Privacy Issues Forum
Keynote Address

Privacy and community: personal space within the public sphere

Privacy Commissioner, Marie Shroff

27 August 2008

Introduction

I would like to extend a warm welcome to everyone here today. I am sure it will be a stimulating and rewarding day. We have attendees from a number of government agencies, especially health agencies, and a range of business areas – including information technology, law, banking and insurance. We also have representatives from community agencies, unions, and academia. All of us contribute in different ways to the lively and wide-ranging debates that swarm around privacy. We are a key part of the operational privacy community. We are organisers or agenda-setters and all of us, in one way or another, are practitioners. We have a wealth of expertise within this room. I hope today you will find something from the smorgasbord of topics on offer that appeals to your professional privacy palate!

Community – personal space in a public sphere

You will see behind me a looming apparition. It is a representation of my "digital shadow." And, whether you realise it or not, you have one too! Your digital shadow is all the digital information silently generated about you on a daily basis. The quantity of that information now surpasses the amount of digital information you have actively created yourself.

We are all participants, whether willingly or unwillingly, in this “digital century”. For example, 78% of us use the internet; 53% do online banking weekly. We are experiencing an “information revolution”, but are we in the middle of it; or just at the start? Where will it end up? With technological progress has come changes in the nature of information and the value of it.

There can be no doubting now, the huge commercial value that there is in personal information. The internet is a key part of that. In fact, one of the business delegates at the recent OECD conference on the future of the internet put it much more strongly, when he said, “Don’t talk about the ‘*internet* economy’ just talk about ‘the *economy*’ “.

There is much to be gained commercially from exerting control over personal information – and on the other hand – much to lose in dollar terms when control is

wrested from a business. For instance, in recent weeks, Google (which owns YouTube) was ordered by a US judge to hand over a database about online viewers and the videos they watched, to competitor, Viacom. Simon Davies, director of Privacy International in London said at the time: "The chickens have come home to roost for Google. If they were going to unnecessarily keep this information, there was always the chance that someone was going to grab it." A US retailer that lost details of 45 million credit cards recently estimated this cost them a $168 million hit on their bottom line.

The value of personal information stored online is in part due to the ease with which vast quantities of data can be amassed, accessed and manipulated. Your information is a honey-pot. And it can be a case of snatch and grab. So how do we limit the harms and maximize the freedoms in that freewheeling space that is rapidly becoming the operating platform for our banks, governments and major businesses?

Managing our data in common

Regulating cyberspace is an activity that has produced much heat – and soon I hope some light. We are faced with a borderless, digital universe, which is global in context. Personal information is flying every-which way. Simply, we can't really control it; certainly not by using domestic legislation in an uncoordinated way. Yet there is growing recognition that there is a need for some form of regulation. We may all be affected, but none of us has ultimate control, or even a majority share.

The communal character of the internet has led to suggestions that it should be treated as a new type of "commons"; and that regulation should reflect that.[1] A "commons" is something that is close to a public good, but also has some qualities of private property. (Other examples might be certain sorts of intellectual property, or international air quality.)

"Cloud computing"

We no longer sit and type contentedly at our standalone computer. Most of us use the internet daily in our professional lives, and regularly in our personal lives, to find out information or to email others. Beyond that, an increasing number of us will bank online, may choose to store our medical records with Google (although I think I won't!) and may use a website, rather than a hard drive, to store our digital photos. Perhaps we keep our CV on another website and store our personal contacts and

[1] *The Economist,*"Commons sense", 31 July 2008. "The concept of the commons is also spreading to new areas. Their essential feature is that they share one characteristic with private property and one with public goods. Like public goods, they are not "excludable": the common resource is too extensive to keep people out very easily. But they are also "subtractable" (or "rivalrous"), like private property: if one person uses them, another's access is diminished."

address details using another online application. This latter cluster of activities can be classed as computing in the "cloud". "Cloud" computing has been defined as[2]:

> [A] networked collection of servers, storage systems, and devices – to combine software, data and computing power scattered in multiple locations across the network.

Cloud computing has also been described in graphic terms as the "neutron bomb" of the internet. We might debate how extensive those changes will actually be. But there seems little doubt that our privacy, information security and our digital identity will be altered in significant ways by the technological shift that is occurring:[3]

> It may very well be that our fundamental ideas about identity and privacy, the strategies that we have collectively pursued, and the technologies that we have adopted, must change and adapt in a rapidly evolving world of connectivity, networking, participation, sharing, and collaboration.

