KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 Eye Street, NW
Suite 1100
Washington, DC 20006

June 1, 2013

Federal Trade Commission
600 Pennsylvania Avenue N.W.
Room H-113 (Annex B)
Washington, DC 20580

Re: Comments for November 2013 Workshop on the "Internet of Things"

The Center for Democracy & Technology[1] (CDT) is pleased to submit comments in response to the Federal Trade Commission's (FTC) call for submissions[2] on the privacy and security aspects of the Internet of Things in advance of the FTC's November 21, 2013 workshop. We focus our comments narrowly to discuss the kinds of issues we suggest the FTC explicitly include for discussion at the November workshop as well as recommendations for speakers the FTC may wish to invite to the workshop in order to further inform that discussion.

I. Introduction

The Internet of Things (IoT) as articulated in the FTC's call for submissions refers to the increasing integration of Internet connectivity into consumer devices such as home appliances, electricity meters, and medical devices.[3] The development and deployment of such devices will create many new opportunities for consumers and companies to create and analyze data regarding the use of technology, especially in highly localized, private environments such as work and home.

As companies and regulators consider the effects that Internet-enabled devices will have on the consumer landscape, addressing privacy and security issues will be crucial. Because of the sensitivity of data that home appliances, medical devices, and other Internet-enabled technologies can collect and transmit, embedding strong, responsive, and flexible privacy and security paradigms and mechanisms from the outset of product research and development will be crucial.

---

[1] CDT is a non-profit Internet and technology advocacy organization working to keep the Internet and digital life open, free, and innovative. CDT promotes public policies that preserve privacy, promote innovation, and enhance civil liberties in the digital age.

[2] "Press Release: FTC Seeks Input on Privacy and Security Implications of the Internet of Things", Federal Trade Commission, (April 27, 3013), *available at:* http://www.ftc.gov/opa/2013/04/internetthings.shtm.

[3] However, see Section II.A for comments on the definition of IoT as articulated by the FTC.

CDT has previously advocated for strong privacy and security practices, based on the Fair Information Principles, in its comments to NIST regarding the development of smart grid technology.[4] Due to the similarities between smart grid technology and the possibilities of Internet-enabled technologies, we feel that similar questions raised by the smart grid discussions will be raised in the context of the Internet of Things. Those issues include proper protections of personally identifiable information; retention and use limitations on the data collected by such devices; and the development of robust security practices to prevent unwanted third parties from accessing consumer data.

Despite the promise created by new technologies that enable consumers to create and monitor their usage of personal devices, CDT does not feel that the questions and issues raised by such technologies are altogether new ones. Though the applications may be new, the fundamental questions of how to protect consumer privacy and security are longstanding issues. To that end, we encourage the FTC to take a balanced approach in regulating such devices by recognizing that privacy and security protections must both protect users and encourage innovation in this promising area.

The remainder of this comment discusses the kinds of sessions we feel would be valuable at the November workshop and some thoughts towards potential panelists and speakers the FTC may wish to invite.

II. Salient Issues in the Internet of Things

In this section we describe three specific areas that would be fruitful areas for further discussion at the November workshop: disambiguating the Internet of Things, important privacy issues, and important security issues.

A. Disambiguating the Internet of Things

In the FTC's call for submissions,[5] the Internet of Things is defined as, "the ability of everyday devices to communicate with each other and with people". This is a very thing-oriented and object-oriented framing of a broader issue involving how people interact with environments that are increasingly filled with computerized and networked devices, sensors and other objects. There are number of important related concepts, such as "ubiquitous computing", "pervasive computing", and "ambient intelligence", each of which share common features with IoT. The FTC may find it helpful and useful in the coming inquiry to focus on the aspects of these areas with which it is most concerned in terms of balancing privacy, security, and innovation. In this section, we discuss the overlap of these various perspectives.

---

[4] "Comments on Draft NIST Interagency Report (NISTIR) 7628, Smart Grid Cyber Security Strategy And Requirements," Center for Democracy & Technology, (December 1, 2009), *available at:* https://www.cdt.org/files/pdfs/CDT Comment NISTIR 7628 Draft 12-02-09 FINAL - updated.pdf.

[5] FTC Press Release, *supra*, fn. 2.

A recent article, aiming to survey definitions of IoT, acknowledged that there was no agreed-upon definition of the term, and identified the following definition as the best one available, because of its broadness and descriptiveness: "The Internet of Things allows people and things to be connected Anytime, Anyplace, with Anything and Anyone, ideally using Any path/network and Any service."[6] Of course, this is significantly different than the FTC's articulation in the call for submissions.

