICT FACTS AND FIGURES 1 (2013), *available at* http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf.

[4] FED. TRADE COMM'N., MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY (Feb. 2013), *available at* http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf; *Mobile Cramming Roundtable*, FED. TRADE COMM'N., http://www.ftc.gov/video-library/index.php/ftc-events/mobile-cramming-roundtable-part-1/2365944702001.; FED. TRADE COMM'N., MOBILE APPS FOR KIDS: CURRENT PRIVACY DISCLOSURES ARE DISAPPOINTING (Feb. 2012), *available at* http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf.

entitled *Mobile Security: Potential Threats and Solutions*,[5] which brought together researchers, technologists, and industry participants from across the mobile ecosystem to discuss a variety of mobile security issues, including the threat posed by the rise of mobile malware. We have also issued reports, conducted research, and developed extensive consumer and business education materials.

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.[6] 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 personal information about users, and prudence suggests that such technologies should include some way to notify users and obtain their permission.

Big Data

According to some reports, ninety percent of the world's data has been generated over the past two years.[7] The amount of data in the world will only continue to increase with the volume and detail of information collected by new technologies, including the Internet of Things.

---

[5] *Mobile Security: Potential Threats and Solutions*, FED. TRADE COMM'N., http://www.ftc.gov/video-library/index.php/ftc-events/workshops/2013/mobile-security:-potential-threats-and-solutions-part-1/2436785714001; Press Release, Fed. Trade Com'n, FTC Announces Agenda, Panelists for Upcoming Mobile Security Forum (May 24, 2013), *available at* http://ftc.gov/opa/2013/05/mobilethreats.shtm.

[6] Press Release, Fed. Trade Comm'n, Path Social Networking App Settles FTC Charges it Deceived Consumers and Improperly Collected Personal Information from Users' Mobile Address Books (Feb. 1, 2013), *available at* http://www.ftc.gov/opa/2013/02/path.shtm.

[7] *Big Data, for Better or Worse: 90% of World's Data Generated Over Last Two Years*, SCIENCE DAILY (May 22, 2013), *available at* http://www.sciencedaily.com/releases/2013/05/130522085217.htm.

Although the ability to collect and analyze large data sets offers benefits in medical, scientific, economic, and other types of knowledge and research, as well as for business innovation, at the same time, the collection of large amounts of data about individual consumers may also raise privacy concerns. 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. 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.

Net Neutrality

Another issue with implications for the evolution of the Internet of Things is the debate over how to regulate the flow of information on the Internet. Some market participants, mainly content providers, want the government to impose network neutrality rules on the owners of the Internet's physical infrastructure and require them to treat all users and all transmissions alike. They think such unfettered access to the network is a key driver of the Internet's continued success, as it allows content providers to find their market and the market to find content providers without interference. Network owners disagree and think such regulations are unnecessary and could stifle innovation on the Internet. They believe the freedom to experiment with business models is what sparked the Internet revolution and point to examples, like AOL, where "walled garden" models that arguably could violate network neutrality principles have flourished and then receded based on natural market forces. The FCC has sided mainly with the content providers and issued network neutrality rules which have been challenged repeatedly by

network owners on multiple grounds – indeed, we are all waiting to see what the DC Circuit decides in *Verizon v. FCC*, which could bring some needed clarity to this area.

From my perspective, we do not need another layer of regulations here. Forcing network owners to treat all users essentially alike, whether they are buying comic books on eBay or exchanging life-saving health services information, in the face of a dynamic and robust online environment would contradict my understanding of good government and could impede development of the Internet, including the Internet of Things. The free market should decide how to distribute network resources, just as in any other industry. The government should instead focus on informed, flexible, and fact-based enforcement of existing competition and consumer protection laws, supplemented with private self-regulation of technical standards through consensus-based multi-stakeholder organizations of engineers, consumers, and businesspeople. To the extent the government is involved, the FTC model of enforcement, advocacy, and industry education is the better model that will allow free markets and innovative technologies the breathing room they need to prosper. At least five different trends are reshaping network access and in the process undermining the possibility of significant bottlenecks, leading me to be skeptical about any regulations that would deviate from the free market deciding how to allocate network resources among content providers. Each of these trends cuts against the need for network neutrality rules and supports the idea that the free market should be left alone, subject to existing competition and consumer protection laws.