The wider community – international developments

So how are we tackling the borderless, digital cloud? In this climate, international links are becoming vital. We often think of privacy as being about individual action and repercussion – and of course that is true. But more and more, data protection and privacy are forged across organisations, regions, nations, – even continents. There is a very good reason for that – we are charging our way into the digital century and international cooperation has become essential to address emerging challenges we face. Luckily, the privacy and data protection arena has always been one which has fostered friendly alliances. Our big, annual, international conference of privacy and data protection authorities is a good example of that. Privacy Awareness Week itself is an Asia-Pacific activity and is growing all the time – to include Canada and Korea next year.

I would like to outline some of the recent co-operative developments that affect New Zealand.

AUS-NZ MOU

The Australian and New Zealand privacy commissioners will this week sign a memorandum of understanding to help us cooperate to protect our citizens.

The agreement reinforces the already close ties between our Offices in tackling emerging privacy challenges. Many information-based businesses such as banks and credit reporters are "trans-Tasman". It makes sense for their watchdogs to talk

---

[2] A. Cavoukian, Information and Privacy Commissioner of Ontario *Privacy in the Clouds: A White Paper on Privacy and Digital Identity: Implications for the Internet.* (Office of the Information and Privacy Commissioner, Ontario, May 2008) 5. See: www.ipc.on.ca/index.asp?navid=46&fid1=748

[3] A. Cavoukian, Information and Privacy Commissioner of Ontario *Privacy in the Clouds: A White Paper on Privacy and Digital Identity: Implications for the Internet.* (Office of the Information and Privacy Commissioner, Ontario, May 2008) 3. See: www.ipc.on.ca/index.asp?navid=46&fid1=748

to each other. The agreement is a practical example of how the recently released OECD Guidelines on Cross-border Cooperation in the Enforcement of Law Protecting privacy can be met.

We are right in the midst of the APEC Privacy Pathfinder project, which I will mention shortly, and the MOU supports that effort. In fact, the MOU has been adopted as a model for a similar agreement proposed for APEC.

IAPP

Like all new and challenging areas, professionalism is needed. And so, on a regional scale, I wanted to draw to your attention the International Association of Privacy Professionals, or IAPP. The IAPP was founded in 2000 to define, promote, and improve the privacy profession globally. It is the world's largest association of privacy professionals. Based in York, Maine, U.S.A., the organisation represents over 5,000 members from businesses, governments and academia across 32 countries. It provides a forum for professionals working in the privacy field to share best practice, track trends, advance privacy management issues, and provide education and guidance.

Importantly, the IAPP is responsible for developing and launching the first broad-based credentialing programme in information privacy, the Certified Information Privacy Professional (CIPP), which has international recognition.

Today is the Australasian launch of IAPP. You can find out more information about IAPP and the certification programme at https://www.privacyassociation.org/

OECD

And on a larger scale again, there are global initiatives involving both APEC and the OECD. In Korea in June this year the OECD held a Ministerial Meeting on the Future of the Internet Economy, where participants agreed on the need for government to work closely with business, civil society and technical experts.[4]

APEC Asia-Pacific Privacy Initiative

APEC is running a number of practical pathfinder projects on privacy. These include:[5]

- Guidelines for accountability (project 2) – focussing on the use of "trustmarks" or "seals" – or other forms of accountability for government agencies.
- Cross-border enforcement cooperation (projects 5, 6 & 7) – focussing on the management of complaints between agencies and agreements between regulators.

[4] The Seoul Declaration is available at www.oecd.org.

[5] See also Nigel Waters "The APEC Asia-Pacific Privacy Initiative – a new route to effective data protection nor a trojan horse for self-regulation?" Privacy Laws and Business 21st Annual International Conference, 8 July 2008, Cambridge, UK.

APPA

There is strong regional cooperation through the APPA forum (Asia-Pacific Privacy Authorities). APPA members are involved in standard setting; research; education; PAW; common standards for case notes; MOUs on complaint handling.

Asia-Pacific model

The Asia Pacific model of regulation is typified by light-handed regulation; principles-based laws, covers public and private sectors and provides for individual rights and redress. One of its strengths has been its flexibility for particular contexts (e.g. by codes of practice in New Zealand, Hong Kong and Australia). The Asia-Pacific model is based on (or highly influenced by) OECD approach.

It is significant too, that the Asia-Pacific model has influenced the nature of the APEC privacy framework. There is a similar standard of protection and underlying concepts to European law, and yet with a lighter, more flexible, regulation.

