

Asian privacy scholars question ‘easy privacy’ at conference

By Andrew A. Adams and Kiyoshi Murata.

On 10 and 11 July 2014, members of the Asian Privacy Scholars Network (APSN) once again convened for a wide-ranging conference at Meiji University in Tokyo. Professors Adams and Murata of Meiji’s Centre for Business Information Ethics hosted the event, in the impressive venue of the Kishimoto Tatsuo Hall on the 23rd Floor of Meiji’s Liberty Tower building, which overlooks the Imperial Palace in Tokyo. Under the high domed ceiling, watched by portraits of the University’s founders, 20 scholars from around the world presented, and more than 30 more debated, pressing issues of privacy and surveillance in the Asia-Pacific region. The stated theme of Easy Privacy wove a subtle thread through many of the talks rather than a strong explicit theming. Ten of the presenters were also involved in meetings on joint academic research over the following days. APSN¹ now has 80 members, involving researchers from most countries in Asia and those from outside the region engaged in Asian privacy issues. This was the fourth APSN Conference since 2010, and past conference chairs form an ongoing advisory committee.

Each day of the event began with a keynote speech consisting of multiple juxtapositions. Professor Luciano Floridi of the University of Oxford presented an academic and philosophical analysis of the problem of helping individuals make better choices, presenting his solution to the question of whether tolerant paternalism can exist and what use it might be in the information age. Mr Naoto Bessho, a senior executive of Yahoo! Japan (a separate corporate entity from Yahoo! in the US), provided a Japanese legal and business view of the right to be forgotten. Yahoo! Japan is one of the most visited websites in the country and as such has watched with keen interest the recent CJEU decision regarding this issue (see p. 27).

FATHER REQUIRES A CHOICE – TOLERANT PATERNALISM

Using computer systems allows and may even require making many choices. Information ethics analyses have long valued “informed consent” as a gold standard of personal information processing principles. Starting from historical ideas of paternalism (acting to curtail the autonomy of another in the best interests of that person or of society as a whole) and tolerance (accepting aspects of others, including their choices, which one finds objectionable to some extent), Floridi tried to identify whether it is possible to be both paternalistic and tolerant at the same time. In a detailed philosophical and logical analysis, he presented paternalism and tolerance not as binary on/off concepts, in which they may be seen as oppositional values, but as measures of the level of interference with free choice. The “Nudge” approach of allowing a selection deemed “negative” but making it more “expensive” to choose than the preferred “positive” selection, he analysed as moderately paternalistic and moderately intolerant. Defaulting to the most common selection where that is known to be harmful to the individual (or society), Floridi claimed, was moderately tolerant but moderately non-paternalistic. In the end, though, he claimed that a middle ground exists whereby the maximum amount of tolerance and paternalism can peacefully co-exist. This is embodied in the “required choice” model whereby information is made available (but choosers are not required to avail themselves of it) about the consequences of each selection and a strictly positive choice is required.

ASIA-PACIFIC PERSPECTIVES

Various speakers presented some single nation-oriented reports. Professor Jim Foster from Keio University gave a US-business-oriented perspective on consultations by the Japanese

government regarding potential revisions to Japan’s lacklustre data protection regime (proposals reviewed by Professor Graham Greenleaf in *PL&B International* August 2014, pp. 23-25). There was some surprising agreement between Professor Foster and privacy activists on some aspects, most notably on vesting data protection authority in a single body and providing clearer guidance on accepted practices. There was less agreement on whether that body should be a proactive data protection commissioner as in the EU or a reactive consumer protection commissioner as in the US.

Wan-Ping Li presented a background and current evaluation of the Taiwanese Personal Information Protection and Administration Systems, in which again there was a call for a more coordinated data protection authority regime. These calls were echoed by Professor Kyung-Sin Park from Korea University, in his review of the paradoxical nature of the Korean Resident Registration Number with respect to privacy and citizen security. One of the failings of the system to help protect citizens from misuse of their data has been the lack of coherence between government departments in their treatment of organisations under their purview for data protection issues. Professor Nohyoung Park, also of Korea University, who chaired a session at the APSN conference, had argued at a seminar the previous evening on Japan’s proposed reforms that Korea’s Personal Information Protection Commission did not in fact constitute as much of a centralised (or effective) data protection authority as it seemed at first sight. So there was a consensus that Asian countries needed clearly-established and effective data protection authorities.

Professor Gehan Gunasekara took us South for an initial exploration of the privacy notices on the websites of major New Zealand firms, concluding that there was much work to be done in

making these policies reflect New Zealand law, best practices and the actual operations of those companies' sites.

