IAPP Asia Privacy Forum 2016, Singapore

19 July 2016

Panel: The Regulator's View

Participants:

- Hilary Wandall, Compliance and CPO, Merck (Moderator)
- Lahoussine Aniss, General Secretary, Moroccan Data Protection Authority
- John Edwards, Privacy Commissioner of New Zealand
- Said Ihrai, Chairman, Moroccan Data Protection Authority
- Travis LeBlanc, Chief of Enforcement, Federal Communications Commission
- Stephen Wong, Privacy Commissioner, Office of the Privacy Commissioner for Personal Data, Hong Kong

Session topic summary: Through efforts like the Global Privacy Enforcement Network, it's clear that regulators around the world are working together like never before. As privacy is increasingly borderless, it's necessary to team up, talk shop and make sure borders don't get in the way of protecting the rights of their citizens.

- But how does this work in practice?
- Do all regulators like to work with companies in the same way?
- Do they fear 'regulator shopping'?

These regulators will discuss their approaches and provide practical tips for making sure a business's regulator interactions are positive ones.

NOTES

As Privacy Commissioner, my role is to administer the Privacy Act 1993.

The Privacy Act applies to almost every person, business or organisation in New Zealand.

The Act sets out 12 privacy principles that guide how personal information can be collected, used, stored and disclosed.

These principles are based on the OECD Privacy Principles which tie closely to European Union data protection legislation which implement the European Commission Data Protection Directive.

My role and that of my office is to work to develop and promote a culture in which personal information is protected and respected in New Zealand.

The office has a wide range of functions, including investigating complaints about breaches of privacy, running education programmes, and examining proposed legislation and how it may affect individual privacy.

Our current priorities include delivering digital privacy and data protection tools that can be easily accessed by the public and organisations alike, to work closely with government agencies on information sharing proposals, especially in the area of protecting vulnerable children, and to engage internationally through forums like GPEN, APPA and the ICDPPC.

Our online privacy tools include online education modules, a request-my-info tool called AboutMe, Privacy Impact Assessment guidance, an online complaint form and Knowledge Base.

My office receives over 800 privacy complaints each year and we work to resolve these complaints using mediation and dispute resolution techniques.

Many of the complaints we receive involve private sector organisations, especially in finance and telecommunications.

We can refer serious cases to a judicial tribunal which hears the case anew and can award damages to a complainant who has been harmed by a privacy breach.

The highest award for a privacy breach suffered by an individual is 168,000 New Zealand dollars for when an employer disclosed information it unfairly copied from an employee’s Facebook page.

We continue to receive a significant number of voluntary breach notifications each year – 121 notifications last year, with 71 from the public sector and 50 from the private sector.

International cooperation

- Privacy and data protection regulators work together to share information.
- When the information of millions of people around the world was hacked from Canada-based online dating service, Ashley Madison, the Office of the Privacy Commissioner of Canada was able to keep us informed of its investigation.
- After the Hong Kong manufacturer of digital toys for children, V-tech, was hacked, jeopardising the personal information of five million people including children, the Office of the Privacy Commissioner for Personal Data in Hong Kong kept other APPA members informed of its investigation.
- Privacy and data protection regulators need to be able to respond rapidly across borders to emerging threats.
- They need to cooperate to deliver effective remedies for their citizens, and there have been a number of steps taken.
- We have established the GPEN, the Global Privacy Enforcement Network, and the Mauritius Declaration of 2014 provides for another option for enforcement cooperation between member authorities.
- Asia-Pacific Privacy Authorities meeting here in Singapore this week and in Mexico later this year.
- International Conference of Data Protection and Privacy Authorities meet annually – the next meeting in Morocco in October.
- But there is much to do, and it is a constant struggle to match the pace of industry innovation.

Future directions

- Mandatory breach reporting is a significant tool for privacy authorities
- It puts the individual at the centre of a security failing.
- If a company has a privacy breach which compromises customer data, those customers are entitled to know about it so that they can take steps to protect their identity and information.
- If there is a level playing field, so that every agency must report, SMEs are more likely to comply.

- New Zealand currently relies on voluntary breach reporting but that is likely to change when the government reforms the country's Privacy Act next year.
- One area that has potential to considerably level the playing field between consumers and providers of digital services is "data portability", the ability of individuals to take their data with them when they choose to exit one service in favour of another.
- In a market where one player can very quickly become dominant, there is a potential for innovation to be stifled by monopolistic practices, and a sense for consumers of being "locked in".
- An ability to freely extract one's data will not only restore power and autonomy to the individuals, but will make it easier for new players to transfer to innovative services that better meet their needs.
- Data portability is a part of the European Union's General Data Protection Regulations that will take effect in May 2018.

