presentations

Presentation by Anna Johnston, Deputy Privacy Commissioner

Privacy and records management in a digital age

for the Records Management Association of Australasia
at "The Future of Managing Records
in a Standards Environment"
11 February 2004, Westin Hotel, Sydney

privacynsw

"Privacy and records management in a digital age"
Presentation by Anna Johnston, Deputy Privacy Commissioner

For the Records Management Association of Australasia
At "The Future of Managing Records in a Standards Environment"
11 February 2004, Westin Hotel, Sydney

I was asked to address you this morning on both the general topic of privacy, and the more specific topic of the new Health Records and Information Privacy Act.

I hope that I will be able to speak about both these topics in ways that are relevant for you as records managers, regardless of whether you are in the public or private sectors. For that reason I won't be going into any detail about the two existing privacy laws in operation in NSW, the PPIP Act for the public sector or the Federal Privacy Act which covers the private sector.

So I will begin with an overview of what privacy is, and why it is important, before I address some of the challenges for you as records managers in dealing with the impact of new technologies, the tensions between privacy and records management, and the risk areas particular to your line of work.

Then I will give you an overview of how the new Health Records and Information Privacy Act may affect you.

What is privacy?

There is no simple definition of privacy to cover all circumstances. A number of elements may be considered, including such things as the right to a sense of personal autonomy, the right to have information about oneself used fairly, and traditionally a 'right to be left alone'.

Many people confuse privacy with secrecy or confidentiality, but privacy is broader than both of these. Increasingly, privacy protection is focusing on the need to ensure the fair use of personal information. The fair use of information is an essential element of an information economy just as the fair use of money or honesty is an essential element of the financial economy.

So privacy laws are really about personal information. They are about ensuring organisations act fairly in the way in which they collect, store, use and disclose our personal information.

Some people will have no difficulty with the notion that all their personal information should be open or shared. They will say: "I've got nothing to hide".

But most people draw distinctions between the parts of themselves they share with a neighbour or friend, and what aspects of their lives they may display to their doctor, their employer, or a stranger.

Privacy is about respecting those choices; allowing each of us to be the best judge as to what information about ourselves we share with other people.

Who cares about privacy?

Privacy can mean many things to many people. Privacy means that the victims of domestic violence can start a new life, without the fear of being haunted by their past. Privacy means that witnesses can give vital information but still feel protected and safe. Privacy means that judges and police can do their jobs without being victims of personal vendettas and revenge.

For many of us, privacy boils down to much more simple, everyday situations. Some of us just don't like having to provide our mobile numbers and email addresses every time we fill out a form. None of us like the feeling that our private lives are being intruded upon. How many times do we sit down to dinner and have the phone ring with someone who wants "Just a few minutes of our time to answer some questions…."?

So who cares enough about this issue to do something proactive? When the American Federal Government recently introduced a free "do not call" service, which blocks home phone numbers from telemarketers, **28 million** phone numbers were listed in the first month alone.

How about some figures closer to home? Surveys done in late 2001 indicated that 68% of Australians regard the use of their personal information for a purpose other than that for which it was originally intended as a breach of their privacy. Around 90% of Australians believe it is important that they know how their personal information might be used by the organisation collecting it, as well as to whom else it might be disclosed.

Sometimes people instinctively protect their privacy because they fear that no matter what promises are made by an organisation, some time in the future the organisation might change its mind, and start to use your information for a purpose you don't know about.

You may remember that in the last Australian census in 2001, there was a question about whether you consented to the government keeping your individually identified census form and releasing it in 99 years, rather than having it pulped as soon as the statistical data was collected, as has been the practice before.

So who cares about privacy? Almost half of all Australians take their privacy so seriously that they refused to let the government keep their census forms for 99 years. But it does differ across the population. Less than 40% of people born in England said "no", but almost 60% of those born in Vietnam said "no".

Is this a measure of distrust of government? Or is it a realistic assessment about the unknown future?

If you were from an ethnic or religious minority, wouldn't you be concerned about how a future government might misuse the information sitting in their vaults? Imagine how a future government, elected on an anti-Islamic platform for example, might force the National Archives to hand over the details on everyone who identified themselves as Islamic.

And what happens if there's a horrific crime, not unlike the September 11 bombings in America. Would you trust our government not to try and sift through the census forms for anyone who fits a 'terrorist' profile?

So it will be interesting to see if this question is repeated in the next census. The American experience has been that post-September 11, legislation aimed at preventing terrorism has since overridden the protection of their census forms, and the Government can now search through identified census documents, originally collected with the promise that they would not be used or released for 99 years.

But why should we care, if the government is only after criminals and terrorists? Politicians like to tell us, "if you've got nothing to hide, you've got nothing to fear".

Privacy protection is not about shielding criminals from legitimate law enforcement activities. It is about shielding innocent people from an over-zealous government, using electronic fishing nets to trawl through vast quantities of personal information in the hope of finding the one who meets a particular profile.

