Managing privacy risks in a digital world

Privacy Commissioner John Edwards

RiskNZ presentation

Time: 12.15pm-1pm

Date: Tues, 1 September 2015

Duration: 30 minutes plus 10 minutes Q&A

Venue: Level 9, KPMG, 10 Customhouse Quay, Wellington

Audience: 50-120 per session (many via videolink)

Introduction

Thank you for the opportunity to speak today.

Risk management is an area that my office has had considerable interest in. It is an interrelated core part of the work we do every day, in analysing policy proposals, helping agencies resolve practical privacy problems.

Risk management is the practice of identifying potential risks to your business, and taking the right precautionary steps or strategies to curb or mitigate that risk.

The right strategy is one that is proportional to the risk that you've identified. You'll know that it doesn't make sense to spend a million dollars preparing for a thousand dollar problem.

I'd like to talk to you today about some of the ways that our office can help you build a stronger privacy-proof culture and highlight a number of tools created by my office that can enable your organisations to comply better with the Privacy Act.

Risk management

A starting point for risk management is the risk of litigation.

There have been recent cases before the Human Rights Review Tribunal that demonstrate how increasingly expensive it can be when an organisation gets its risk management strategy wrong.

The cases are specific to privacy risk and the Privacy Act. In the first, a company gets it wrong by not checking the validity of a disputed bill, and in the second, a DHB failed to follow its own workplace harassment policy, and in the third, a business gets it wrong by unfairly disclosing personal information.

Taylor vs Orcon – This case cost the company $25,000 in damages for a $300 disputed bill which should not have been passed on to a debt collection agency. The disputed amount negatively affected Mr Taylor's credit rating and impacted on his ability to find rental accommodation for his family among other things. The Tribunal's decision to award damages to Mr Taylormakes it clear agencies must take adequate steps to check the accuracy of the information before referring it to a debt collection agency.

Watson vs Capital Coast DHB – This case cost the DHB $15,000 after the Tribunal decided that an investigation into a workplace harassment complaint failed to follow the organisation's workplace policies when the complainant was refused information gathered during the course of the investigation. The complainant, a nurse, received the damages award for humiliation, loss of dignity and injury to feeling.

Hammond vs NZCU Baywide – You might know this case as the rude Facebook cake case. A woman complained because her former employer sent a photo she posted to her private circle on Facebook to discourage other businesses from employing her. The amount of damages awarded to the complainant - $168,000 - is ground breaking because it exceeds by a wide margin the previous highest award of $40,000 set in 2003 (Hamilton v The Deanery). It sets a new benchmark for compensating harm caused by a breach of the Privacy Act for unlawfully disclosing personal information.

That's the litigation risks. What about the financial risks to a business?

Nearly two years ago, a retail chain called Target in the United States suffered a massive data breach of customers' credit card data. It's information system was hacked and the information was stolen. It is still paying the financial consequences for the event.

By the numbers:

- 40 million – the number of credit and debit card numbers stolen.
- 70 million – the number of records stolen that included the name, address, email address and phone number of Target shoppers.
- 100 million US dollars – what Target said it would spend upgrading its payment terminals to support Chip and PIN enabled cards - which if it had been done in the first place might have prevented the theft.
- 200 million dollars - the cost to credit unions and community banks for re-issuing nearly 22 million cards.
- 54 million dollars - the income that the hackers likely generated from the sale of two million stolen credit card numbers.
- 67 million dollars - the sum Target has recently agreed to reimburse Visa for costs it incurred – and it is likely to pay a similar sum to Mastercard.

That's the financial cost. What is less easy to quantify is the cost to a business' reputation.

Our state owned insurer ACC suffered a nearly crippling privacy breach a few years ago that badly damaged the public's trust and confidence in the organisation. The personal information was not stolen but disclosed through human error. As you know, what followed reverberated for months. The matter was widely reported and caused others to come forward with other examples involving ACC, resulting in top level resignations.

