Fusion of the real and virtual worlds: transatlantic regulatory efforts

The Internet of Things, the principle of connected devices and objects that are uniquely identifiable, is becoming a reality. The prevalence and incorporation of technology into everyday life is a growing trend, resulting in a fusion of the real and virtual worlds. Dan Caprio, Senior Strategic Advisor at McKenna Long & Aldridge, and the transatlantic subject matter expert to the European Commission Expert Group on the Internet of Things, provides an overview of the policy and strategic concerns from both US and EU perspectives.

Introduction

The Internet of Things (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*. 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 and smart grids, 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.

To unleash the global potential of the IoT in an age of distributed computing, it is crucial to protect privacy and enable innovation to seize the countless opportunities that the IoT offers. In order to translate the huge potential the IoT offers into concrete benefits for business and individuals alike, we need to address the concerns that currently hamper its uptake, or might slow down global innovation and competitiveness, such as narrow technology-specific regulations or mandates.

Our discussion of IoT privacy must take place in a real-world context with a focus on protecting citizens against consequences rather than focusing on hypothetical harms. Privacy and personal data protection remain an integral part of our ICT system, and must follow the principles of proportionality and transparency.

Transatlantic Policy Issues

Since I have served as the only transatlantic member of the European Commission IoT Expert Group, I am delighted by Federal Trade Commission (FTC) Chairwoman Ramirez's announcement in March that the FTC plans to hold an IoT workshop later this year to understand the opportunities and challenges to IoT adoption in the USA. The FTC's IoT workshop promises to be a fact-finding exercise for the FTC to educate itself rather than the beginning of a regulatory enquiry. The FTC has broad existing authority under section 5 of the FTC Act to enforce unfair or deceptive acts or practices in commerce without the need for additional regulatory or legislative authority in the USA. In Europe, the proposed European General Data Protection Regulation provides a sufficient horizontal and interoperable regulatory framework to address privacy concerns without IoT-specific privacy legislation.

Privacy and Data

Protection Adhering to privacy and data protection remains paramount. In Europe, we need a strong legal framework that would continue to ensure privacy and data protection while concurrently facilitating innovation and the free flow of data in a strong, flexible and workable framework which remains technology-neutral in nature and will address a wide range of privacy concerns in a horizontal manner. Moving beyond the scope and aims of the proposed Regulation with IoT-focused policy initiatives 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 the 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 organisations, should take privacy into account from the very start of all processes. A 'one-size-fits-all' approach and a prescriptive model of the '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.

Under the current European regime, the 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 on the threat to privacy. These analyses must be coupled with transparent practices of an organisation, so the individual would be able (depending on the context) to receive reasonable and appropriate notification as to the type(s) of data collected and how it will be used. The type of data collected will help to determine what 'reasonable' and 'appropriate' notification is. These privacy principles must of course be bolstered by education initiatives, allowing individuals to understand the implications regarding their privacy considerations and equip them with the necessary tools to control which of their data is collected and how it can be deleted.

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, the possibility remains 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 dearly define the guidelines and expectations for IoT operators in ensuring data confidentiality, integrity, and availability. 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

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 — known as *horizontalization*. Open standards among IoT devices and technology must be driven by industry experts, utilizing the effectiveness of current global standards-setting organizations (including fora and consortia) that involve industry and government collaboration.

Governance

The IoT concept includes a very broad range of technologies and applications that are still in the early phase of development and market deployment. Whether they will raise specific public policy issues

that are fundamentally different from those discussed in the internet domain is still unclear, however, a new, dedicated IoT Governance framework is not necessary at this point in time. IoT-specific policy issues must be dealt with in the framework of existing internet Governance platforms. At the same time, the ITU (International Telecommunication Union) is not the place for the IoT. Rather, existing IoT multistakeholder platforms taking place in the Internet Governance Forum (IGF) are the right fora.

Dan Caprio
Senior Strategic Advisor
McKenna Long & Aldridge
dcaprio@mckennalong.com

[D]iscussion of IoT privacy must take place in a real-world context with a focus on protecting citizens against consequences rather than focusing on hypothetical harms

facilitating the innovation		