First, growth in mobile broadband is now outpacing all other modes of access and is becoming the default means by which people interact with the Internet, especially outside the United States. Wireless networks are competing fiercely against the legacy wireline and cable last mile systems.

Second, backbone facilities and regional networks have established numerous additional interconnection points, altering the old three-tiered Internet hierarchy and creating further redundancy in the system. Regional networks now engage in secondary peering and multihoming, by which they can route their traffic directly either to another regional network, avoiding the national backbone altogether, or directly to another node on the national backbone. These relationships allow for more efficient use of the Internet and mitigate concerns over concentration of market power in termination monopolies or other bottleneck providers.

Third, new network technologies are enabling content providers to exercise greater control over delivery, both long-distance and at the last mile. For example, more content and applications companies are turning to new content delivery networks (CDNs), which connect content providers with local caches near last mile networks, reducing the use of long-distance networks and mitigating the possibility of hold-up. Content providers also are constructing or renting server space around the country and entering peering relationships as part of private networks to minimize use of the backbone and to save on transit costs.

Fourth, Internet capacity continues to grow at roughly 50% per year. An FCC study showed that supply has been roughly matching demand, with internet access performance improving each year—wireline ISPs last year averaged 96 percent of advertised download speeds during peak usage periods and speeds are getting faster.[8] From 2011 to 2012, the same FCC study showed that the experienced speed for users in the United States increased 38%.

However, although better speed and service during peak periods point to successful competition, the Internet of Things will add to growing consumer demand as perhaps billions of devices are connected and communicating. This steep expansion of demand, along with the

[8] FCC, MEASURING BROADBAND AMERICA: A REPORT ON CONSUMER WIRELINE BROADBAND PERFORMANCE IN THE U.S. (July 2012), *available at* http://transition.fcc.gov/cgb/measuringbroadbandreport/2012/Measuring-Broadband-America.pdf.

Internet's interconnected architecture and the physical limits of our spectrum and other transmission resources, means congestion management likely will remain an issue for years to come.

As in any other industry, however, free-market price setting should be the default mechanism to allocate resources and incentivize development of congestion solutions. Tiered pricing or pricing flexibility for network operators helps sort out higher priority from lower priority uses of relatively scarce resources. Enforcing a one price, all-you-can-eat approach to network access will distort investment incentives and allow free-riding by heavy users. Even worse, it could also interfere with the prioritization of traffic for Internet-connected devices that provide crucial or time-sensitive monitoring and responses, which may hamper the development of these services and ultimately reduce consumer benefits from the Internet of Things

Fifth, private parties have developed sophisticated and increasingly global multistakeholder organizations (MSOs) to help govern the Internet. Although these organizations are not perfect, they have successfully managed the Internet's complex and thorny problems with bottom up, consensus-based decision making of the most interested and arguably best-situated parties – engineers and businesspeople. The important point about MSOs is that they help mitigate the possibility of concentrated market power with their broad participation, consensus-based organizational structures, and adherence to principles like openness, transparency, and accountability.

There have been relatively few disputes about vertical foreclosure on the Internet, which tells me that the design characteristics and changes to the network's structure, along with increasing use of MSOs, together tend to mitigate the possibility of consumer harm or durable market power. Certainly, we need to be vigilant about vertical restraints and foreclosure, but the limited number of known transgressions to date strongly suggests an enforcement approach

would be more appropriate, and less invasive, than new regulations. We should continue to focus on encouraging businesses to expand network capacity and abide by our existing antitrust and consumer protection laws. We should also think twice before fundamentally changing something that appears to be working so well for so many.

Conclusion

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, offers 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. I am happy to take questions.