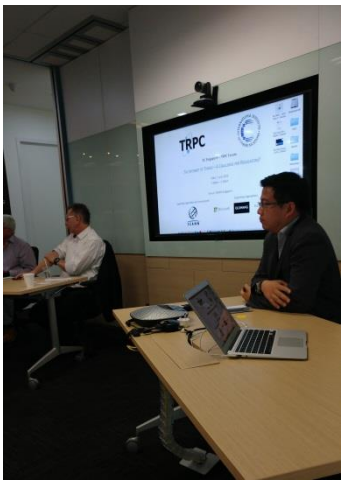
IIC Singapore – TRPC Forum

THE INTERNET OF THINGS – A CHALLENGE FOR REGULATORS?

Date: 2 June 2016, 3.00pm – 5.00pm

Venue: ICANN Singapore



Event summary

Kelvin Wong, Head of Outreach for the Internet Corporation for Assigned Names and Numbers (ICANN), introduced the forum, followed by speakers Andy Haire, ex-Deputy Director of the Infocomm Development Authority of Singapore (IDA) and Rajesh Sreenivasan, Head of Technology, Media and Telecommunications of Rajah & Tann Singapore LLP.

Just about every IT company on the planet is now working towards products and services that are being called the Internet-of-Things (IoT). From wearables such as smart watches, to connected vehicles, to devices of all sorts, data is already being generated on a humungous scale. It's Big Data in terms of volume, but it is also Wide Data in terms of the proliferation of sources, and it's Deep Data in terms of what we infer from it. The more sources available, the greater the possibilities of triangulation and individual personal identification, even from pseudonymous data. Personal data protection based upon the consent of the data owner becomes impractical in such a world. The focus needs to shift from the way data is collected to the way data is used and onto how it is monitored.

During a review of the challenges of IoT it became clear that while each connected device will need an address, most will not come under a DNS. This raises the question of how to ensure the integrity and authenticity of the "thing" (wearable, device, machine, etc.) and the data coming from it. The discussion centred for a while on the importance of distinguishing between data privacy issues and data security issues, although the two often overlap. Putting both into perspective, the backdrop is how rapidly the volume, nature and usage of data is changing, so much so that many of the best through-through approaches to both privacy and security from a decade ago no longer meet the challenges of an IoT emerging world. In the realm of personal data privacy and protection, the idea (or 'ideal') of "consent" is losing its operational meaning. This is partly driven by the spread of data-generating technologies, by Big Data algorithms that can literally scan billions of bits of data in seconds, biometric recognition technologies, etc., all of which make a nonsense of anonymization, and partly by changing business models that seek to monetize that data.

How should regulators react? Should they try to defend the line, despite its impracticality? Should they bend with the trends, which means they become purely reactive? Or should they adopt a new approach, which will require a rethink of policy issues? The emerging view seems to favour the latter in the form of shifting the focus of regulation from data collection – but not giving up the need for consent, transparency, the right to access own data, etc. – to data usage, to whether the data is being used for the purposes it was intended when collected. How this would be monitored would then become a regulatory issue. Could this be done without adding to the cost of compliance? Would this require industry or sector codes of conduct? These questions seem to imply that there has to be a new relationship developed between the regulators and the regulated, one that is two-way, flexible and yet avoids the issue of regulatory capture. Does that depend upon the personalities involved, or are there institutionalized ways to avoid capture? Transparency as well as accountability would seem to be at the heart of

this issue. Without it, today's widespread lack of trust in those who manage the economy (public and private sector alike) which currently seems so all-pervasive, will make finding workable solutions to these challenges almost impossible.

Among other issues, below are highlights from the Q&A session:

- Recent developments in machine-to-machine (M2M) data sharing have raised new concerns regarding privacy. The meeting discussed despite that being a computer or a machine, that fact in itself does not preclude the abuse of personal data. A practice is undertaken by email providers in the recent past where machines read personal email for marketing data and preferences. Just because a machine is reading the information does not mean data is any less at risk or compromised.
- It is now an accepted notion in society that consumers give up personal data depending on the value or perceived returns. Consumers "sign away" and provide consent if it provides them access to services or free apps. This carefree practice creates problems for regulators, in that most people give up their rights and consent to providing data in all sorts of circumstances, without knowing what they have provided their consent on.
- The complication arises whereby obtaining consent from users is no longer meaningful. Consent can be obtained but usually it is unclear how the data will be used. Additionally in most click wrap agreements, the data processor may use the information in many unexpected ways in the in future.
- The session also touched on immediate or real-time communication with the data owner regarding new or potential uses of his/her data. Would there be a way to contact the owner of the data to request permission sporadically? In this case a dynamic consent procedure is a useful model, however, potentially unpractical.
- There were other positive comments raised about predictive and personalised advertising—where one's preferences are used for predictive marketing purposes and on the Internet.
- Regulators have many upcoming challenges in the future to find a right balance between regulating and allowing information to be used for analytics. Regulators will need to look at the categories and uses of personal data as opposed to merely obtaining "consent."

The issue of security received less attention in this forum, yet there are very key issues involved in the role regulators, either general regulators or sector-specific regulators, have to play in not only raising awareness of the challenges of cyber-security, but changing ("nudging"?) organizations into taking serious steps to improve security and imposing requirements as necessary, possibly backed up by penalties. These topics will be the focus of a future forum.

TRPC and IIC Singapore would like to express our appreciation to ICANN for hosting the forum, despite it coinciding on the week of Communicasia in Singapore. Registrations had to be limited to around 50, and so popular was the topic that a full house was achieved several days early, despite only two weeks of notification.

Event URL: http://trpc.biz/iic-singapore-trpc-forum-the-internet-of-things-a-challenge-for-regulators/

For more information on our events please visit: http://trpc.biz/news-events/forums/