ACC has since had to work extremely hard to overhaul its processes to restore trust in its reputation. It has been successful in dramatically bringing down the number of data breaches and acknowledges it still has plenty of work to do to regain and maintain public confidence.

Privacy and data protection is now a top priority for ACC.

Making privacy a top priority

Earlier this year, the international technology and market research company, Forresters, predicted 2015 as the year privacy and security became competitive differentiators.

The law firm, Simpson Grierson, recently advised its clients that while last year was all about health and safety, this year data protection and privacy should be on every boardroom agenda.

Organisations worldwide are investing a great deal of resources in getting their personal information and data protection practices up-to-date and ready to deal with emerging privacy threats.

This growing awareness of privacy risks is also reflected in our public opinion polling.

New Zealanders are more and more concerned about the protection of their personal information. The public is increasingly aware and concerned about privacy, especially personal information collected and held by organisations.

One in two New Zealanders say they are becoming more concerned about privacy issues. This is the highest yet recorded level in our surveys dating back to 2001.

Four out of five New Zealanders say they are concerned about the security of their information on the internet.

There's also increasing awareness that government is not the only big player collecting personal information - with concerns about personal information held by businesses and online service providers.

Case example: Ashley Madison data breach

Here's a very a recent example of what happens when things go drastically off-road in privacy risk management.

All of you are probably familiar with what happened to the dating website Ashley Madison. If there ever was an agency that should make privacy the very bedrock of its business, it is this one.

A hack of Ashley Madison a couple of weeks ago has reportedly put the personal information of 37 million users around the world at risk. Many thousands of New Zealanders are also said to be caught up in the breach.

The hacker - or hackers – has since dumped 9.7 gigabytes of customer records on the Dark Web. These include profiles with all the customers' secret sexual fantasies

and matching credit card transactions, real names and addresses, and employee documents and emails.

This is worrying news for anyone who used the service – and for Ashley Madison's parent company, Avid Life Media, which was preparing a 200 million US dollar initial public offering later this year.

Putting moral judgement aside, even the users of Ashley Madison are entitled to the promise of privacy that the website has clearly failed to guarantee.

When asked in an interview before the breach "in what area would you hate to see something go wrong?" the company's chief technology officer had answered - "security".

Take for example Ashley Madison's full delete feature. When a customer was finished with the service, for a payment of 19 US dollars, the website offered to completely scrub the person's payment and address details from its records.

But the hackers showed that this wasn't the case for those that paid for the full delete feature; purchase details could still be found in the servers used by the company.

And because nearly all the transactions were carried out using credit cards, the information included real names - even though many people would have used pseudonyms for their online profiles.

So what could the company have done better?

For starters, it could have applied the principles of Privacy by Design when setting up its service.

Privacy should have been its default setting. Users should not have to select privacy-enhancing features – they should automatically exist as the underlying standard. The full delete function should have been available at no extra cost.

Another default setting should have been encryption. The data in Ashley Madison's servers should have been scrambled to ensure that if it was breached, all a hacker would see is meaningless code.

With hindsight, we can say the customer data should have been encrypted or at least anonymised and connections between the dating data and billing data made less accessible.

Ashley Madison's problem is a fundamental one that it failed to address until it was too late. From the very beginning, it should have interrogated everything it did as a potential security problem.

Instead it modelled and engineered itself on hundreds of online retail websites – even though its users could potentially be exposed to greater degrees of harm because of the nature of the personal information it held.

By adopting an inadequate model, the company set itself up for an inevitable breach – one that could cost as much as its parent company's estimated 200 million dollar proposed public offering.

The key lesson is that if you don't invest in prioritising and protecting privacy at the very beginning, the price you pay could be a lot more when playing catch up. And that price may even be your entire business.

Vision

As I've only given you examples of privacy risk management fails, what then might success look like?

My vision of making privacy easy is aimed at compliance for government and business; easy option for consumers to chose; easy for people to access effective remedies when things go wrong.

We've developed some tools to help with this:

- interactive online training resources
- an online directory of privacy professionals
- privacy enhancing tools, like a privacy impact assessment toolkit
- a focus on communicating key messages in the digital space
- online lodgement of privacy complaints.