We are likely to see much change in the coming few years. For instance:

- Modernising of existing national laws. There is comprehensive law reform work occurring in Australia and NZ at the moment, and the likelihood of many new privacy laws throughout the region.
- APEC developments will continue (major work ongoing on implementing Cross Border Privacy Rules and in the area of cross border enforcement cooperation).
- We might expect greater cooperation amongst regulators (e.g recent coordination of approaches to security breach notification).
- Even in Europe, the home of privacy law since the 1980s, moves are afoot to re-examine the privacy principles to see if they can deal with the information revolution and the digital cloud.

Technology and connectedness

New Zealanders are enthusiastic adopters of new technology, and recent research backs that up. The Broadcasting Standards Authority (BSA) surveyed New Zealanders about their use of media earlier this year.[6] The results show that New Zealanders are confident users of technology:

- 88% of households have a computer
- 62% of children aged 6-13yrs use the internet.

And similarly, the New Zealand World Internet Project surveyed 1430 New Zealanders about their use of, and attitude to, the internet. It found:

[6] Broadcasting Standards Authority (BSA), *Seen and Heard: Children's Media Use, Exposure and Response* (May 2008). See www.bsa.govt.nz (Research undertaken by Colmar Brunton.)

- 78% of New Zealanders use the internet
- 61% of those surveyed thought it would be a problem if they lost access
- Every week, 28% participate in social networking sites like MySpace of Facebook.

Technology development and impact on society

We are in the midst of an information revolution – largely fuelled by technology. Technology enables details about individuals to be collected, used and disclosed on an unprecedented scale, both in New Zealand and overseas. Clearly it's an area of huge opportunity for growth and development – both to facilitate existing, and to generate new business opportunities; but it's also an area where there are huge risks:[7]

> Our digital footprints and shadows are being gathered together, bit by bit, megabyte by megabyte, terabyte by terabyte, into personas and profiles and avatars – virtual representations of us, in a hundred thousand simultaneous locations. These are used to provide us with extraordinary new services, new conveniences, new efficiencies, and benefits undreamt of by our parents and grandparents. At the same time, novel risks and threats are emerging from this digital cornucopia. Identity fraud and theft are the diseases of the Information Age, along with new forms of discrimination and social engineering made possible by the surfeit of data.

Our notions of privacy are fast-developing in response to these wider societal changes. And our expectations of privacy are evolving as well. We are no longer tolerant of party lines on telephones, or poor handling of medical records. In today's world, what you do with a person's information does matter. We want to have the choice whether to "opt out" of telemarketing calls, or to have a say in what information is released about us. We recognise that there are dangers in taking a overly casual approach to personal information and expect government and business to treat it with care. And yet, we are surveilled, tracked and monitored. We are watched and recorded like never before. How many of our grandparents would have believed that an employer could require a urine test; or a finger-scan; or that a baby born today would have its DNA held for decades – maybe centuries – in a database?

We easily forget that enormous data breaches – as have been experienced in the US and UK recently (the latest one just last week) – are new challenges. Identity theft and fraud is a real and growing issue. There was much publicity last year about the massive theft of credit card details from US retailer TJX and others. There is a huge ripple effect. The theft is thought to have affected over 45 million cards, and

[7] A. Cavoukian, Information and Privacy Commissioner of Ontario *Privacy in the Clouds: A White Paper on Privacy and Digital Identity: Implications for the Internet.* (Office of the Information and Privacy Commissioner, Ontario, May 2008) 3. See: www.ipc.on.ca/index.asp?navid=46&fid1=748

some banks now estimate that it is closer to 100 million. Strikingly, US Attorney, Michael J. Sullivan said the thieves were not computer geniuses, but were just opportunists, who looked for accessible wireless internet signals to hack into the retailers' networks. At a press briefing earlier this month, Secretary of the U.S. Department of Homeland Security, Michael Chertoff said that the charges "… are a reminder of … the fact that each individual's greatest asset is their names, their identity."

Within the last week, a hacker successfully breached the IT defences of the Best Western Hotel group's online booking system and sold details of how to access it through an underground network operated by the Russian mafia. The attack scooped up the personal details of every single customer that has booked into one of Best Western's 1312 continental hotels since 2007. The stolen data includes a range of personal information including home addresses, telephone numbers, credit card details and place of employment.[8]

So bigger doesn't always mean better. And while technology is a solution, it can also be a problem. Therefore, data protection and privacy have become a business issue – which can be a facilitator, an enhancer, and enabler – if you approach it right. If not, it can be your downfall. Accidents cause loss of trust, branding damage and ultimately endanger your bottom line. So, how are we in New Zealand doing?