What all definitions of IoT have in common is that they focus on how computers, sensors, and objects interact with one another and process data. Ambient intelligence and ubiquitous (or pervasive) computing[7] are concepts related to IoT. But instead of taking as their reference point how objects interact, ambient intelligence and ubiquitous computing describe how humans interact with IoT. Ambient intelligence and ubiquitous computing aim to describe the nature of user experience.

Ambient intelligence and ubiquitous computing present alternative visions of how humans will interact with and control the computers and sensors in their environment once the Internet of Things takes root among non-corporate consumers. The two mechanisms of engagement are probably not mutually exclusive. As McKinsey's analyses of IoT illustrates, where a responsive system of computers and sensors is not integrated into the personal life of humans, IoT can be discussed without reference to ambient intelligence or ubiquitous computing.[8] This is because, unlike IoT, ambient intelligence and ubiquitous computing are visions of personal user experience.

CDT believes that the FTC should not just be concerned with IoT via objects and things that consumers purchase but also must take into consideration the forces that work to make consumers' surrounding environments *frictionless* in terms of data collection and use. For example, without notice, feedback, and technical configurability from a privacy and security perspective, consumers may not feel comfortable with environments saturated by IoT.

---

[6] Charith Perera, Arkady Zaslavsky, Peter Christen, and Dimitrios Georgakopoulos, "Context Aware Computing for The Internet of Things: A Survey," *IEEE Communications Surveys & Tutorials Journal*, 1–44 (2013) (forthcoming), *preprint available at:* http://arxiv.org/abs/1305.0982 (last accessed 30 May 2013).

[7] Here, we addresses ubiquitous computing and pervasive computing together, calling it ubiquitous computing. In the past, "ubiquitous computing" was associated more with what we understand today as "mobile computing" and "pervasive computing" was more about frictionless user experience in the face of interoperability and seamless functionality between arbitrary networked devices. For a helpful discussion, *see*: Emile Aarts and Boris de Ruyter, "New research perspectives on Ambient Intelligence," *Journal of Ambient Intelligence & Smart Environments*, **1**:5, 5–7 (2009), *available at:* http://boris.borderit.com/docs/JAISE.pdf.

[8] James Manyika, Michael Chui, Jacques Bughin, Richard Dobbs, Peter Bisson, and Alex Marrs, "Disruptive technologies: Advances that will transform life, business, and the global economy," McKinsey Global Institute, 52–61 (2013), *available at:* http://www.mckinsey.com/insights/business_technology/disruptive_technologies (last accessed May 30, 2013).

In this respect, it may be helpful to have an initial session at November's workshop that asks what pieces of this ecosystem — IoT, ubiquitous computing, ambient intelligence — various stakeholders believe the FTC should monitor and/or actively engage with.

B. Privacy Issues

In many respects, IoT will facilitate intensive data collection and usage, despite that consumers are only just now starting to become aware of these activities on the Internet and World Wide Web. Familiar and controversial tracking and behavioral profiling issues may be embedded into IoT, potentially in combination with other data sources such as online behavioral data. Simply put, when a consumer five years from now buys a carton of milk, they may not expect or otherwise know that the carton will report back to the manufacturer (and/or distributor) information such as, for example: usage frequency information (e.g., each time the consumer opens the carton, how long it is kept open), manner of use information (e.g., if the consumer drinks directly from the carton; if the consumer uses it as a doorstop instead of a foodstuff), and/or environmental data (e.g., the temperature a consumer stores their milk at; details about other kinds of products in the consumer's refrigerator). Just as in the case of Do Not Track and web browsing, CDT feels that the proper balance between the public interest in privacy and in innovation lies in effective mechanisms for consumer control and notice of collection and use of data that consumers believe are privacy invasive.

Much of the discussion surrounding IoT, ubiquitous computing and ambient intelligence contemplates directly inserting networkable computing components and sensors into the home and workplace, contexts that enjoy heightened expectations of privacy and heightened barriers to access under the 4th amendment for government search and seizure (as well as other state and common law protection).

