Personal Data Protection Seminar, Singapore : 20 July 2016

Panel 1:

Capitalising Smart Cities and Nations – Data Protection in the Age of Data

Panellists:

- Edith Ramirez, Chairwoman, Federal Trade Commission
- John Edwards, Privacy Commissioner, New Zealand
- Christina Peters, Chief Privacy Officer, IBM
- Jane Horvath, Senior Director of Global Privacy, Apple
- Kelvin Kwek, General Counsel, Samsung Electronics

Introduction

As New Zealand's 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 legal obligations apply to both the private and public sector.

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, providing education programmes on privacy and data protection, 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.

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

We are also working 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.

The view from my office is that new technology is a force for good because it is encourages and stimulates innovation.

This applies to the emerging world of sensors, the Internet of Things and Smart Cities and the attendant privacy concerns that come with new technologies.

Some of you will be familiar with Gartner's 'hype cycle'.

Gartner is an American IT research and advisory firm.

It's 'hype cycle' concept applies to new technologies.

The concept is the idea that each promising new technology goes through a similar set of phases before it is widely adopted.

Step one: A new technology is developed.

Inventors, innovators, designers and engineers get their hands on it and figure out how to monetise it.

Word starts to get around about the capabilities, people get excited about it.

Step two: The "Privacy activists" find out about the new technology and come to dampen the mood of excitement.

They spread warnings about worst case scenarios which get picked up by the mainstream media.

In turn, public perceptions start to shift.

Once the technology becomes more widespread, once we start to see real world applications and realise it might not be so bad, we get to step three.

This is when the fear deflates.

Step three is punctuated by mini panics over time, but the general direction of anxiety is down.

Some examples include Samsung's Smart TV, the Jeep Cherokee smart car, the Amazon Echo smart speaker and the new augmented reality game, Pokemon Go.

What's important to recognise is that the impact of each privacy 'scare' plays a part in ensuring that future developments are more privacy-friendly.

Privacy warnings form a vital part of risk assessment.

When business and government assess the risks of a project, even where a risk is high impact but unlikely, it still gets put in the risk register.

These panics form part of the overall process of developing privacy laws and norms.

Where good privacy analysis comes in is recognising the value in, or even predicting, that panic, and in designing solutions that prevent those fears being realised.

Privacy panics help shape approaches for the future.

They help businesses and innovators know where the danger zones are and how to avoid them.

Privacy regulators are here to help.

We're here to help you take the right direction when there is a privacy panic about the customer data you work with and to comply with the privacy laws of your country.

Big data

- The world of sensors and the Internet of Things can be described as the Third Age of Big Data
- The First Age took off with the internet
- The Second Age was the rapid spread of mobile technology and social media

- Now we have a Third Age – the emerging world of soon-to-be ever-present always-on, always-collecting sensors and the Internet of Things
- Each of these ages had its own privacy challenges
- They have in common the collection of big data
- The amount of digital data produced increased exponentially
- Digital data became easier and more plentiful to collect and analyse
- We are now entering the age of sensors and the Internet of Things – in our homes, in our cars, on the street, in our cities.
- For businesses and governments, it has never been easier to accumulate information about people
- There's a big temptation to collect everything you can - the more data points you can string together, the more useful conclusions you are likely to draw.
- We're seeing a transition to what has been also described as a 'web of things' – billions of devices, appliances and sensors collecting pin pricks of information which when combined with other data sets can reveal phenomenal detail about the life of an individual.

Internet of Things

- This 'web of things' is becoming one of the biggest privacy concerns of our age
- The boundaries between the digital world and the physical world are becoming more fluid, more opaque
- Big data on steroids – the big data issues we have today will be multiplied by the Internet of Things
- The Internet of Things has characteristics that make it different to most existing digital technologies up to now
- For example, there's a limited sense of verification with many IoT devices – because they will be in homes and workplaces, and once set up, they will require no subsequent verification of identity required
- IoT devices make accepting terms and conditions more difficult because there's usually no screen interface
- IoT devices are usually on all the time – always collecting data

