Being a modern privacy regulator: using digital tools to make privacy easy

Presentation by Privacy Commissioner John Edwards

ISACA – Information Systems Audit and Control Association

3 August 2015

Christchurch

Introduction

We've been hearing a lot about the death of privacy.

If media reports are to be believed, privacy has been dying a death by a thousand cuts through new technological changes and the collection of internet and communications metadata.

But in truth, people have been heralding the death of privacy for forty or more years - like this Newsweek cover story from 1970.

I've always maintained that privacy isn't dead because we care so much about the future of privacy.

Privacy isn't dead because it still matters.

There is a long term trend in our public opinion polling. New Zealanders are becoming more and more concerned about the protection of their personal information.

New Zealanders are increasingly aware and concerned about privacy, especially information held about them by government agencies, by businesses and online providers.

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.

Another theme that has emerged is a feeling of lack of control:

- 37% do not feel in control of the way businesses use their information.
- one third of New Zealanders say they do not feel in control of the way government agencies use and protect their information.

Focus group participants made striking comments about interacting with government.

"You don't have a choice because if you want to get what you want then you have to share your information and hope they won't release it."

"I think you are basically stuck there because you are in a position where you need to give them the information if you want their service."

There's also increasing awareness that government is only one of the players collecting personal information with increasing concerns about personal information held by businesses and online service providers.

Vision

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.

Here's how: by developing interactive online training resources; a new online directory of privacy professionals; creating privacy enhancing tools, communicating key messages in the digital space, and enabling people to lodge privacy complaints to us online.

Communication

We are taking more steps to communicate this vision and to build of build public confidence in the role the Office plays in safeguarding personal information.

We've got to tell people what we are doing, so that agencies can learn from the way we resolve complaints and know about the contribution we make to policy projects.

People need to have good information about their rights, the limits on those rights, and what to do if things go wrong.

And we also want to be on the spot to help business make privacy work for them.

Engaging online

One of the ways I've changed the way the Office works is to engage and interact more with people online and through our website.

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

The Privacy Act is your guide to protecting personal information – it ensures that the security of personal information is part in parcel with complying with your overall privacy obligations and responsibilities.

Today I want to talk about how you can deliver on your Privacy Act obligations without compromising your other obligations by making sure privacy is present in the training, culture and values of your organisation.

I also want to show you how we can help and to tell you about a number of free online tools that are available to help bring your organisations privacy and data protection practices up to speed.

Making privacy a top priority

Let's begin by taking stock of the growing global awareness about privacy risk management.

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 future-facing.

Ashley Madison data breach

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

Some of you may already be familiar with what happened to the dating website Ashley Madison.

If you're not aware of it, Ashley Madison is a hook-up website for people in relationships who want to cheat on their spouses.

If there ever was an agency that should make privacy the very bedrock of its business, it is this one.

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.

A hack of Ashley Madison a couple of weeks ago has reportedly put the personal information of 37 million largely American and Canadian users at risk.

The hacker - or hackers - has threatened to reveal all customer records, including profiles with all the customers' secret sexual fantasies and matching credit card transactions, real names and addresses, and employee documents and emails,

This is terrible news for anyone who has 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.

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 is finished with the service, for a payment of 19 US dollars, the website offers to completely scrub the person's payment and address details from its records.

But the group or individual that hacked the website says this wasn't the case for those that had paid for the full delete feature – their 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 most people had used pseudonyms for their online profiles.

As one security engineering manager at a cyber security firm observed:

"Dating site users are likely to feel more violated after a breach than those caught up in a retail or government website breach and they are less likely to reach out for help and advice on how to manage their identity information after a breach."

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 ideally have been its default setting. Users should not have to select privacy-enhancing features – they should automatically exist as the underlying standard.

It's interesting to see the website included data protection as part of its marketing – you can see here it advertises a SSL site certificate.

But Ashley Madison seems to have overlooked security in its servers. The data should have been strongly encrypted to ensure that if it is obtained by a hacker, all they 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.

Because of the nature of the service it provided - i.e. enabling infidelity - the website – to be successful - had to claim it offered genuine privacy and market its privacy-protected qualities.

But 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 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 maybe that price could even be your entire business.

Information privacy principle 5

As many of you are auditors of information systems, I hope you will already be familiar with information privacy principle five of the Privacy Act.

It is one of 12 information privacy principles – each one governing different aspects of how an agency manages personal information – including collection, notification, correction, access and disclosure.

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 for reasonable 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 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.

Taking a harm-based approach should improve the ability of privacy officers and businesses to adopt a structured approach.

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.

Samsung, for example, would have benefited from taking such an approach to its new Smart TV which was revealed to collect people's conversations – much to the company's embarrassment, and something they were forced to address.

Privacy impact assessment

What tools then can be developed for businesses to turn this harm-based approach to privacy risks into concrete action?

One such aid is our new Privacy Impact Assessment toolkit.

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.

Our new PIA 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.

Take for example cloud storage solutions because lots of medium and large organisations – such as local governments – are moving or have moved towards the cloud.

My view is that the cloud, in and of itself, is no more or less prone to privacy breaches than any other solution.

This is not to say that it is infallible, just as other solutions are not infallible.

Data breaches happen with alarming frequency in the offline world and there's nothing inherently safer about the online world.

The leak of personal photographs of Hollywood celebrities prompted much discussion about the potential vulnerabilities of the cloud.

Undertaking a Privacy Impact Assessment if you are considering a cloud storage option is an excellent way of assessing risks and benefits.

