Filed on behalf of Transatlantic Computing Continuum Policy Alliance [1]

Introduction

We appreciate the opportunity to comment and appreciate the interest of the Federal Trade Commission (FTC) in holding a workshop on the Internet of Things (IoT).

The IoT must be considered as a continuum of Internet connectivity, smart objects and applications complemented by the elements of the Cloud as both IoT and Cloud *are not distinct but rather interrelated technologies that will use the Internet as a communication platform.*[2]

Things and people will all be part of our future Internet connectivity. The IoT or machine to machine (M2M) communications has the potential to bring about many societal benefits like smart cities, smart grids, and smart health care and is an integrated aspect of the single Internet rather than a "parallel Internet." The potential opportunities brought about by the IoT are vast including considerable societal, economic and environmental benefits. However, context is critical.

We hope the focus of the FTC IoT workshop will have three main goals:

1. Consider the opportunities and practical challenges of the IoT without getting mired in what is theoretically possible;

2. Address the common IoT perception that every device will be connected to the internet via its own unique IP address. While there are estimates that billions of devices will be connected to the internet by the end of 2020, [3] the business case does not support a scenario where every object an is connected to the Internet and it's likely that sensors will be mediated through a local area network or a console; and

[1] The Transatlantic Computing Continuum Policy Alliance is compromised of Intel Corporation, Oracle Corporation, and AT&T, Inc. and is represented by Dan Caprio, McKenna, Long & Aldridge, as a subject matter expert to the European Commission Expert Group on the Internet of Things established in 2010.

[2]" Internet of Things, Fusion of the Real and Virtual Worlds: Transatlantic Regulatory Efforts," Dan Caprio, Data Protection Law & Policy, April 2013, volume 10 ISSUE 104, available at www.e-comlaw.com,

[3] available at http://postscapes.com/infographic-cisco-internet-of-things

3. Move away from a discussion about collection with much more discussion about accountability and appropriate use avoiding a fine level of granularity.

We do believe a distinction does need to be made where PII is identifiable and where it’s not identifiable. Where PII is identifiable, it needs to be protected. There are bright line examples of where the IoT does not implicate PII so those distinctions need to be made as well.

The IoT is an evolutionary process since it magnifies existing privacy issues with the transformation of devices that are more connected and more powerful. As such, we hope the FTC will launch a conversation about the types of information that need to be protected and how that information can be protected/encrypted if necessary.

Broadly speaking, we are in the midst of a transition in technology with respect to privacy that strains the existing Fair Information Practice Principles (FIPPS). A question to be considered is how to manage notice and choice realizing its not working since the concept of individual control in a connected world puts the burden on individuals. We hope to have a broader discussion about how to alleviate the burden on individuals to protect themselves in an era when notice has been deemed insufficient.

An individual's applications and data will move as that person moves through his or her day. The person will wake to having data on a certain device in his or her home, will transition to a car that has access to those applications and data, will have access at work (which often will not be in a traditional office), and then will access the data and applications after work either at home or while socializing. To manage these applications and data, the individual will use a wide assortment of digital devices including servers, laptop computers, tablets, televisions, and handheld PCs.

The development of the computing continuum will have substantial benefits for consumers. One example illustrates this well. Soon, a Smartphone will be able to communicate with an individual's car. The GPS functions in both devices will "know" that the devices are in the same location and that they are traveling at the same speed; thus, they will know that a specific individual is driving with the phone in the car. If the driver gets a text message, the message would not be displayed on the phone. Instead, the speaker in the car can ask the driver whether he or she wants the car's computer to read the text message. When the phone leaves the car, the devices will communicate with each other and the phone can again display text messages directly on the device.