Profiling, in which conclusions are drawn about people from different sources of data rather than asking the person direct, highlights the possibility of accurate information being misinterpreted. A simple example is this: what would you think of someone whose Cabcharge records showed frequents trips to and from the taxi rank at Star City casino? You might jump to a conclusion that that person has a gambling problem. But maybe they are in fact going to visit a sick relative who lives across the street.

As American academic Jeffrey Rosen noted in his book *The Unwanted Gaze*,

> "Privacy protects us from being misdefined and judged out of context in a world of short attention spans, a world in which information can easily be confused with knowledge".

Then there are the dangers of inaccurate information being held against people, which can be even more disturbing. Examples that we see at Privacy NSW by way of enquiries or complaints include:

- The false accusation of paedophilia that ruins a teacher's employment chances
- The error on your credit rating that stops you getting a home loan
- The unfair listing on a tenancy blacklist that prevents you from renting a flat
- The incorrect fine which leads to a loss of your drivers licence

So in summary - the over-arching objective of privacy laws is to help each of us assert and preserve our dignity and autonomy, by allowing *us*, rather than governments, corporations, or other people, to control and define information about ourselves. The protection of privacy is about shifting the locus of power away from governments and corporations, and back to citizens and consumers.

Privacy protection as a public interest

Yet at the same time, privacy is not just for the benefit of the individual. It is about how we function as government and as a society. In law enforcement, the protection of informants means that criminal law can be properly enforced. In the health sector, anonymity and confidentiality means greater trust and also improved public health.

Privacy of thought supports freedom of expression, freedom of speech, and freedom of association. Anonymity can foster creativity.

And privacy makes possible the idea of the fresh start. It is a necessary support structure for a society committed to equal opportunity.

For let us not be fooled into thinking that governments never make mistakes, or that organisations never act in discriminatory ways. Do you think that some of the new technologies now at our fingertips – such as relational databases, genetic testing, biometric identifiers and so on – would have been applied in a neutral fashion towards Jews in the 1940s? Towards members of the Communist Party or homosexuals in the 1950s? How might they be applied today towards protesters outside Woomera detention centre? Or people with HIV or Hepatitis C?

So why is the protection of privacy important for you?

I hope that I have given you an insight into why privacy matters to individuals, and why it matters to a functioning society. Now the question is : why should it matter to your organisation?

Commitment to the protection of individuals' privacy is not only important for organisations because of their legal obligations. Privacy protection is integral to trust, and trust is the cornerstone of effective relationships. This is true no matter what kind of relationship we are talking about: from your personal and family relationships, to commercial transactions, to e-government initiatives involving the relationship between the citizen and the state.

The Federal Privacy Commissioner's research indicates that Australians rank respect for personal information equal first with quality of product or service. More than 40% of respondents said they had totally refused to deal with particular organisations because of concerns over the use and protection of their personal information.

While you might not think that last figure relevant for government, since our 'clients' do not always have the ability to protest with their feet, you should note that 14% of respondents said they had decided not to deal with *government* because of privacy concerns.

Our challenge as government is to build on the balance of privacy, accountability and transparency. People must have confidence in this balance. On one hand, they must know that government is working effectively to provide services and security in a transparent manner. On the other, we must also be able to trust the government to uphold the respect of each individual's rights, including the right to privacy.

When people's private information is involved, this trust can only be achieved through a commitment to the fair and responsible handling of personal information.

We at Privacy NSW believe that the link between privacy protection and trust, and between trust and successful and accountable government, is clear. It is no coincidence

that Canada is at the forefront in e-government, since it is also a leading country in terms of privacy protection[1].

So we see privacy compliance not as a cost to public sector agencies, but as an investment, in both customer and employee goodwill; an investment increasingly necessary in the 'Information Age'.

Privacy and records management

Tensions between privacy and records management

The most obvious area in which privacy and records management appear to conflict, at least at face value, is in the area of retention periods. Privacy laws typically say that records should be kept for no longer than that required for the purpose for which the information was originally collected. By contrast records management laws or archiving policies may err on the side of keeping records for as long as possible.

But in fact this tension is fairly easily resolved for the NSW public sector records manager, for the retention periods established under the State Records Act require you to keep records for minimum periods. The NSW privacy law does not override this.

Another area of tension is with respect to the amendment or correction of records. This is more difficult. Privacy law says records must be corrected or deleted if they are found to be inaccurate or misleading. For NSW public sector agencies the law is fairly clear: the PPIP Act overrides the State Records Act. However in practice there are often further reasons why records cannot be completely deleted or amended – because sometimes to do so would be to create a further problem. For example if your health record incorrectly said you were diabetic, that error might put into context some subsequent treatment decisions. If you go back to delete the original incorrect statement, you may now have a history of treatment which does not make sense.

A third area of tension is related to requests for disclosure of information from your records. As records managers you are bound to respect the privacy of people who – now you have their information – have little say in the secondary use of that information. Privacy law will often guide your decision, but in some cases the law defers to the professional ethics of archivists or Human Research Ethics Committees.

Here the "values of individual autonomy and of freedom of research collide"[2]. You are being asked to decide on how to balance privacy versus disclosure, "the right to forget and the right to know"[3].