Launch of UMR privacy survey: Public attitudes to technological change

With our new survey,[9] we tried to test some of the perceptions and trends about personal information and privacy – particularly in health and business and new technology. The results give some clear messages to both business and government about where New Zealanders' concerns lie. Many of you will be interested in the detail of this survey, which is now on our website.

General trends

The results show that many New Zealanders have a strong and growing awareness of privacy and information technology issues. A third of people surveyed (32%) reported that they had become ***more*** concerned about issues of individual privacy and personal information in the last few years. (64% said their concern had stayed about the same.) Pacific Island and Maori respondents showed relatively higher levels of concern (46% and 40% respectively). This is a consistent feature of our survey – similar levels recorded in 2001 and 2006.

Business

The survey results again showed high levels of concern about potential breaches of

[8] To read the complete article (24 August 2008) see:
http://www.sundayherald.com/news/heraldnews/display.var.2432225.0.0.php
http://www.telegraph.co.uk/news/uknews/2613095/Hackers-steal-details-of-millions-of-Best-Western-hotel-guests.html
http://www.ptinews.com/pti%5Cptisite.nsf/0/92DB9DF6977BE4B8652574AF002EDCA4?OpenDocument

[9] Previous UMR privacy surveys were run in March 2006 and September 2001.

individual privacy by business. Ninety-percent (90%) of people said they were concerned (74% very concerned) if ***a business they didn't know*** got hold of their personal information. This concern is reflected across all age groups, occupations, and personal income, and is demonstrated with great clarity in the ethnic breakdowns, where Pacific Island people and Maori expressed 100% and 93% concern respectively. The lowest level of concern was among students (81%).

Eighty-six percent of respondents were concerned if information supplied to a business ***for one purpose was used for another purpose***.

A new question showed that New Zealanders are not necessarily comfortable with the globalisation of personal information. Eighty-one percent (81%) of respondents were concerned with their personal information being held by overseas businesses and, out of that number, 61% were very concerned. Concern was somewhat higher among women (85%) than men (77%).

Trust

Levels of trust in the way different organisations use and protect personal information vary widely. Health service providers, including doctors, hospitals and pharmacies rated highly, with 92% of New Zealanders saying they were trustworthy. The level of trust in Police handling of personal information was also high (84%). Approximately two-thirds of respondents said they had trust in the way government departments (65%) and ACC (69%) handled personal information.

By contrast, businesses selling over the internet recorded the lowest level of trust for their personal information handling – only 25% of New Zealanders believed those businesses to be trustworthy (17% in Australia.).

People who have become more concerned about privacy and personal information are generally less trusting. The Australian results show they are significantly less trusting than New Zealanders, suggesting that trust may also trend downwards here. Perhaps more awareness means more mistrust. Our survey certainly shows the flipside, that (generally speaking) the lower the concern, the higher the confidence. It also showed that levels of trust decreases with age – younger people are more trusting than older people. Rural, provincial, homemakers, Maori and Pacific island respondents are, typically, more concerned and less trusting.

Unsurprisingly, people who have become more concerned about privacy and personal information in the last few years are generally less trusting towards all of the organisations tested in the survey.

Credit reporting – trust

Trust in credit rating agencies was also relatively low (42%) when it came to personal information handling. Trust in credit rating agencies was highest among Pacific island people (56%) and Maori (48%) while for other ethnicities it was 40%.

Across the total population, as personal income increased, the level of trust in credit rating agencies decreased.

Targeted marketing

Two-thirds of respondents (67%) said they were uncomfortable that internet search engines and social networking sites tracked internet use in order to deliver targeted advertising. This is entirely consistent with our very strong anecdotal evidence that people strongly dislike unsolicited direct marketing by phone and snail mail.

Employment

The survey has shown a continuing downward trend when people are asked about employer monitoring of e-mails and internet use. In 2001, the level of concern was 51%; that concern rested at 50% in 2006 and has decreased in the 2008 survey to 46%.

Health

Half of New Zealanders (50%) were *unaware* that everyone in New Zealand has their own national health index number which identifies them in the health system. Knowledge of the existence of the NHI was highest (71%) among those respondents classified as 'homemakers'. In the different regions, knowledge of the NHI was lower in rural areas (46%) but for some reason, was lowest in Christchurch with only 38% of those surveyed reporting awareness of the NHI.

Genetic information and insurance

Concern about insurance companies being able to make decisions using genetic information was generally high, with 74% of respondents being either concerned or very concerned. The number of respondents who felt 'very concerned' rose with age (61% of those aged 60 plus felt 'very concerned').