There may be technological solutions to these barrier-crossing issues that consumers can configure to control the amount and nature of data transmitted by IoT-capable sensors and devices in sensitive locations. For example, it may be possible to design "middleware" networking equipment[9] that a member of the household or business could configure to selectively allow or disallow networked objects from communicating outside of the household network. Ideally, such a privacy appliance could easily identify data emitted by IoT-capable products in the home network, but that relies on manufacturers inserting the right tags into their network communication that such an appliance could read. This would probably require significant standards work and manufacturer buy-in (or a legislative or regulatory mandate) to support this kind of functionality. Another option may be to design a standard element to the networkable components of IoT objects — say a pull-off tab or shielding element — that consumers can activate in order to toggle or disable networking functionality. Given that certain

[9] For example, a network appliance — a small, networking-specific computer — that attaches to the network cable from the internal network to a network switch, cable/DSL modem, etc.

activities and areas in one's home are particularly sensitive towards arbitrary data collection — bedrooms, bathrooms, children's areas — there may be a level of tracking and data usage that above which is simply not appropriate for those products or that industry commits to making connected and disconnected versions.

At the November workshop, we suggest FTC include discussion from both academic and industry perspectives of how privacy controls and responsiveness in areas such as IoT and ubiquitous computing have evolved and prospects for the near future.

C. Security Issues

For IoT objects that include more sophisticated programmable components, there undoubtedly will be security flaws in their design and implementation. That is, computer science has not yet figured out a way to write software that is without flaws, and there will need to be mechanisms to update, freeze, isolate, or disable such components. Ideally, manufacturers will support and update components for the shelf life of the product, but for some more durable or non-perishable products, this will be difficult (the patchwork of Android mobile operating system security updates is instructive[10]). Accordingly, CDT recommends that FTC include a discussion of the feasibility of the following alternatives (the first two are not mutually exclusive):

- Freeze: Perhaps IoT objects can be frozen in a state that makes further software updates impossible. This would allow continued network interactions with the object but would not allow any malicious software updates that might later modify functionality to an undesired state.

- Isolate: Perhaps IoT objects can be isolated from the outside network. This would allow continued networked interaction on the home/business network but no connections to or from the larger outside Internet.

- Disable: Finally, if the software and network functionality of a given device is not fundamental to the functionality or operation of that device, perhaps this functionality could be entirely disabled by the consumer. This would mean that the software and networking ability that makes a given device a participant in the Internet of Things would be entirely disabled; essentially taking the Internet out of the Internet of Things.

Finally, a somewhat technical issue that the FTC may want to discuss and address in the November workshop is that of *composable security*. That is, when devices designed in isolation to be secure are brought together and used in a combined or composed system, the original security assurances often do not

[10] Craig Timberg, "'Fragmentation' leaves Android phones vulnerable to hackers, scammers," The Washington Post, (February 6, 2013), *available at:* http://articles.washingtonpost.com/2013-02-06/business/36942653_1_android-phones-android-ecosystem-android-devices.

apply to the larger system.[11] As the precise purpose of IoT is to assemble vast quantities of sensors and devices into composed systems, it is hard to imagine the resulting system being as secure as the individual pieces. This is a particularly hard problem in computer science and has been an area of active research for over three decades. CDT has no particular advice here other than to encourage the FTC to discuss this at the November workshop as part of the security discussion.

III. Some Suggested Panelists/Speakers

We have a few suggestions for possible speakers and panelists that the FTC may wish to invite to the November workshop. Below, we list some names of individuals that have been involved in or hold significant expertise in IoT, privacy, and security.

Experts in Internet of Things and ubiquitous computing:

- Marco Castillo (Responsys);
- Adam Greenfield (Urbanscale);
- Usman Haque (Haque Design + Research);
- Trevor Harwood (Postscapes.com);
- Laura James (Open Knowledge Foundation, Makespace)

Experts in privacy issues related to Internet of Things:

- Justin Brookman (CDT);
- L Jean Camp (Indiana University);
- John Canny (UC Berkeley);
- Peter Swire (Georgia Tech)

Experts in security issues related to Internet of Things:

- William Arbaugh (University of Maryland);
- Urs Hengartner (University of Waterloo);
- Peter G. Neumann (SRI International);

[11] "it is possible to connect two systems, both of which are judged to be secure, such that the composite system is not secure.**"** Daryl McCullough, "Noninterference and the composability of security properties," *Proceedings of the 1988 IEEE Symposium on Security and Privacy*, (1988), 177–186, *available at:* http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8110&isnumber=427.

Thank you for the opportunity to submit comments and please do not hesitate to contact us with further questions.

Sincerely,

/s/

Joseph Lorenzo Hall
Senior Staff Technologist; CDT

/s/

G.S. Hans
Plesser Fellow; CDT

/s/

Lauren Henry
Intern; CDT