- IoT software is upgradeable – functionality can change and the nature of the information being collected can also change without the consumer being aware of the change
- IoT appliance software has implications for security - can be vulnerable to hacking
- IoT devices can provide collective intelligence for the business that makes the product enabling it to collect a mass of data across one type or brand of product or range of products
- IoT will make it difficult to distinguish between personal and device data - when an appliance is on-sold, care needs to be taken to separate out personal data in the device or in the cloud
- IoT security has been described as poor because it is often not a priority for the manufacturer
- There are a lack of incentives to improve security, and lack of skills - for example, washing machine manufacturers know how to make washing machines, not how to implement good IT security
- IoT also presents a greater opportunity to use personal data to personalise marketing and advertising
- But IoT manufacturers need to be careful about making assumptions about what the consumer is willing to give away in personal information
- Are people willing to trade privacy for convenience? This is a debate that needs to be had

Data re-identification

- There is concern about big data techniques that can re-identify individuals using anonymised data when combined with other data sets
- New Zealand's Privacy Act says organisations should collect personal information for a stated lawful purpose.
- Organisations can't use personal information collected for one purpose for another purpose
- The way around this is by anonymising or de-identifying the information so that it is stripped of information about identifiable individuals

- In theory, anonymised or de-identified data is no longer personal information and therefore not subject to our Privacy Act
- But as data sets become more sophisticated, the technical possibility of undertaking 'jigsaw' re-identification of anonymised data increases
- Jigsaw re-identification is the ability to identify people using two or more different pieces of information from two or more sources of information
- A famous example of the dangers of anonymising personal information was demonstrated by an American researcher, Dr Latanya Sweeney
- One study showed in an anonymised dataset of 1.5 million telecommunications consumers' locations over a one year period, researchers could identify individual records with 85 percent accuracy, if they knew where they had been just four times in than year
- These examples reveal that our intuitive beliefs about anonymity and identity are often misplaced
- The distinction between personal and non-personal information is becoming increasingly blurred
- Rapid advancements in technical capability exacerbate that blurriness even more
- They raise ethical issues in relation to informed consent, trust and what security of information means and how best to secure it
- Even privacy advocates are divided on the issue
- Dr Ann Cavoukian - the former Ontario Privacy Commissioner recently published a paper suggesting that re-identification isn't as much a concern as Dr Sweeney led others to believe
- But if people can't trust the organisations they do business with, they will look for competitors they can trust
- The public demand for restraint will be met both in the marketplace and in regulation

Smart cities

- The use of sensor technology – as it might be applied to traffic management, crime fighting and public security, energy conservation, crisis management and in dealing with weather or natural events – has unquestioned advantages

- Collecting and analysing data - everything from information about available parking spaces, the brightness of street lighting, flooding and even the rubbish levels in bins - help in the allocation of resources and even in understanding problems that might not have been revealed otherwise
- Six broad categories of privacy to consider:
    - Identity privacy – protecting personal and confidential data
    - Bodily privacy – protecting the integrity of the physical person
    - Territorial privacy – protecting personal space and property
    - Locational movement privacy – protecting against special tracking
    - Communications privacy – protecting against communications surveillance
    - Transactions privacy – protection against the monitoring of monetary transactions
- The challenges of a smart city:
    - Tackling perceptions of a surveillance state
    - Dealing with a public backlash
    - Cyber attacks and ransomware
    - Large and complex cyber attack points
    - Human error or sabotage
    - Employee browsing
    - Collection of inaccurate information
    - Unable for people to opt out
    - Weak anonymisation of the data
    - Dependency on third party providers
- Building the right privacy framework:
    - Have clear policies on what data is being collected and how it will be used
    - Carry out privacy impact assessments
    - Be transparent to the public
    - Build in privacy protections from the bottom up – Privacy by Design
    - Give individuals a way to access data that is about them
    - Strong anonymisation of the data
    - Encrypt the data

- Locate sensors in public spaces only
- Don’t share the data with third parties which may use the data for a different purpose
- Dispose of the data safely once it has served its purpose
- Carry out regular audits
- Carry out penetration testing and identify vulnerabilities
- Have a data breach response plan