Range of issues

The survey asked people about a range of specific situations. Concern about privacy was greatest in the areas of safety of children on the internet (87%), and security of personal information on the internet (82%).

Although CCTV use is the subject of a great many media stories and is a constant source of enquiries to our Office, the survey once again showed that video surveillance in public places provoked the lowest level of concern (27%).

Awareness of Office

The survey also asked people about their awareness of the Privacy Commissioner. This was a "toe in the water" question to see what impact the Office might be seen to have. Overall, the response was fairly good, with 63% of people responding positively. Older age groupings reported a relatively higher level of awareness of the Office. More concerning was the fact that Pacific Island respondents reported a much lower level of awareness (26%) than the rest of the survey population. The Office clearly has some work to do in better targeting information and material to that community. (Australia 45%.)

Government Information Sharing

An interesting result was that concern about government departments sharing personal information rose from 37% to 62% between the 2006 and 2008 surveys. Perhaps this was partly due to making the question clearer – but it shows again that awareness equals concern. Business is not alone in needing to embrace privacy as an issue.

Conclusion

How to summarise and make sense of all this? Some of my initial thoughts are:

- People continue to distrust business use of their information; and there is no sign of this decreasing.
- New Zealanders are confident users of computers and the internet.
- But they are extremely suspicious of internet risks to their privacy and personal information.
- Levels of trust are low and dislike of tracking of computer use and consequent targeted marketing on the internet are extremely high.
- Concern about risks to children is extremely high.
- Maori, Pacific Islanders, older people, rural and provincial people and homemakers are generally less trusting and more concerned about privacy invasions.

But the main conclusion I draw is that we all need to take this issue more seriously. If information is the currency of the 21st century we need to gain and keep people's trust – and keep that currency flowing freely.

Privacy Issues Forum – Privacy is Your Business

But of course the reason we are all here today is to commune, listen and engage with current privacy issues. So what is on the agenda?

We start with a rousing round-up from a dynamic duo from the Law Commission, Sir Geoffrey Palmer and John Burrows. They have been given free rein to develop their session as they wish, so I have little idea what it might contain! As many of you will know, the Law Commission is part way through a magnum opus – a review of privacy! Our Office is involved in the review and of course has a keen interest in the recommendations and outcome. I know the Commissioners will welcome any contributions or comments that you have.

After the morning break you have a varied selection. You can hear about the business realities of applying privacy in practice from the likes of TradeMe and BP. And later, there is the chance to be updated by experts in employment law and privacy. As many of you will realise, the employment arena is one that bulges at the seams with privacy-related questions and issues.

Alternatively, there are sessions covering the latest in health and DNA technology. What are some of the possibilities and should we be concerned? Find out about the

use of DNA in the criminal justice context, and hear how the sex-offender registration system works in practice.

For those legal eagles amongst you, there is an update on recent privacy cases – including the rapidly-developing tort, and a chance to get to grips with how the Official Information Act and Privacy Act knit together.

There is a focus on criminal investigations in the other stream, and the role of the private investigator. Hear about the emergence of "e-crime".

And we have a session on technology that includes a focus on social networking. Something for everyone, I hope.

Practical help - Employment book

You might be wondering how you can best tackle privacy issues at a practical level. There is some help to hand. We have just launched a new guide: *Privacy at work: a guide to the Privacy Act for employers and employees* to mark the beginning of Privacy Awareness Week. I hope that it gives some practical help for both employers and employees facing difficult and potentially contentious workplace privacy issues.

The book offers much needed guidance about applying the Privacy Act in the workplace. Privacy issues at work affect most of us, one way or another, and it is an area that generates a great range of questions. For example employees may be concerned that CCTV cameras have been installed at work, or that they have been asked to undergo workplace drug testing. Employers may be unsure about whom they can contact as a referee when processing a job application, or may want to know how long they can keep personal information.

The book gives tips on use of technology in the workplace, such as monitoring staff email and internet use, or GPS tracking and finger-scanning. It also offers guidance about handling personal information on databases – including unauthorised employee "browsing" of client records. Copies are $20 and are available by contacting our office.

Conclusion

The race to take advantage of new science and technology is an exciting one, and we are lucky to be part of it. A silent revolution has occurred in the way our personal information is handled. This revolution has the potential to be as far reaching as pervasive in its effects as the invention of the printing press or the development the motor car. Data about us is being collected on an unprecedented scale both here and overseas. Responsible stewardship of this information is a key performance measure for business and government. Our survey shows that this is not an optional extra – people are aware and demanding control over their information. Our challenge is to respond to that creatively – using the technology itself to protect privacy.