ISO/IEC standards

There's been a lot of timely work that's been done on ISO/IEC standards as international benchmarks that ensure cloud providers offer suitable information security controls and governance.

Until fairly recently, ISO/IEC standards addressed information security management without specifically addressing the growing cloud computing component.

But the newer ISO/IEC cloud computing standards – 27017 and 27018 which are supplementary to 27001 and 27002 - offer information security advice and assurance for *both* cloud service customers and cloud service providers.

ISO/IEC 27018 includes public cloud service providers as data processors if they process personal information for and according to the instructions of a cloud service customer.

Organisations that demonstrate compliance to ISO/IEC 27002 - and which extend that compliance in accordance with ISO/IEC 27018 - will help bolster customer confidence in the protection of personal data in cloud computing.

The increased consumer trust that will flow naturally from the adoption of ISO/IEC standards on information security will have positive spinoffs for business and profitability.

Increasingly, customers are going to seek privacy and security. These factors are becoming significant business differentiators.

In an age where with a few mouse clicks or a telephone call, consumers can switch power companies, banks and mobile or internet providers, a loss of confidence due to a data protection error can lead to a migration away from the company, and a subsequent loss of shareholder value.

I know I'm labouring this point but being careless or complacent with personal data has financial and economic implications.

Transparency reporting

Another area of increasing consumer confidence is transparency reporting – something my office has devoted considerable resources in working on recently.

Transparency reporting is an important development in helping consumers understand what happens to their information.

As it happens, information about people is of considerable interest to law enforcement agencies which have powers to compel organisations to hand over that information.

Many types of businesses hold large databases of personal information. These include:

- cell phone providers
- large customer loyalty card programmes
- banks; and
- utility companies.

Up to now – Trade Me being one of the notable exceptions – not many companies publicly report the number of requests for personal information they get from the Police, IRD, SIS and other agencies.

I singled out Trade Me because for the past three years it has been reporting the number of requests it receives and complies with.

Trade Me also has a story to tell about how one Inland Revenue request for user information potentially involved 1 million people but Trade Me was able to redefine IR's search criteria and reduced that number to 40,000 – something that benefited both organisations in terms of public perception and workload.

Transparency reporting can have real benefits for individual privacy, including:

- encouraging requesting agencies to make sure they are using their coercive powers proportionately
- giving consumers more insight into how companies are using, protecting and disclosing the personal information they hold
- giving the public insight into the range of government agencies with statutory powers to request information; and
- encouraging companies to improve their processes for handling requests, particularly those that are broad or ill-defined.

By getting real information out there, we also think that transparency reporting is helpful in terms of responding to public concern about the use of government information gathering powers.

This slide is an image taken from an art installation called Secret Power by a New Zealand artist Simon Denny who exhibited it at the world art fair, the Venice Biennale, this year.

Secret Power takes the New Zealand connection with Five Eyes and the NSA in particular as its theme.

I see this as another manifestation of public concern about surveillance by the government and other governments.

Transparency reporting is helpful for companies because it allows them to compare themselves to their competitors in terms of how they handle requests for information.

To support and encourage the growth of transparency reporting in New Zealand, we are planning a trial of public reporting by companies about requests for information from government agencies for law enforcement or national security purposes.

We will ask companies to provide their data to us in a way that allows for comparisons between companies and sectors. We will then publish this data in one place.

Why is it important that this kind of report comes from us?

- First mover disadvantage - companies that do report may experience an initial drop in customer trust as they reveal the requests from law enforcement agencies that they have complied with, where customer had previously been unaware of this.
- Each company taking its own approach leads to poor comparability - and if companies do not report the full range of information a misleading picture may be presented.
- Consumers don’t know what they don’t know, so there may not be customer pressure for transparency reporting until a certain critical mass has been reached.
- Companies may not be sure what they can report and may fear legal repercussions. We can help by clarifying the legal position on what information can be reported.

We’ve made an initial approach to a range of companies, and the response has been positive so far.

But this is a pilot, and it's the early stages so we're looking for feedback.

Making a privacy statement

Last year, my Office published our 'Making the Future' technology strategy.

It is available on our website if you want to read it.

When we talked to people about our 'Making the Future' strategy last year, they asked for simple tools.

We launched one of these tools in June - the Priv-o-matic privacy statement generator.

The Priv-o-matic is built 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 will help to differentiate your organisation over another one.

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

Although both have come under criticism at times for privacy issues, both now offer products and features directly responsive to marketplace calls for easily accessible privacy options and security, including encryption.

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.

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 are currently three modules – Privacy 101; Health 101; and now, 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 want to get colleagues in your organisation up to speed with aspects of the Privacy Act, I encourage you to let them know about our online privacy training modules.

The online modules are free and each of them can be completed in stages – each one will allow you to stop at any point and to continue later from that point.

Law reform

The topic of my presentation this evening refers to being a modern regulator.

It’s a reference to how long we’ve been working with the current Privacy Act which is now over 22 years old.

The Privacy Act was drafted and enacted before the Internet became our default and ubiquitous communications network.

The 12 information privacy principles are ‘technology neutral’.

That means they are adaptable to a privacy environment where technology is constantly evolving.

But while these principles are enduring, the government has recognised the need to reform our privacy law to make it more future facing.

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;

Already we are seeing voluntary data breach notification being adopted in NZ – especially with larger corporates and government departments.

A law change in the area of breach notification would be a game changer.

Why? Because it shifts business expectations and creates a level playing field for all across the public and private sector.

The government has signalled it may introduce the law change this year or next year.

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.

Since I've been Privacy Commissioner, we named one agency and come close to naming another.

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.