Smart and Resilient Cities Series hosted by Public Sector Network

22 November 2018, Wellington

"Get the balance right: Good privacy & open government practices when adopting new technology"

Kia ora koutou katoa

Thank you for the opportunity to speak to you about bringing a privacy lens to your work in building safer, smarter, more resilient cities.

I'm pleased that you've recognised the importance of that perspective, even though it is only one of many.

I hope that by the end of my brief comments you will have a better understanding of the way in which the Privacy Act and principles not only do not get in the way of initiatives to improve the functioning of our cities, and the quality of life of citizens, they are actually enabling and supportive of beneficial technologies.

One of the key messages I hope to leave you with is about the importance of taking people with you, of building and maintaining trust

When the law commission reviewed the Privacy Act in an extensive work programme that lasted from 2006 to 2011 it concluded that while it needed me tweaks to bring it into the 21st century its fundamentals were sound.

Key to that is the fact that the information privacy principles, which form the heart of the Act are 'technology neutral".

What does that mean?

It means that when we get a issue like this [slide of Paxster] even though it involves technology that did not exist in 1993, we are able to address it within our 25 year old historical framework.

This was a case of an unthinking adoption of a new technology, ostensibly in the service of safer workplaces, and by extension, safer cities.

An employee complained, and we found that it NZ Post was in breach of IPPs 1,3, and 4.

Drones were science fiction in 1992 when the Privacy Act was drafted. Now they are ubiquitous. They are making dangerous jobs safe, they are giving us a perspective on our cities that lets us appreciate the hitherto unseen beauty of the hidden corners, and allow us to journey, magic carpet like across our cityscapes. They also pose a threat to aviation, are a boon for perverts, and really piss some people off.

We partnered with NZ Police, CAA, and retailers to produce some collateral to insert into the supply chain – something that your nephew will get with the package when he opens his Christmas present and finds a buzzing aerial

The importance of privacy

- 2018 Privacy Survey – latest in our biennial tracking surveys
- 55 percent of those surveyed are more concerned about individual privacy now than they were in the last five years
- 79 percent are concerned about businesses sharing personal information
- Only 32 percent say they trust companies with personal information
- You need to take these concerns onboard when you're adopting new technology
- Both the current Privacy Act and the new Bill are enabling pieces of legislation
- There is room for flexibility and creativity when it comes to introducing new technology
- But you must be aware of the privacy risks

New technology and privacy – examples

Body cameras for parking wardens

- A local council approached us for feedback on a proposal to equip parking wardens with body cameras.
- The council wanted us to authorise it to collect personal information in a way that it thought would be a breach of a privacy principle.
- We advised the council that its policy didn't breach a privacy principle, so it didn't require our authorisation
- The council had a legitimate purpose for using the cameras – to reduce assaults
- We worked with the council to develop clear policies about when wardens can film people and how the council can handle the footage
- Wardens only turn the cameras on when needed, so the collection of personal information is proportionate
- This clarity around the structure of the Privacy Act gave the council the certainty it needed to implement its cameras
- The cameras have been successful in reducing assaults

CCTV

- CCTV cameras are a vital tool for local government and law enforcement protecting public safety and property Kaikoura public toilet
- But your use of CCTV should be necessary and proportionate
- Camera location is a factor – a camera on a busy street is easier to justify than one in a public toilet
- Be careful about introducing new technology such as facial recognition or audio recording
    - You'll be collecting more personal information
    - You may alarm or upset people
    - Is it necessary? Or are there other options that will improve security without intruding on personal privacy?
- Wherever you use CCTV, put up clear signage letting people know:
    - that cameras are operating
    - that you own the cameras
    - how people can contact you for more information
- Put your full CCTV policy up on your website so people can read it

Facial recognition

Ease of adding technology to the infrastructure eg facial recognition

- A trial by London's Metropolitan Police showed that their facial recognition software got it wrong 98% of the time
- They should take the risk of misidentification seriously and ask themselves what controls and processes they can put in place to minimise the risk.
- Don't leave it up to automated systems alone.
- When it comes to identifying people accused of a crime, getting it wrong can have a severe impact on the person affected.
- Any sort of facial recognition technology runs the risk of misidentifying people.
- A study on bias in facial recognition software by Joy Buolamwini, a researcher at the MIT Media Lab published in the New York Times in February showed that:
    - "Gender was misidentified in less than one percent of lighter-skinned males; in up to seven percent of lighter-skinned females; up to 12 percent of darker skinned males; and up to 35 percent in darker-skinner females.