EUROPEAN IMPACT ON ASIA-PACIFIC PRIVACY

The EU, when taken as a single country-like entity, is the largest economic bloc in the world. Its regulatory approach, particularly when it differs substantially with that of the US (with only a slightly smaller economy), can have major impacts around the world and the EU's data protection regime is clearly one of those areas in which impacts are considerable. Accordingly, a number of speakers included a European flavour in this Asia-Pacific focused conference. Gertjan Boulet from the Free University of Brussels presented exploratory work on mutual recognition of sanctions between data protection regimes as a way of improving cross-border protection but also easing cross-border trade, featuring EU Member States' approaches amongst others. Professor Greenleaf then compared the activities of data protection penalty-application bodies between the EU and Asia-Pacific, in terms of their power to levy such penalties and their track record of doing so. Lachlan Urquhart highlighted the challenges for the development of ubiquitous computing devices and services of complying with current and proposed reforms of EU data protec-

tion law, highly relevant to at least Japan, which has strong developing industries in these cutting-edge technology areas.

THE SHADOW OF SNOWDEN

The revelations by Edward Snowden of the activities of the US NSA, the UK GCHQ and other intelligence agencies around the world was a strong theme again this year. Professor Kiyoshi Murata presented some startling differences between the attitudes of Japanese university students and their compatriots in Spain regarding Snowden's actions. In particular it was heartening to see so many young Spaniards following up their evaluation of the rightness of Snowden's actions with a claim that they would follow the same path themselves in similar circumstances. Less heartening was the Japanese students' unwillingness to take any risks and in particular "not to stick their neck out for anyone". Professor Andrew Adams provided a philosophical and practical guide to why so many (including himself) are outraged by the scope, targets and intensity of the NSA's and GCHQ's operations. He focused on the chilling effects for democracy of such all-seeing eyes, and the degradation of everyone's personal security that lack of privacy brings. Dr David Murakami Wood completed the Snowden session with questions about why NSA activity in Japan is so little

reported, despite their major open presence at Misawa airbase. The lack of press coverage of Snowden's revelations in Japan is particularly strange, he believes, given that Snowden himself was based in Japan for a number of years and was well-known online for his enthusiasm for living there.

CONCLUSION

The 20 presenters and 31 other attendees made this a lively and vibrant event. *Privacy Laws & Business* sponsored the conference dinner, as it has since its inception. The APSN events are succeeding in bringing together privacy scholars to present their findings to each other, and in bringing policymakers from various Asian countries (particularly from Thailand this year) to listen and to engage in these debates.

AUTHORS

Andrew A. Adams is Professor of Information Ethics at Meiji University, Tokyo. Kiyoshi Murata is Professor of Management Information Systems at Meiji University, Tokyo.
Emails :aaa@meiji.ac.jp
kmurata@meiji.ac.jp

INFORMATION

This article covers only a portion of conference presentations. More details can be found on the conference website www.kisc.meiji.ac.jp/~ethicj/APS4/ including slides for many presentations.

CNIL issues public warning to Orange France

France's Data Protection Authority, the CNIL, has sanctioned the mobile telephone company, Orange France, for a data security breach. The public warning, issued on 25 August, follows a security breach which jeopardised personal data of more than one million customers. Information stolen in a cyber attack included customers' names, email address, mobile and land-line phone numbers and dates of birth.

Back in April, Orange notified the CNIL of the breach of personal data related to a technical failure by one of its providers. All publicly available EU electronic communications services are obliged to report data breaches to the regulator.

In May, the CNIL carried out an

inspection on Orange and its subcontractors, XL Marketing and Gutenberg Networks, working on its promotional email campaigns. The CNIL found gaps in data security, and initiated the enforcement proceedings.

According to the CNIL, the company claimed to have taken all necessary measures to fulfil its data security obligations, but had not conducted a sufficient security audit before using a certain technical solution for sending email campaigns.

The CNIL has a fining power of a maximum of 150,000 euros, and where similar previous offences have been committed, up to 300,000 euros. It can also issue an injunction to stop processing. In this case, after giving details of

the breach and Orange's defence of its position, and giving the company a month to comment on its draft decision, the DPA issued a public warning.

The CNIL considers that Orange should have had sufficient financial and human resources to manage these problems.

• See www.cnil.fr/linstitution/actualite/article/article/la-societe-orange-sanctionnee-pour-defaut-de-securite-des-donnees-dans-le-cadre-de-campagnes/

For the CNIL's detailed decision, see www.cnil.fr/fileadmin/documents/approfondir/deliberations/Formation_contentieuse/D2014-298_avertissement_ORANGE.pdf