Privacy beyond data at the 11th IAPP ANZ Summit

By Annelies Moens, First published in News and Insights, TrustArc on 19 January 2020

12 December 2019

Introduction

This year's 11th IAPP ANZ Summit, was for the first time organised by the IAPP in the USA, since the recent transition of ANZ operations to the USA. The Summit was held in Sydney, with many international guests, including Hilary Wandall from TrustArc, making the journey to Australia's largest capital city. Unfortunately Sydney was subjected to significant levels of air pollution as bushfire season had started early.

The ANZ Summit is focused on privacy developments in Australia and New Zealand. It is the preeminent forum in which both the Australian and New Zealand Privacy Commissioners provide keynote addresses to delegates.

Regulator addresses

Angelene Falk, the Australian Information and Privacy Commissioner spoke about a number of regulatory priorities in her keynote speech including the development of a Code to regulate digital platforms arising out of the ACCC's Digital Platform Inquiry. Funding has already been allocated to the OAIC for some of this work. The Australian Government has further responded to the Inquiry on 12 December 2019. Legislation to increase penalties for breaches of the Privacy Act will come before Parliament in 2020. Penalties will increase to $10 million, 10% of annual turnover or three times benefit received, whichever is highest. These penalties would then align with those found in the Competition and Consumer Act 2010 (Cth). Other provisions of the Privacy Act as recommended by the ACCC will also be reviewed in 2020 and finalised in 2021.

John Edwards, the New Zealand Privacy Commissioner focused his keynote speech on addressing the power asymmetry of the big tech companies, and the impact of global technologies at local level. This was particularly topical from a New Zealand perspective because of the recent shootings in Christchurch which were broadcast live on social media. Facebook had made some attempts to use artificial intelligence (AI) to identify content that could harm viewers, but its AI did not identify these shootings as it had been trained on ISIS beheadings, and the shootings in Christchurch were not "gory enough". The New Zealand Privacy Act currently does not have extraterritorial reach (but is expected to once amendments come into effect mid 2020), so can do little about perceived privacy harms perpetrated by foreign companies, even if they affect New Zealand citizens. This contrasts with the Australian Privacy Act which has extra territorial reach.

The New South Wales (NSW), Queensland and Victorian Privacy Commissioners also spoke on a panel addressing their key areas of concern and priorities. Of note were concerns around AI, in particular state governments introducing AI to make decisions about people with limited risk assessment and guidance. For example, the NSW government has passed an Act which enables AI to analyse photos of every driver to see whether they are using a mobile phone whilst driving and places the onus of proof on citizens to disprove their use of a mobile phone.

Applying accountability to AI

I was on a panel with the Australian Human Rights Commissioner, Edward Santow, Samantha Brown, an attorney from Microsoft, and Dr John Selby from the Optus-Macquarie University Cyber Security Hub. Privacy risk assessment methodologies can be augmented with the added risks that AI presents around bias and differences between human and machine decision making to create algorithmic impact assessments. The Australian Department of Innovation and Data 61 released an updated set of ethical principles for AI after receiving extensive feedback on its Discussion Paper released earlier in the year. The focus of AI development in Australia is on data sets relating to natural resources and environment; health, ageing and disability; and cities, towns and infrastructure.

Protecting people, not just data

Professor Woodrow Hartzog, one of the international guests at the ANZ Summit, spoke about data protection being unable to solve all harms. He made the point that legitimate processing of data can still be harmful, for example, addictive technology, fake news, manipulation, and collection of massive amounts of data affecting mental well-being and social relationships.

Hartzog argued that we need a more holistic approach to privacy as power is amassed through the collection of personal information and privacy is agnostic to external harms such as environmental harms (through mass processing of data), erosion of democracy and hijacking our attention.

There is also a need to update tools (such as notice and consent) and regulatory models. There are limits to consent from cognitive overload, industry intentions and incentives. There are incentives for businesses and governments to hide risks and to shift them to individuals, who are least able to bear risk.

Christchurch call

There were many other panels including a panel on social media which focused on the response to the viral streaming of attacks in Christchurch. New Zealand and France are leading the way to eliminate terrorist and violent extremist content online with the support of technology companies, civil society groups and other economies, in the Christchurch call.

iappANZ legacy

For the last 10 years a volunteer group of privacy professionals (including myself as a co-founder of iappANZ and a past President) have steered the development of the privacy profession in Australia and New Zealand. Hundreds of members and a decade of successful conferences left a large surplus of funds which were distributed prior to IAPP taking over operations. To recognize the dedication of this startup group of volunteers and members, $AU180,000 in funds was distributed to Australian and New Zealand organisations to fund privacy subject prizes and privacy research. Results of these efforts will be published in due course.