International developments

- The European Court of Justice ruling in the Max Schrems-Facebook case put an end to the Safe Harbour agreement between the EU and the US.
- Safe Harbour has been replaced by the Privacy Shield which took effect this month to enable the continued flow of data from the EU to the US while maintaining the same level of protection for EU citizens' data which is found in the EU under its data protection laws.
- We're also waiting to see what happens next after Britain voted to leave the European Union because it calls into question the process of creating a single digital market and EU adequacy standards.
- We now have a situation where there is likely to be two jurisdictions where one now currently exists for technology issues including data privacy.
- In Australia, when a government agency decides to use an overseas cloud based service that provider needs to comply with the country's Privacy Act and the Act's storage and security of personal information requirements
- In our part of the world, in New Zealand, our Privacy Act does not extend beyond our territorial borders

- However, the European Commission ruled in 2012 that New Zealand's privacy law provided an 'adequate level' of privacy protection to meet European standards.
- This adequacy status means that personal data information can legally be sent here from Europe for processing without special additional measures being taken by the European companies.
- My office and European Commission officials informally agreed a process for facilitating the ongoing monitoring of the functioning of the 2012 decision.

Data sovereignty and data localisation

- One emerging trend that has serious implications for the free movement of data is the growth of data localisation requirements, and restrictions on trans-border flows of data.
- Some countries such as Canada, Germany, Switzerland, China and Russia have data residency and sovereignty laws which require citizen data to remain in country or for offshore service providers to comply with the domestic data protection requirements.
- In cloud environments, where data centres are located in various parts of the world, cloud data 'tokenisation' can be used to keep sensitive data local resident while replacement data is stored and processed in the cloud.
- Data tokenisation – commonly used in e-commerce - is the process of substituting a sensitive data element with a non-sensitive equivalent, referred to as a token.
- https://www.bluecoat.com/resources/cloud-governance-data-residency-sovereignty
- The mapping from original data to a token uses methods which make tokens virtually impossible to reverse without the tokenisation system which, for example, might be a system of generating random numbers.
- Domestic legislators could also insist on having their citizens' data stored outside their borders strongly encrypted.
- China recently reiterated in a proposed first draft of a new cybersecurity law that Chinese citizens' personal data would have to be stored domestically.

- A recent data localisation law in Russia came into effect in September last year mandated that personal data on Russian citizens must be stored in databases physically located within the country itself.
- It is therefore a big challenge for businesses that do business in these countries, and which are likely to store data in numerous locations across the globe in cloud-based services, to ensure Russian data lives in Russia and the same for China.

Being innovative in engaging with the private sector:

- Against that background, what role is there for an innovative regulator?
- Governments and regulators need to be innovative in the way they provide support to innovative business.
- We need to "make privacy easy" by providing assistance and privacy-enhancing tools for business.
- Some of the things we've done are:
    - An online tool for SMEs to generate privacy policies
    - Online training resources – (my colleagues at France's CNIL have created an impressive library of digital education resources, for example)
    - Online tools that enable people to easily request access for information about themselves - like our About Me tool
    - Privacy Impact Assessment tools (training and guides)
    - Online breach and complaint notification.
- A successful strategy needs carrots but a comprehensive privacy strategy also needs sticks.
- In order to build and maintain consumer trust in the digital economy, citizens and consumers need to be assured that there will be consequences for breaches of that trust.
- Governments must respond by giving privacy and data protection authorities real tools for enforcement, such as:
    - the power to issue fines to make declarations of illegality – as used in many European jurisdictions

    - to warn consumers by calling out poor practices or to bring enforcement proceedings – like the FTC did with Uber to improve its practices
    - privacy regulators in Ireland, Belgium and Spain can bring enforcement proceedings.
- As a privacy regulator and an enforcer, here's a privacy checklist that I look for:
    - organisational culture and awareness of good privacy practice
    - levels of training for staff
    - sensible, clear policies and privacy statements
    - use of privacy impact assessment
    - engaged privacy officers
    - awareness of data breach notification and mitigation
    - a risk management framework backed up by effective governance.
- If my office was investigating a hypothetical complaint, these elements would demonstrate whether the organisation has got its privacy mix right.