    - “Overall, male subjects were more accurately classified than female subjects and lighter subjects were more accurately classified than darker individuals,”
- So if a vendor advertises that its facial recognition software is 99 percent accurate, I expect an agency looking at using it to have a high level of scrutiny over how accurate it is and how thoroughly is has been tested for use in New Zealand.
- Introducing this technology can also alarm and upset people. We saw a spike of concern earlier this year then it was revealed that Foodstuffs were using facial recognition in their supermarkets

Other sensors

Dog control – barking dogs complaint – decibel meter in the garden – freaked the people out who complained to us.

New Privacy Bill

- Privacy Act is 25 years old.
- The Act gave people a clear avenue for a privacy complaint.
- My office provided a simple mechanism with an ombudsman-like investigation into complaints and a non-adversarial approach.
- But it needs modernising.
- PA was enacted in a pre-internet age.
- There have been rapid changes in information and digital technology, data science, and changes in international data protection, such as Europe’s new GDPR.
- Reflect on smart phones, Internet of Things, mobile apps, surveillance cameras and drones, artificial intelligence and data mining.
- Privacy Act reform – what are the key changes?
    - Mandatory breach notifications
    - Access determinations
    - Stronger powers
    - New offences
    - Ability to recommend fines

Not in Bill

From GDPR

- Algorithmic transparency/the right to object to automated processing.
- Right to be forgotten

- Data portability
- Reidentification prohibition – what should you do with all that ‘de-identified data? Victoria Health example – telecommunications example

Again, we can and must make our existing principles work. And the PA does help us to do that. Do privacy impact assessment, do privacy by design.

If you are rolling out new technologies think about confidence levels, think about inbuilt bias

Good example = Boston potholes.

What is the impact on people? Is it proportionate/helpful – after 9/11 profiling algorithms misidentified a US traveller as a terrorist 1500 times a day.

Imagine being that guy!

What you can do

- The best way to make sure you’re ready for the new Bill is to be up to date with your privacy responsibilities under the current Privacy Act
- Become familiar with the privacy principles
- Have privacy in mind whenever you’re looking a new tool or technology
- Put measures in place to mitigate privacy issues
- Take responsibility when issues arise
- Ask OPC for help

OPC resources

- We provide free privacy training modules on our website
- The courses cover a variety of privacy topics, including one that covers privacy in the employment context
- Taking these courses will make sure you’re up to speed and foster a culture of privacy compliance
- If you want to try something new with personal information, do a privacy impact assessment to find out the potential risks
- Recent example from the news; facial recognition technology
- Search “privacy impact assessment” on our website to find our PIA toolkit

- OPC receives about 8,000 general enquiries and 300 media enquiries each year.
- We created AskUs as a search engine to answer privacy questions more efficiently.

- Recently I launched the Privacy Trust Mark.
- The Trust Mark identifies products and services that I consider to be outstanding in the way they manage personal information.
- If you put in the work and take account of privacy values in the design of your product or service, the Trust Mark gives people more confidence to engage with it
- You can find out more about the Trust Mark and how to apply for one on our website.

Conclusion

- This has been a year of dramatic change and development for privacy in New Zealand
- Much of our focus for the future will depend on the outcome of the Privacy Bill, but we are keeping an eye on trends and developments that are affecting privacy on a global scale
- We are holding an International Privacy Forum next month, where privacy experts from around the will discuss GDPR, Cambridge Analytica, artificial intelligence, DNA testing, right to erasure, and more
- The forum will be in Wellington on 4 December 2018.
- Go to privacy.org.nz/int-forum to learn more and register