Engaging online

I've changed the way our Office works, by engaging and interacting more with people online and through our website.

This means using our blog, Twitter, YouTube and Facebook channels.

I want to help your organisations deliver on your Privacy Act obligations and I want to do this without compromising your other obligations by making sure privacy is present in the training, culture and values of your organisations.

Information privacy principle 5

How many of you are familiar with the Privacy Act and its 12 information privacy principles?

The Act is based on 12 information privacy principles which themselves are based on OECD privacy principles. Each principle governs different aspects of how an agency manages personal information – including collection, notification, correction, access and disclosure.

They work together in representing stages in the life cycle of information. Information is collected, used, stored, disclosed and eventually, disposed of.

From a risk management perspective, one that may be of interest to you is principle five.

Principle 5 says an agency that holds personal information shall ensure that the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against:

- loss; and
- access, use, modification, or disclosure and other misuse

The key word in that definition is the word reasonable.

What security safeguards are reasonable in the circumstances?

In the case of Ashley Madison, clearly the threshold of reasonableness is very high, as it is for government agencies, banks, insurers and health providers.

That’s because the risk for harm to a person is also high – if that person’s personal information is disclosed.

And you can argue that the larger the potential for harm to individuals, the higher the risk to an organisation in terms of reputation, lost custom, legal costs, and eventually, compensation and damages.

By assessing the data privacy implications of new products, services and other activities from the perspective of possible negative impact on individuals, the aim should be to reduce the likelihood of serious harm.

Privacy impact assessment

What tools then are around for businesses to turn this harm-based approach to privacy risks into concrete action?

If you’re going to adopt a new data management system – whether it is in the cloud or otherwise - you need to do a comprehensive review of its privacy implications - not just into how it works, but how it will be used.

A Privacy Impact Assessment - or PIA - is methodology that you can use to flush out any latent privacy risks in a new project.

Then you can assess each risk and determine which steps you need to take in order to deal to them.

By running a PIA at the start of a project, you can avoid the time and potential expense of data breaches in the future.

We have developed a PIA toolkit to help with this process. The new toolkit is divided into two parts:

- The first part helps you determine whether you need to do a PIA.
- The second part walks you through the process of actually doing one.

Finding and managing privacy risks ahead of time is much easier than dealing with the fallout later, particularly if fixing a privacy risk involves changes to your system.

It’s much easier to change a system as you implement it - rather than make changes once it’s entrenched in your organisation – see Ashley Madison.

Making a privacy statement

Last year, my Office published our ‘Making the Future’ technology strategy. When we talked to people about the strategy, they asked for simple privacy tools to assist them. If you’re interesting in reading our Making the Future document, you can find it on our website.

So that’s what we have begun to do – make simple privacy tools to help people comply with their privacy obligations.

We launched one of these tools in June - the Priv-o-matic privacy statement generator which is designed to help generate ‘principle 3’ statements.

As I mentioned earlier, the Privacy Act has 12 information privacy principles.

Principle 3 is the obligation to let people know what information is being collected, how it is collected and who is collecting the information.

A principle 3 statement let customers know clearly, and in plain English, what’s going on with their information.

When you use our Priv-o-matic, you might notice that it doesn’t generate the fully fledged often extremely long and legalistic privacy policy you often see used on websites.

What it does produce is a minimal compliance statement that you need to show people when you collect their personal information.

It is targeted at the small to medium size business to use, so don’t expect it to be able to create a privacy statement for an organisation the size of Fonterra.

In a marketplace where there is little difference in price for the good or service, a simple, clearly explained privacy statement can help to differentiate your organisation over another one.

We see examples of this trend around the world – take for example Apple and Facebook.

Although both have come under criticism at times for the way they have handled customer data, both now offer products and features directly responsive to

marketplace calls for easily accessible privacy options and security, including encryption.

