Citizens Advice Bureau

AGM

Loaves and Fishes Hall, St Paul's Cathedral

Challenges to Personal Information in the Digital Age

Marie Shroff – Privacy Commissioner

Tuesday 27 August 2013

[SLIDE ONE – TITLE]

Introduction:

- Pleased for the opportunity to be here.
- Some insights and updates on Privacy Law and the rapidly evolving information technology environment which it now has to apply to.
- Hope also that you will be able to see how this is directly relevant to your role within your organisation and communities.

[SLIDE TWO – DATA RAIN]

Definition of privacy:

- Privacy law is concerned with information that is about a person – or can be connected to a person (called personal information).
- The Privacy Commissioner cannot look at the use of company or official information, only information about an identifiable individual – a natural person.
- Privacy commissioners exist in most developed countries – and are often alternatively called 'data protection commissions' or similar - expanding in number worldwide in recognition that the protection of personal information is essentially a human right.

[SLIDE THREE – ABOUT US]

How is the Office set up?

- The New Zealand Privacy Commissioner's Office is an independent Crown Entity that was set up in 1993.
- The Privacy Act was passed unanimously.

- PC is appointed by the Governor-General on the recommendation of the Minister of Justice.
- Report to Parliament through the Minister of Justice.
- Funding is from the public purse.
- Independent - can and do investigate complaints against government departments; Ministers of the Crown.
- Excluded from the Act: MPs in his/her official capacity; courts; royal commissions; media; Privileges Committee.
- The Office is free to comment on privacy implications arising in proposed new laws and information matching programmes.
- Also a regulator – power to make industry codes of practice e.g. Telecoms,

[SLIDE FOUR – WATCHING THE WATCHERS]

Personal information

- Information is held about you by businesses, government, health providers.
- There are many databases holding information about you, your income, family, house, education and lifestyle.
- Quite a lot is open to the public – e.g. your birth certificate, marriage certificate, passport and entry on the electoral roll.
- A national health index number links to any information about you held by a hospital, GP, medical laboratory or pharmacy.
- Financially, information relating to income tax, superannuation, insurance and annuity details, information held by credit reporting agencies, such as Bay Corp, and banks.
- Mobile phone records, the video store, the library, the sports club, Ticketek, customer loyalty schemes such as Fly Buys, Trade Me, and your internet service provider to name a few.
- Also if you are a member of a political party or professional association.
- There may be information about you held by the Security Intelligence Service, traffic fine information, or details held by the Police or courts.
- You will have given some of that information voluntarily, and some is required by law. But:
    - what happens to it?
    - how securely is it held? and
    - who has access to it?

[SLIDE FIVE – TECHOLOGY IS CHANGING]

The digital information revolution:

- Technology has transformed the way information is held and used, and it is transforming the way we do business, communicate and socialise.
- Information is stored in computers and likely they are not in New Zealand.
- Recent privacy related developments.

- Google Glass
- Unmanned Aerial Vehicles or drones
- Biometric sensors
- Powerful smart phones
- The cloud
- Social media

[SLIDE SIX – RED RIDING HOOD]

- Change is happening and it affects you:
  - as an individual
  - as a business person
  - as an employee
  - as a parent.

Our 'digital shadows':

- In financial records, on mailing lists, through web surfing histories or images taken of us by security cameras in airports or by CCTV cameras, a digital shadow is being created around us.
- Estimates are that only about half of a person's digital footprint is made by deliberate actions, such as taking pictures, sending emails, or making digital voice calls – the rest accumulates passively as we go about our daily activities.
- With the billowing quantity of personal information created, comes an increasing chance of it ending up in the wrong hands – whether by design or accident.
- Digital universe; borderless world; global context: can't control it.
- Information really is the new "currency" of the 21st century. But not all good. With that comes "privacy pollution". Small incursions building into something big and bothersome and problematic.

