ISOC-TRPC-IIC Roundtable on

Privacy in an Internet of Things World

2-6pm, Mon, December 15, 2014

State Room 3, 8th Flr, Westin Grande Sukhumvit, Bangkok, Thailand

Event Report

Extended and lively interaction marked the discussion around the "Privacy in an Internet of Things (IoT) World" Roundtable in Bangkok. Local and international participants and speakers were present at this Roundtable held during the afternoon of December 15 at the Westin Grande Sukhumvit in Bangkok, with the vast majority of the 60-strong participants staying through to the end and beyond. The Roundtable was co-organized by the **Internet Society (ISOC) Asia Pacific Bureau,** regional technology policy research specialists **TRPC**, and the **Thailand Chapter** of the **International Institute of Communications (IIC)**.

The discussion came at an opportune time given growing public concern around privacy and increased interest in IoT and Big Data. In fact, one speaker pointed out that the heightened concern around privacy has kick-started Thailand's discussion around a Personal Data Protection Act – which looks like it may finally be pushed through, after being delayed for more than 10 years. Indeed, keen interest in the subject was evident from the level of attendance with well over 60 participants, including senior government officials and policymakers, leading academics, industry body and private sector representatives, and representatives from civil society. The high quality of discussions between panellists and participants continued well beyond the forum due to the interest and questions, and many groups were engaged in follow up conversations even after the Roundtable had been concluded.
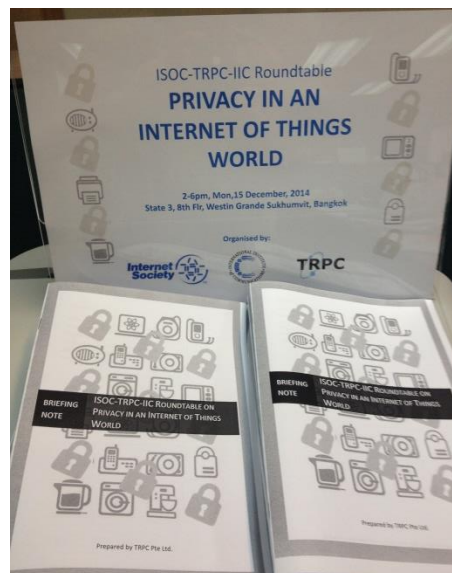
In the first panel of the day, discussants from the private sector and academia looked at the opportunities presented by IoT and Big Data, what the challenges are, and how frameworks can be better in place to better harness the issues. It was noted that only 20% of available data is being used to make important decisions today, which begs the question of how to best analyse and utilize the remaining 80% of data. Improvements in this area will impact everything from improving the consumer shopping experience, to early detection of national threats, to finding cures – or preventive measures – for deadly diseases.

However, while IoT and Big Data may represent tremendous opportunities, there needs to be a balance between mining data, and maintaining safeguards and ensuring privacy. The issue of respecting and maintaining privacy has become an increasingly challenging task, and even the concept of a privacy framework differs across different countries, depending on history and culture, and other norms. Indeed, one of the key issues raised was jurisdictional and cultural differences – with one speaker pointing out that Thailand doesn't actually have a word for "privacy" – and the importance of factoring norms into both understanding regulatory development and implementing it. One way to mitigate the complexities of privacy is of course to anonymize data, where data can be cross-referenced when required, but questions were raised throughout the sessions as to the viability of anonymization as a path forward. Another way is to be advocating for the ethical (and not just innovative) use of data, insofar as companies respect users when they collect, process, and secure data, and are required to remain transparent and accountable for their actions; one speaker called this the "Era of Ethical Data".

Thailand was the first country to digitize and require personal data to be located – centralized – in a single government database. However, there still appears to be a low level of awareness on privacy issues, although this has been increasing in recent years. But while personal data protection is provided for in various others laws and regulations, efforts to pass a comprehensive law on data protection has been on-going for many years, and it remains uncertain when this legislation may eventually be passed. Policy makers will need to consider carefully the local social and cultural nuances, and consider a full range of available approaches, including education such as social learning, and raising public awareness.

In the second session, speakers shared the different experiences and perspectives on privacy and data protection from the European Union (EU) and other countries in South East Asia. While data protection in the EU was originally driven from a perspective of protecting human rights (and is currently being strengthened for online privacy, including regulations around the "Right to be Forgotten"), other countries have data protection laws motivated by different issues, such as economic drivers, national security etc. How a country such as Thailand, ultimately decides on formulating and implementing its Personal Data Protection Act, will be determined by its motivations in doing so, and will need to consider the cultural, historical, and legacy issues when doing so. Several participants suggested that the Fair Information Practice Principles, and OECD Guidelines provided a good initial reference point to consider.

Thailand's privacy and technology regulatory landscape is dynamic and challenging, with the new government proposing reforms on digital economy, and strengthening the current Electronics Transaction and Computer Crime Acts. More cooperation and open discussion between the government and private sector is encouraged to facilitate a balance between innovation and privacy, without stifling innovation and creativity. If done right, Thailand stands at a position of being able to productively advance as a leading digital and Internet economy.