The development of the computing continuum also allows computing to become personalized and contextually aware. Devices across the continuum will combine "hard sensing" and "soft sensing" inputs. For instance, "hard sensing" inputs would know whether a user is sitting in front of a laptop (via the laptop camera), whether an individual is sitting, walking, or running (through an accelerometer), whether an individual is chatting, commuting, or listening to music (through a device microphone), whether an individual is outdoors or indoors or whether it is light or dark (through sensors on the device), and the individual's location (through GPS). "Soft sensing" inputs could pull information from an individual's calendars, social networking activity, browsing habits, personal preferences, and device activity. For a more complex interaction, a music player might determine that an individual is running, that it is the morning, and that the individual has been awake for at least 30 minutes. Based upon the user's preference for listening to music in the morning while running, the music player will automatically know the appropriate music to play. The aggregation of context over time and over devices will fundamentally change the way that consumers interact with their computing devices.

All of this innovation requires a policy environment in which individuals feel confident that their privacy interests are protected. Building a trusted environment in a systemic way not only benefits consumers and increases their trust in the use of technologies, but is vital to the sustained expansion of the Internet and future economic growth.

New regulation will invariably trail innovation of new technology. Technology neutrality also ensures that the regulatory environment does not favor an incumbent business model and can account for new business growth and innovation. Therefore, a focus on the application of principles -- neutral to the technology used -- enables a flexible, effective, and timely response.

Privacy and Data Protection

To unleash the global potential of the IoT, it is crucial to protect privacy and enable innovation to seize the countless opportunities that the IoT offers. Protecting privacy and enabling innovation are not mutually exclusive [4] and must consider principles of accountability and privacy by design. In order to translate the huge potential the IoT offers into concrete benefits for business and individuals

[4] Rob van Kranenburg, Dan Caprio et al., *The Internet of Things* (2011), p. 42 *available at* *http://berlinsymposium.org/sites/berlinsymposium.org/files/paper_iot-new_covertext.pdf* (paper prepared for the First Berlin Symposium on Internet and Society.

alike, we need to address the concerns that could hinder its uptake, or might slow down global innovation and competitiveness, such as narrow technology-specific regulations or mandates.

Since 2006, the Transatlantic Computing Continuum Computing Alliance has advocated for an interoperable, technology neutral, and horizontal privacy and data protection framework between Europe and the United States. To date, the European Commission has resisted separate regulation of the IoT. We hope the FTC will include an international panel since the FTC has a rich history of studying new technology with international partners with a view to protecting privacy and enabling innovation. Such an approach could continue to reinforce the need to avoid prescriptive new regulation of the IoT in Europe.

Moving beyond the scope and aims of the proposed European Data Protection regulation or section 5 of the FTC Act with IoT-focused policy regulation will not only be over-burdensome and confusing but also run the real risk of not keeping pace and becoming quickly outdated, given the evolving nature of technologies within this digital information society.

IoT technologies should be developed with a focus on ensuring the transparent collection and use of data. Individuals should have confidence that these representations are complete and reliable. Data collectors should make certain collected data will be protected with the same rigorous privacy principles applied to personal data collected from other sources. With this ideal in mind, both public and private organizations, should take privacy into account from the very start of all processes. A “one-size-fits-all” approach and a prescriptive model of a so-called “Privacy by Design” principle (PbD) should be avoided and will be unworkable. In addition, Privacy Impact Assessments (PIAs) are an important privacy enhancing tool to measure risk assessment and risk mitigation. Given the wide range of technologies used in IoT ecosystems, prescriptive rules on PIAs specific to IoT would not effectively protect data subjects.

Principles relating to personal data processing, namely proportionality and transparency, impose stringent conditions for the collection and processing of data. Proportionality in this context requires a balanced analysis of assessing risk and mitigating risk based upon the threat to privacy. The type of data collected will help to determine what “reasonable” and “appropriate” notification is.

Accountability through Privacy by Design

Regulators in multiple jurisdictions have called for more formalized and widespread adoption of the concept known as "Privacy by Design." Privacy by Design asserts that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must become an organization's default mode of operation.