[SLIDE SEVEN – PRIVACY TRAIN WRECK]

Current state of privacy in New Zealand:

- 2012 a watershed year for data breaches for the public sector.
- Failures on a number of fronts:
  - ACC – email breach in August 2012 – details of 6700 clients leaked.
  - MSD – unsecured WINZ information booths.
  - EQC – email breach in

- Also in the private sector – Telecom/Yahoo/Xtra breach in February 2013 when the email accounts of 60,000 New Zealanders were compromised.

- Also in recent days, stories covered by the news media:
    - Former employee dismissed by Air New Zealand for misusing sick leave – Employment Relations Authority ruled that she had make her Facebook page and bank account records available.
    - ACC employee who had a notebook stolen in a burglary in Christchurch, endangering the personal information of 35 clients.
    - Gisborne man dismissed after posting photos of himself at a waka festival in Rotorua while on sick leave.

- Evidence of a ground shift in public's thinking – more savvy, more aware, and increasing expectations of reliability and security.
- The current debate on the GCSB Amendment Bill versus civil liberties.

[SLIDE EIGHT – UMR SURVEY]

2012 UMR opinion survey results:

- 88% of respondents said they wanted businesses punished if they misuse people's personal information.
- 97% said the Privacy Commissioner should have the power to stop a company breaching the Act.
- 82% said they were worried about the government silently sharing their personal information.
- General concern about privacy in the past 10 years has risen

[SLIDE NINE – PRIVACY PRINCIPLES]

Some OPC stories:

Example one:

- A woman wanted to take legal action for work undertaken by her local council that had caused damage to her property.
- The council advised its insurance company of the potential legal action. The insurance company arranged for a geotechnical report to be carried out, to try and establish the cause of the damage.
- The woman later asked for a copy of the geotechnical report. The insurance company refused.
- *Principle 6* gives people the right to request, and have access to, personal information held by an agency.
- The insurance company thought the report was not personal information about the woman.
- We disagreed. While the report did not refer to the woman by name, it referred to the "property owner" at a specific address. We considered this was sufficient to identify the woman and it was personal information because the report provided information about the

woman's property, the damage to the property, and had direct implications for her situation.

Example two:

- A woman told us that she had applied for a job as a part-time retail assistant with a large retail chain employer.
- The job application had been completed online on the store's website and she was required to consent to the store carrying out a credit check on her. The woman's application was unsuccessful, and she complained to us that she considered the store's collection of her credit report was unnecessary for the purpose of determining whether she was a suitable applicant.
- We contacted the store, who advised that no credit check had been carried out on the woman. It said that credit checks were only carried out after interviews had been conducted and a preferred candidate for a job identified. It said consent was obtained from every applicant via the online application process for reasons of efficiency.
- We relayed this to the woman who subsequently decided not to pursue the complaint.
- *Principle 1* requires an agency to only collect personal information if it has a lawful purpose connected with a function or activity of the agency, and the collection of the information is necessary for that purpose.
- We did not think that it was necessary for a credit check to be carried out for the position of a part-time retail assistant. Under the Credit Reporting Privacy Code 2004 employers can only access credit information where a job involves significant financial risk to the employer. The store accepted this view, and undertook not to carry out credit checks for sales assistant positions in the future.
- *Principle 3* generally requires that, when an agency collects personal information from an individual, they tell that individual why they are doing so, and what the information will be used for.
- We considered that the store's online application process did not make it sufficiently clear to applicants what personal information was being collected about them and for what purpose, including that credit checks would only be carried out at the end of the recruitment process.
- The shop accepted our views and amended its processes and we closed our file.

Example three:

- A man attended a function run by a community organisation to which he belonged.
- The organisation later received several complaints about the man's aggressive behaviour at the function, including that he had struck another man who had asked him to leave.
- The man asked the organisation for copies of the complaints it received about him.
- The organisation gave him a summary of the complaints, but refused to give him copies because it thought it couldn't do this without identifying who had made the complaints.

