MEMORANDUM

TO: ESPC

FROM: D. Reed Freeman Jr.

Libby Greismann

DATE: November 20, 2013 FILE: 68223-0000001

RE: FTC Workshop: The Internet of Things -- Privacy and Security in a Connected World

---

We write to provide you with a summary of the Federal Trade Commission ("FTC" or "Commission") workshop entitled "Internet of Things: Privacy and Security in a Connected World" held November 19, 2013.

The "internet of things" refers to a world in which machines can communicate with each other via the internet without human intervention. The FTC indicated in May 2013 that it would hold this workshop to explore **the privacy implications of this rapidly emerging business model** and how these implications weigh against possible societal benefits of the technology.

The workshop consisted of a presentation on the technological landscape of the internet of things, remarks on contextual privacy, a keynote address from Vint Cerf, Vice President and Chief Internet Evangelist at Google, and four panel discussions. FTC staff moderated the panel discussions. Panel members consisted of industry representatives, private advocacy groups, and academics.

EXECUTIVE SUMMARY

In her introductory remarks, **Chairwoman Ramirez**:

- Identified ***three main challenges to consumer privacy*** presented by internet-connected devices:
  - Ability to collect **vastly greater amounts of data** that, when patched together, may present a full profile of our health, preferences, and identity;
  - **Unexpected uses of data**; and
  - **Data at great risk**, as devices connected to the internet are subject to hacking.

In remarks prefacing the afternoon sessions, **Commissioner Ohlhausen** (a Republican):

- Emphasized balancing efficiencies and benefits with protecting consumer privacy; and
- Stated that the FTC's approach will be to conduct policy R&D, educate consumers, and challenge any harms that do arise with traditional enforcement approaches.

In closing remarks, director of the **FTC's Bureau of Consumer Protection Jessica Rich**:

- Noted that the next step for the FTC will be to issue a report about best practices; and
- Invited public comments through January 14th, 2014.

These were the only substantive pronouncements by the FTC at the workshop. However, questions asked by FTC staff moderators suggested they think the internet of things presents unique privacy and security threats that must be balanced against possible great societal benefits, and that traditional notice and consent frameworks will not be sufficient to inform consumers of how their personal data is being used. No questions were answered by FTC staff.

In all four discussions, panelists disagreed over:

- ***Whether harms outweigh benefits in connecting devices to the internet***
  - Industry representatives suggested that the benefit potential was huge, while privacy advocacy groups tended to weigh the harms more heavily.
- ***The degree of sensitivity of data that would be collected from these devices***
  - Should consumers care about data collected in the aggregate and anonymously?
  - Should consumers worry about "harmless" data points such as energy consumption or fitness metrics?

However, there was general agreement that:

- ***Consumers and vendors do not understand the implications*** of the data-collecting devices they are using.
- Internet of things ***policies should be technology-neutral***.
- ***Transparency and consumer empowerment is key, as is implementing a "privacy by design" framework*** into connected devices.

PRESENTATION: WHAT IS THE "INTERNET OF THINGS?"

Keith Marzullo of the National Science Foundation began the workshop with a technical framing of the internet of things. Mr. Marzullo explained the three main categories of internet of things technology:

- ***item identification based on RFID***
- ***sensors applied to inert machines or objects***
- ***embedded intelligence***

PRESENTATION: TRUST AND CONTEXT IN A CONNECTED WORLD

Carolyn Nguyen of Microsoft spoke about the impact of the internet of things on the individual, specifically how it can assist individuals in making optimized and context-appropriate decisions. She emphasized that:

- For data driven ecosystems to be sustainable, the ***ecosystem must show that it is capable of earning individuals' trust.***
- This trust is gained by using data only for ***context-specific purposes where consumers gain the most value***

PANEL 1: THE SMART HOME

This panel examined both the benefits of the increased connectivity of products and services for the home as well as the various associated privacy and security concerns. The panel also focused on what products are available, including smart meters for energy usage, smart appliances, and connected monitoring devices.

Panelists were divided over the weight of the benefits conferred by the "smart home"

- Mike Beyerle of GE and Jeff Hagins of SmartThings believe that the smart home can provide significant convenience and value to the consumer.
- Lee Tien of the Electronic Frontier Foundation and Craig Heffner of Tactical Network Solutions were more skeptical, and were concerned about the vast amounts of data being collected about individuals' personal lives.
    - Mr. Tien voiced concern over the fact that consumers are either unaware of real privacy issues, or have tendency to underestimate what can be done with this "humdrum" data.

While panelists agreed that privacy and security risks are present, they pointed to different sources of these risks

- Craig Heffner pointed to the lack of financial incentives to make devices secure, and the fact that companies are cutting costs and hiring lower quality engineers
- Jeff Hagins noted that companies don't have all the skill sets they need to address security from top to bottom.

PRESENTATION: KEYNOTE SPEAKER VINT CERF

Vint Cerf of Google gave a general overview of the internet of things environment, including the global implications, challenges and opportunities presented by this evolution. Mr. Cerf noted that:

- There is ***huge potential for global optimization of resource management***, as well as ***potential health management, wellness, and educational improvements.***
- Industry ***must continue to innovate*** on a global scale, while respecting privacy.