Accountability is a well-established principle of data protection, having longstanding roots in many of the privacy and security components comprising global trust. Accountability requires an organization to make responsible, disciplined decisions regarding privacy and security. It shifts the focus from an obligation on the individual to have to understand complicated privacy notices to an organization's ability to demonstrate its capacity to achieve specified objectives. The accountable organization complies with applicable laws and then takes the further step of implementing a program ensuring the privacy and protection of data based on an assessment of risks to individuals. For example, companies can demonstrate accountability by innovating to build trust, such as by developing and selling more secure and privacy-enhancing component parts that have been vetted through processes such as development lifecycles that have privacy and security integrated as foundational elements.

Privacy by Design principle should encourage the implementation of accountability processes in the development of technologies and services. To achieve its objective, the principle should avoid mandatory compliance to detailed standards, or mandatory third party detailed product reviews, as this would decrease time to market and increase product costs. This would be particularly the case when it is unclear whether third parties would have the appropriate resources or skill sets to effectively review the technology. Instead, Privacy by Design accountability model should focus on making certain privacy is included as a foundational component of the product and service development process. We view Privacy by design as a necessary component of accountability mechanisms.

Need for Greater Consumer Education

We agree that strong consumer education is needed to better inform individuals about data practices and the IoT. The FTC conducted a highly successful education campaign to promote the National Do Not Call Registry, and we would encourage the Commission to conduct a similar effort on this issue. Moreover, we would call the Commission's attention to efforts surrounding Data Privacy Day, an annual international event to raise awareness and generate discussion about information privacy.

Over the past few years, privacy professionals, corporations, government officials and representatives, academics, and students in the United States, Canada, and 27 European countries have participated in a wide variety of privacy-focused events and educational initiatives in honor of Data Privacy Day. They have conducted discussions, examined materials and explored technologies in an effort to bring information privacy into our daily thoughts, conversations and actions. We would encourage greater U.S. government involvement in this event in order to raise privacy awareness and specifically encourage the government to partner with non-profits and industry to develop similar programs.

Security

Security is another key component in IoT development and deployment as end-user trust in devices is critical, particularly in terms of any new technology or innovation. This trust requirement becomes ever more evident with increasing levels of data and information (both personal and non-personal) being exchanged via various methods. While industry always works to mitigate risks, it always remains a possibility that the security or integrity of devices and personal data (in particular data in transit) could be compromised in one form or another. For its part, to help mitigate such risk, industry should work on further implementation of appropriate safety and security requirements tailored to address types of risk.

Within ICT collaborative initiatives, the public sector should help, along with industry, to clearly define the guidelines and expectations for IoT operators in ensuring data confidentiality, integrity, and availability. Policymakers and industry should also promote interoperable standards that are consensus based, globally recognized, and market driven.

Additionally, policymakers should assist in working with industry to help tackle some of the major problems, while also resisting prescriptive, legislative security initiatives that would either limit its scope to focusing on certain technologies or lose its relevance in future years. To that end, companies should be encouraged to determine appropriate security requirements for specific applications upfront when designing architectures, in conjunction with security requirements and solutions based on interoperable standards that are consensus based, globally recognized, and market driven.

Interoperability and Standardization

Interoperability and standards are of central importance in facilitating the innovation and marketing of the smart devices, objects and applications that will continue to populate the IoT, and should therefore be fostered as a dedicated policy goal. In addition to industry-scrutinized security standards, the focus should be placed on interoperability of privacy regimes to generate general privacy standards. Doing so will help to ensure that interoperability also helps promote trust in devices and services within the IoT. Global, voluntary and industry-driven standards are a key enabler not only for interoperability, but for the IoT ecosystem as a whole as this will allow for the growth of the IoT from various verticals to a horizontal deployment . Open standards among IoT devices and technology must be driven by industry experts, utilizing the effectiveness of current global standards-setting organizations, including consortia that involve industry and government collaboration.

Thank you for the opportunity to comment. We appreciate your interest and your consideration of our request to participate in the workshop.