- We were satisfied that the writers of the complaints would be identifiable to the man from the details in their letters, even with their names removed.
- It was our view that the organisation could withhold copies of the complaints under a section that allows an agency to withhold personal information if disclosing it would be likely to endanger the safety of any individual.
- We considered that because the man had already struck another member of the organisation and behaved aggressively to others at the function, and there was a real risk that he may act violently if he were to identify who wrote the complaints.
- We formed the view that it would be unwarranted to give the man information about the people who had complained about him.
- The information was withheld according to *Principle 5* and *Principle 11*, and overrode *Principle 6*.

[SLIDE 10 – HOW TO PROTECT YOURSELF AND OTHERS]

Top tips:

- Advise people to ensure the computer/tablet/mobile phone is secure – use passwords for protection and security.
- Advise people not respond to requests for passwords and PIN numbers by phone or email or social media messaging, especially if they come from unknown sources.
- Advise them to avoid unknown or risky websites.
- Remember that genuine business will not pressure people.
- Secure mail and destroy bills safely.
- Encourage young people to use social media wisely.
- Get people to check with others when they are suspicious of online approaches for money or donations or inheritance/lottery winnings.
- Tell people about dispute complaints services.
- Be alert for online scams.

[SLIDE 11 – CON AIR]

[SLIDE 12 – SCAMS]

One type of security breach - scams:

- New Zealanders lost more than 4 million dollars to internet scams in the last year (NetSafe).
- Cyber criminals became better organised and more resourceful.
- The largest losses recorded were to inheritance and government grant-type scams.
- More than 1.5 million dollars was handed over in these schemes.
- The scam which held the previous top spot, romance ploys, fell to No. 2 this year with almost 1.3 million dollars lost.
- The largest number of reports came under the online trading category.
- More than 350 people reported they lost money buying goods online.

[SLIDE 13 – INFORMATION BOOTH]

Access requests - an important right:

- Where an agency is covered by the Act, people are entitled to obtain from that agency confirmation of whether or not it holds personal information about them.
- If so, people are entitled to gain access to that information (Principle 6 of the Act)
- Access requests apply across both business and government.
- Accessing information via a Privacy Act request is similar and complementary to the Official Information Act.
- Contact the agency that's likely to holding the personal information, explaining – via an email or a letter – what is being sought.
- The agency has up to 20 working days to respond.
- If a person doesn't receive the information and is not convinced by reasons given for withholding, they can make a complaint to the OPC.

Citizen's Advice Bureau website:

- Very encouraging that CAB includes comprehensive information about its privacy policy on its website which includes:
- A commitment to protect people's privacy.
- Information about the collection of people's information, what that information is for and how it is stored.
- An undertaking to respect anonymity.
- An undertaking to give people access to their personal information.

International collaboration and GPEN:

- The office collaborates with overseas Privacy Enforcement Authorities.
- Recent Global Privacy Enforcement Network (GPEN) internet sweep by 19 countries.
- New Zealand results show nearly one third of NZ websites have little or no privacy information on their websites and this has to improve.

What the OPC has to do:

- Help people to help themselves – turn them into digital citizens - give them the knowledge and the tools so they can manage their information in the way they want, and self-resolve disputes.
- Encourage businesses and government to get things right before they get things wrong and to make them realise their obligations when looking after people's personal information.
- When things do go wrong, hold them to account for how they handle personal information - both at home and abroad.

[SLIDE 14 – GOALS]

Finally:

- Changes to the Privacy Act will mean the OPC will have greater powers – breach notification, compliance notices, a 'do not call' register, enable class actions and other new measures.
- Our website (www.privacy.org.nz) and our freephone line (0800 803 909) are there to help you. We have guidelines on our website specifically designed to help businesses.
- "The price of freedom is eternal vigilance" (Thomas Jefferson).
- And with summer coming, I thought I'd leave you to ponder on this final cartoon.

[SLIDE 15 – BEACH]