PANEL 2: CONNECTED HEALTH AND FITNESS

This panel examined both the benefits of the connected health and fitness devices and apps, as well as the various associated privacy and security concerns. The panel also focused on what products are available today or will soon be available, including glucose pumps for diabetics, FitBits (fitness monitoring wearable devices), and connected pillboxes.

Panelists agreed that the data collected by these devices and apps is rich and highly personal

- Scott Peppet of the University of Colorado School of Law explained that the data coming off sensors is extremely high quality and can create a rich picture of the individual's personal lifestyle.
- Stan Crosley of Indiana University agreed, and emphasized that far more information about health is generated outside the walls of traditional healthcare today than within them.

Panelists also agreed that traditional user notice and consent methods are highly unlikely to be effective

- Joseph Lorenzo Hall of the Center for Democracy and Technology stated that there is no practical way to have a consumer consent every time a device records something, as the device would simply not be practically useful.
- Jay Radcliffe of InGuardians, Inc suggested the industry come up with a new way to obtain consent, as nobody actually reads written privacy policies or manuals
- Scott Peppet stated that privacy policies leave important things out.

Each panelist also provided his top security concern that doctors and consumers should be aware of as they decide whether to use these devices

- Panelists were concerned about lack of encryption, lack of consumer understanding of importance of security, and potentially unreliable data.

PANEL 3: CONNECTED CARS

This panel examined the emergence of smart cars and various integrated consumer-facing technologies, and the associated privacy and security concerns. Panelists focused on

concerns related to data collection and existing vulnerabilities in the systems, including OnStar, remote access devices, and Event Data Recorders ("black boxes").

Panelists first discussed the benefits from connected cars

- Christopher Wolf, of the Future of Privacy Forum, named a host of benefits including:
  - Car can call first responders if driver is in accident, car can alert driver to hazardous road conditions or malfunctions, parents can track children's driving habits, etc.

Panelists focused on differences between automobile industry and other connected industries

- Mr. Wolf explained that consumers are eager to see certain capabilities brought inside automobiles such as maps and personalized settings.
- Yoshi Kohno, of the University of Washington, noted that in the auto industry, unlike other industries, manufacturers are very aware and focused on security and privacy issues related to these technologies.
- Wayne Powell, of the Toyota Technical Center, emphasized that the fact that the car is physically moving down the road makes it a riskier environment if systems are hacked, as well as a challenge to provide consumers with data in a safe way.

Moderator Karen Jagielski, of the FTC's Division of Privacy and Identity Protection, was particularly interested in the unique issues as to long-lasting ownership, and multiple owners, of automobiles.

- Most panelists were not concerned.
- Mr. Powell explained that when a car is sold to an individual, all off-board data from previous owner is gone as soon as accounts are closed, and cannot be retrieved.
- Mr. Nielsen also clarified that data derived for maintenance is collected only in the aggregate, and times out after 40 seconds.

PANEL 4: PRIVACY AND SECURITY IN A CONNECTED WORLD

In this panel, the moderators presented the panelists with four scenarios and asked them to discuss broader privacy and security issues raised by the internet of things, including best practices for managing privacy and security with new interconnected devices, and the incentives for designing products with privacy and security in mind.

Scenario 1: At what point should small businesses begin to think about privacy?

- Panelists agreed that privacy should be considered as **soon as the concept for the business is developed**

- Michelle Chibba, of the Office of the Information and Privacy Commissioner of Ontario, suggested that small startups without IT infrastructure should collaborate and consult with other companies. She also supported data minimization as a way to promote security from the outset.

Scenario 2: Do connected devices put consumers on notice that companies will collect private data?

- Panelists agreed that **traditional notice and choice mechanisms are no longer sufficient** for data collected from connected devices
  - Professor Calo emphasized the need to innovate around notice just as we do with other things in the industry
    - He also expressed concern over the "bait and switch" scenario, where companies do not give consumers full disclosure regarding the monetization of their data
  - Drew Hickerson of Happtique and Dan Caprio of McKenna Long & Aldridge both saw a need for creation of some kind of standardization so that consumer know a product is trustworthy
    - Suggested a seal of approval

Scenario 3: What should vendors do when their connected device is breached?

- Panelists generally agreed again that **security and breach protocol should have been built into the design**
- There was slight disagreement over appropriate actions to take
  - Ms. Chibba suggested that the company shut down the system immediately
  - Mr. Rogers countered with the fact that shutting down the system is not often safest for the consumer – for example, an internet-connected lock in a door should not be shut down to lock the consumer out or to unlock completely

Scenario 4: If you were the FTC, what would you do next?

- Panelists focused on **education and research before regulation or legislation**
  - Mr. Jacobs believed that enforcement was appropriate, and the FTC is off to a good start with the TRENDnet investigation
  - Mr. Hickerson suggested that we continue to educate consumers and the industry and create partnerships with the industry as well as other agencies to avoid duplicative rulings
  - Ms. Chibba noted that the privacy by design framework is successful in Canada and could be in the United States as well