Albany
Atlanta
Brussels
Denver
Los Angeles
Miami
New York

McKenna Long & Aldridge LLP
1900 K Street, NW
Washington, DC 20006
Tel: 202.496.7500
mckennalong.com

Northern Virginia
Orange County
Rancho Santa Fe
San Diego
San Francisco
Seoul
Washington, DC

DANIEL W. CAPRIO, JR.
Direct Phone: 202.496.7348
Direct Fax: 202.496.7756

EMAIL ADDRESS
dcaprio@mckennalong.com

January 10, 2014

Mr. Donald S. Clark
Federal Trade Commission
Office of the Secretary
Room H-113 (Annex B)
Washington, DC 20580

Re: Internet of Things, Project No. P135405

Dear Secretary Clark:

On behalf of Transatlantic Computing Continuum Policy Alliance,[1] I am pleased to submit these comments in response to the Federal Trade Commission's (FTC) request for public comment on the privacy and security implications of the Internet of Things (IoT). We commend the FTC for holding its IoT workshop on November 19, 2013 and appreciate the opportunity to participate.

The Need to Foster Innovation

The Internet of Things is a broad term that describes the ecosystem of sensors that interact with each other, persons, and services in computer-aware environments supported by analytics. The complexity of this ecosystem includes sensors that will only interact with each other, sensors that will interact with the broad ecosystem through local area networks (LANs) as well as sensors that may

[1] The Transatlantic Computing Continuum Policy Alliance consists of AT&T Corporation, General Electric, Intel Corporation and Oracle Corporation.

be in direct contact with the Internet. All actors need to consider the breadth and potential implications of all policy actions on this emerging, yet complex, ecosystem.

The IoT represents a transformative 21st century technology that promises to revolutionize homes, cars, health care and industry in general. The IoT presents the opportunity and the challenge of protecting privacy and security and encouraging innovation. Whether we call it the Smarter Planet, the Internet of Everything, or the Industrial Internet-- the IoT is about innovation and the future of the internet ecosystem itself.

But despite the existence of sensors for decades, we are still at the beginning of the beginning of the promise of IoT. Business models must be allowed to develop. The potential benefits of the IoT are only now emerging, as sensors can interact with other objects or people in computer-aware environments to make use of cloud-based services supported by Big Data and powerful analytics. While consumers are already using internet enabled devices to reap the benefits of social media and e-commerce, industry has only begun to explore ways in which connected devices can improve the safety and reliability of complex industrial processes; achieve greater energy and operational efficiencies; create faster more cost effective means of communications; and improve the safety of medical devices and services. If the vast societal and economic benefits of the IoT are to be realized, the FTC must embrace a broad vision for the IoT and confront the opportunities and challenges with evidence-based work toward practical solutions that protect the individual, encourage responsible use of data, and foster robust innovation.

Some IoT devices will employ user interfaces which will clearly indicate to individuals how data is being collected and may offer controls directly or through LANs as appropriate; other technologies will collect and transfer data with little to no recognizable interface and with little or no communication to the individual about the nature of the data collection. Further, while some IoT devices will interact directly with the consumer and be designed principally for the consumer, others (such as connected airplane engines, wind turbines and locomotives) will operate principally in the industrial space and therefore involve a separate set of considerations on issues such as the practicality and utility of one-to-one consent.

The Need to Focus on Transparency, Use and Security

Some IoT applications challenge traditional notions of how to apply privacy frameworks like the Fair Information Practice Principles (FIPPS) that have been in place since the 1970's. Those established frameworks serve us well but much has changed since the era of centralized databases, highly structured data and relatively straightforward consumer transactions involving one buyer and one seller. Unlike the client server infrastructures of fifteen years ago, today's internet ecosystem contains an abundance of unstructured data, is highly transactional and thrives on a one-to-many model with many players including cloud services providers, intermediates routing traffic and establishing connectivity and entities providing enhanced security. Similarly, other industries using IoT devices, like the health care industry, now involve a complex network of providers, payor entities, product providers and service agendas, and researchers.

The advent of the IoT compels policy makers, industry and civil society to confront traditional notions of notice and choice, security and accountability and consent. While we should not abandon the FIPPS, we do need to adapt, interpret and update them in a way that serves the IoT environment.

The model that underlies US privacy protection is notice and choice. We need to move away from an approach centered on the collection of data to focus in practical terms on what happens to that data and how it's used, bearing in mind the real world harms and consequences. That does not mean that there is no role for notice and choice, but rather that we must review the context of the implementation and potential societal benefits from how the information may be used to determine what controls are needed to protect privacy within the circumscribed use. We need to think through how we manage notice and choice - not to change existing privacy principles, but to provide more guidance about how to apply the existing principles in this new IoT environment.

We now enter a computing continuum era of technology, where many of the devices make it difficult or impossible for an individual to read something that looks like a privacy policy. Data aggregation from sensors and machine-to-machine communications --the IoT-- and the increased value from data analytics

mean individuals will not always know who holds data relating to them. At the same time, many IoT applications will be designed to give users more customization, and provide for better authentication and greater control over their data.

We must adapt notice to individuals to provide real time, context- specific information that will help them make decisions, such as a message that a mobile application would like to collect location data. These context-specific choices are something engineers, working alongside privacy and security professionals, can help bake into products.

Accountability requires that mechanisms are in place to demonstrate the responsible use of data--whether or not an individual has had the opportunity to consent. We need to confront when it is reasonable to expect an individual to consent to their data being processed. Unfortunately, consent often places an unreasonable burden on individuals to understand how their data will be used in complex environments, while at the same time consent may be impossible to obtain in many contexts. Together, we need to continue to invest in providing individuals with easier and more automated methods for consenting, while also protecting privacy in those contexts where consent is not possible. This is where we need to spend a lot of time thinking through use cases and outcomes.

Therefore, it is important for us to more fully explore what are appropriate and accountable uses of data. A focus on accountability and use shifts the burden from the individual back to the organization that holds the data, as it encourages responsible behavior even for situations where consent cannot be obtained. This shift, in turn, will promote innovation and the development of new business models, while, encouraging responsible behavior even for situations where consent cannot be obtained.

The complex data environment of the computing continuum will put an even higher priority on security. As technology stores more data relating to individuals, the threat of potential exposure of the information will increase. These threats, and the possible increased risk to the individual, require increased focus on the mechanisms and technology tools used to secure data.

The future of technology shows us an environment where we can no longer burden the individual with having to make choices about all issues concerning the processing of their data. In sum, we must increase transparency and safeguard security while we work together to define what is the appropriate use of data.

Conclusion

Policy experts, academics and regulators have, on the whole, not succeeded in predicting the emergence and success of future business models. To avoid well-intentioned but unintended consequences, the FTC needs to avoid unnecessary constraints on innovation or adoption of proscriptive polices to allow IoT markets to develop. Industry stands ready to work together with government and civil society in the spirit of a true multistakeholder process to address these very important issues. The potential societal benefits of the IoT are enormous and we need to ensure the policy framework to protect privacy and security supports trust and confidence in the IoT going forward.

Very truly yours,

Daniel W. Caprio, Jr.
Senior Strategic Advisor

DWC