Some thoughts about spreadsheets

I recently gave a presentation in Christchurch and one of the questions I was asked was if there's one thing I could tell an organisation to do to protect itself against a data breach, what would it be?

The answer: Don't use spreadsheets unless you absolutely have to.

If you want to engineer a really good privacy breach, do it by grabbing all your customers' data and put it in a poorly-secured Excel document. Combine this with a lax approach to data loss prevention, and someone in your office will eventually, accidentally, email it out to somebody who shouldn't have it.

If you hold large amounts of personal information and you're using spreadsheets to collate it all, you're opening yourself up to user error and possibly breaching your obligations under the Privacy Act.

In the data breaches reported to us involving spreadsheets, the numbers of individuals affected per breach has ranged from dozens to thousands.

While some of the systems involved had data loss protection or security procedures in place, there were holes and user error always finds a way.

If you have to maintain a database, you should be thinking about a purpose built database management system. This approach can also help lay the groundwork for a more customer-driven solution to accessing records.

It's not always going to be an appropriate solution, but letting the customer access their own information through a web service will minimise the chance of them being accidentally emailed their information along with 900 other customers' details.

And if you must use spreadsheets, don't email them around. Export the data you need from the spreadsheet and just send what you need. Convert the sheet to PDF or put the data directly into a table in the email if it's a small enough set.

Finally, if you absolutely need to email a spreadsheet to someone, protect it with a password.

When it comes to solutions, what you really want is to create a culture where people think about what they're sending and where they'll regularly check the addressee details and the attachment contents.

Grow a culture of awareness

Effective privacy risk management depends on having solid organisational support and structure. One of the foundational elements effective risk management is to have an organisational culture that has good levels of awareness.

That awareness encompasses:

- an understanding of the way your organisation uses personal information
- an understanding of the 'information lifecycle'
- an appreciation of typical areas of legal risk
- a willingness to consider mitigating strategies and effective remedies when things go wrong.

Awareness can be a tough thing to develop across a complex organisation.

Online privacy training

One of the key roles that my office plays is education. We have education for both organisations and consumers and we provide it online and for free.

Our online privacy training modules were launched earlier this year and there are currently three modules – Privacy 101; Health 101; and one on government Approved Information Sharing Agreements.

The next module will be on Privacy Impact Assessments - with others to follow on data breach notification, positive credit reporting, and frontline staff.

If you and your colleagues want to get up to speed with aspects of the Privacy Act, I encourage you to work through our online privacy training modules.

The online modules are free and take about two hours each to complete. They can also be completed in stages – each one will allow you to stop at any point and to continue later from that point.

Law reform

The Privacy Act is now over 22 years old - drafted and enacted before the Internet became our default and ubiquitous means of communications.

The government has recognised the need to reform our privacy law to bring it up to date. Reform has been a long process which began with a thorough review of the Privacy Act by the Law Commission that was completed in 2011.

The commission has recommended strengthening the Act in a number of key areas. The main recommendations include:

- giving the Privacy Commissioner the power to issue compliance notices, and, where there is a good reason for it, to require an audit of an agency's information-handling practices;
- streamlining the complaints process under the Act, including giving Privacy Commissioner the power to make binding decisions on complaints about people's right to access their own personal information; and
- mandatory breach notification if the breach is sufficiently serious;

A law change in the area of breach notification would be a significant game changer. Why? Because it shifts business expectations and creates a level playing field for all across the public and private sector.

The time frames for legislative change are uncertain. So, in the meantime, we are making robust use of the enforcement tools we currently have as a regulator.

For instance, we have formulated and publicised a policy on naming agencies that in our view deliberately, systematically or consistently flout the law. We have stated that we will be more proactive in naming non-compliant organisations and have clarified the conditions under which that may take place.

Conclusion

As a privacy regulator and an enforcer, here's a checklist of some of the sorts of things that I will be looking for in the event that things go wrong (think Ashley Madison again):

- 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 we are investigating a complaint against your organisation, these elements will become relevant and if your organisation has got its privacy mix right, it will reflect well on your organisation.