Before the U.S. Federal Trade Commission

In the Matter of the Internet of Things	)
	)
FTC Project No. P135405	)
	)
	)
	)
	)

Comments of the Information Technology Industry Council

January 9, 2014

I. Introduction

The Information Technology Industry Council (ITI) appreciates this opportunity to provide comments to the Federal Trade Commission ("FTC") relating to the agency's examination of the privacy and security issues posed by the Internet of Things. ITI is the premier voice, advocate, and thought leader in the United States for the information and communications technology (ICT) industry. ITI's members comprise the world's leading technology companies.

ITI commends the Commission for convening a workshop on the Internet of Things (the "Workshop") in November 2013.[1] As Chairwoman Ramirez stated in her opening remarks, the Internet of Things can enable us to "track our health, help us remotely monitor an aging family member, reduce our monthly utility bills, and alert us that we are out of milk."[2]

The Chairwoman further noted the estimated 3.5 billion sensors that already continuously transmit data in real time as part of a ubiquitous network.[3] She also commented that some experts predict that number to increase to the trillions within the next decade, and

---

[1] FTC Workshop, *Internet of Things – Privacy and Security in a Connected World* (November 19, 2013), http://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-and-security-connected-world.

[2] *See* Workshop transcript, (available at http://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf), remarks of Chairwoman Ramirez, FTC, at 7.

[3] *See* Workshop transcript, remarks of Chairwoman Ramirez, FTC at 7.

that it is "still early when it comes to the Internet of Things."[4] The Chairwoman pointed out that the Internet of Things is "poised to transform manufacturing, business, and agriculture" and highlighted that the potential in these areas can be realized without collecting information about individuals.

Because not all Internet of Things capabilities will implicate privacy and security-related concerns, ITI urges the FTC to begin its analysis by determining the circumstances that in fact raise privacy and security issues. For example, the FTC should consider whether data that is de-identified or aggregated raises the same privacy concerns as other types of data.

Because the Internet of Things is in its early days, we further urge the FTC to move deliberately and thoughtfully to allow stakeholders and policymakers to develop a greater understanding of the capabilities being created by the Internet of Things. We encourage the FTC not to immediately develop guidance, but rather continue the conversation among policymakers, academics, industry, and other stakeholders. We believe the FTC should convene additional workshops to gather additional information and deepen the public's understanding of the Internet of Things. Issuing guidance in this area prematurely could compromise the Internet of Things' dynamic growth, capacity for innovation, and potential to deliver benefits for individuals, commerce, research, and education. We urge the FTC in its examination of the Internet of Things to consider that guidance about the collection, use, and processing of data – whether in the commercial sector or otherwise – should be flexible. Such flexibility will make it possible to realize the promise of the Internet of Things. Data collected through inter-connected devices enable companies, academics, and government to address problems in ways that were previously not feasible. As pointed out by Vint Cerf at the Workshop, the ability of a city to monitor traffic data (whether such data is collected directly by the city or by the commercial sector) can benefit consumers tremendously.[5] It is the collection of that data that would enable consumers to adjust their routes based on patterns that they can be

[4] *See* Workshop transcript, remarks of Chairwoman Ramirez, FTC at 7.

[5] *See* Workshop transcript, remarks of Vint Cert, at 135-136 ("a city that is able to monitor what is going on in the city, with traffic flow being an obvious example of that, could make quite a big difference for people trying to select which routes to take").

made aware of in real time. The collection of data for such beneficial uses is necessary, and should not be stifled by restrictive requirements.

II. Existing Rules and Flexibility

The Internet of Things incorporates technologies that collect a wide variety of data, much of which is already subject to existing laws, including laws that impose privacy requirements.[6] If the maximum benefit is to be derived from the Internet of Things, any new guidance the agency may issue should not add additional layers of regulation or requirements that burden the technology and data ecosystem and do little to enhance the privacy of individuals.

Any guidance should hone in on instances where privacy and security issues in fact are implicated and raise the risk of consumer harm – such as cases where personally identifiable information is not adequately secured. The FTC's recent announcement that it settled charges against TRENDnet, Inc., the company that markets video cameras designed to allow consumers to monitor their homes remotely, provides an example of a circumstance where privacy and security are implicated and where consumer harm can result.[7] In this case, the company's failure to utilize reasonable security measures led to, among other issues, transmission of live feeds from consumers' homes on the Internet. We commend the FTC for this enforcement action, as it focuses on the harm that can result when interconnected devices and the data associated with them are not sufficiently secured.

Additionally, any guidance offered by the agency must be flexible. The complex technologies, networks, and data sharing that fuel the Internet of Things could in some cases render the application of traditional notions of the Fair Information Practice Principles (FIPPs) impractical. While in certain situations, the full gamut of FIPPs protections may be applied to a positive effect, in others, implementation of the FIPPS may be unworkable or may need to be adapted to the Internet of Things environment.

---

[6] For example, in sectors such as health and financial, there are existing laws that impose privacy requirements. In addition, the FTC's existing authority under Section 5 of the Federal Trade Commission Act reaches unfair or deceptive practices in connection with Internet of Things technologies.

[7] *See In the Matter of TRENDnet, Inc.* FTC File No. 122 3090 (September 11, 2013) (proposed consent order), *available at* http://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles

The Internet of Things often involves networks of wired and wireless communications technologies embedded in physical objects we carry, the vehicles we travel in, the buildings in which we live, work, and visit, and even the streets and public places where we travel. The Internet of Things will rely on geo-location technology, sensors, RFID, and many other technologies in development or that have yet to be invented. To derive maximum benefits, it will be necessary to retain data for longer periods and share it in new ways. Many of these aspects of the Internet of Things are not anticipated by our traditional notions of how FIPPs protections are applied. Therefore, flexibility is necessary to enable the Internet of Things to continue to evolve and to provide tremendous benefits to society and individual consumers.

III. Conclusion

ITI appreciates the opportunity to submit these comments to the FTC. If you have any questions about these comments, please contact Yael Weinman, VP, Global Privacy Policy and General Counsel, Information Technology Industry Council, at 202-626-5751, yweinman@itic.org.