This decision is often now one you need to make up-front. That is : what information should you put on the internet, to be accessible to all people? How does that affect the privacy of individuals?[4]

---

[1] In 2002 Canada became the first national government in the world to introduce mandatory Privacy Impact Assessments for new government projects and policies, and in a recent global survey, Canada was placed first of 22 governments in e-government innovation.

[2] Eric Ketelaar, "The Right to Know, the Right to Forget? Personal information in public archives", *Archives and Manuscripts*, Vol 23(1), 1995, pp.8-17; p.16.

[3] Ketelaar, p.16.

[4] American academic Gary Marx has noted: "We are becoming a transparent society of record such that documentation of our past history, current identity, location, communication and physiological and

Forgive and forget

This discussion leads us to ask:

Are we going to reach a state of transparency overload? How does the internet affect our capacity to forgive and forget?

Perhaps some day we will look back upon this period of history, and call it the "Google Age". I believe we are at an awkward time, in which unprecedented amounts of information are available to the public, to search through almost instantly. Yet we don't quite know what limits we should place upon the use of such information.

How much do we need to forget, as a pre-condition to forgiveness? What happens when Google never ever forgets?

Before the advent of the internet and its powerful search engines, you could be reasonably confident that fairly minor, trivial or embarrassing details of your life would not resurface. The school photos showing that disastrous period when you tried to dye your own hair could be safely buried at the back of your own bookshelves. The high-spirited 19 year old who cops a 'drunk and disorderly' fine will later become the 50 year old law-abiding and respected doctor.

But now? Now your neighbour, your boss, your bank manager or your new boyfriend can run a 'google' search. What will they find?

We have a regime of "spent convictions" in NSW. This is a law that says, if you commit a minor offence, and then don't do anything bad again, in 10 years' time we will officially forget it. Your record won't disappear entirely – it can still be brought out if you commit another new crime – but as long as you behave, then you are allowed to say to an employer "no, I don't have a criminal record". The State has forgiven and forgotten you.

Having a spent convictions scheme helps with rehabilitation. It provides a great incentive not to commit any offences in the future.

But now that scheme is being undermined by the internet. In the interests of open justice and accessibility of the law, more and more court decisions are being published on the internet. In the past, only significant cases were reported, and then in dusty law journals that most people don't go near. Newspapers often reported minor cases, but there was no way to search for individual names in their archives. But now if the 'drunk and disorderly' conviction is written up on the internet, in 30 years' time it will still be there, for anyone to see.

It's not just criminal convictions at issue here. How about court records relating to family law? Newspaper reports about a neighbourhood dispute? Photos taken of you at a party by someone you've lost contact with?

---

psychological states and behavior is increasingly possible. With predictive profiles and DNA there are even claims to be able to know individual futures". Gary Marx, "Privacy and Technology", *Telektronik*, January 1996.

So the questions for this "Google Age" are : When does shaming end? How long should people remain in the "digital stocks"?[5]

I would suggest that in the coming years the records management industry will have a significant role to play in answering those questions.

Challenges for records managers

The challenge for both businesses and government agencies is how to respect the personal information of the many and varied people they deal with.

As with any new compliance issue, it can be hard work.

First, there is the challenge of competing interests.

The implementation of privacy laws and policies inevitably involves difficult decisions, in which competing interests will have to be weighed. In particular, one must always consider the public interest in the protection of individuals' privacy, as well as the public interest in open and accountable government decision-making.

But I would suggest to you that these two particular interests are not necessarily in conflict. As I mentioned earlier, privacy, like freedom of information, is about shifting the locus of power away from the government and business, and towards the citizen and consumer.

A second particular challenge is the need to be proactive.

Unlike other administrative law areas such as FOI, it is becoming harder to protect privacy by default.

There used to be certain natural barriers that protected people's privacy by default – the barriers of time, distance and cost. In the days of paper files, the sheer effort of collecting and tracking detailed personal information about the average person was simply not worth the effort. And hence privacy was, for the most part, protected by default.

Those days are gone, and that's why organisations have to be much more pro-active than they used to be to ensure that they are 'privacy compliant'.

And a third challenge is that of data security.

I will use a real-life case study to illustrate the particular risk area for you, which is inappropriate access to, and use of, personal information held in your organisation's records. The names have obviously been changed.

A University student, Ms Smith, received an email sent to her University email address from Mr Jones, who was employed by the University in an area dealing with student records. Mr Jones and Ms Smith had previously worked together at a different organisation. The email sent by Mr Jones was not related to University business, and

[5] These questions have been drawn from a panel discussion led by the Victorian Privacy Commissioner, Paul Chadwick, at the International Conference of Data Protection and Privacy Commissioners, Sydney, September 2003 : "Open justice, forgiveness, compassion, context and proportionality".

invited Ms Smith to meet him socially. The email also commented on Ms Smith's change of name since they had last met.

Ms Smith was concerned that Mr Jones might also be able to access her academic marks, financial records, scholarship applications and more sensitive information such as counselling records.

She made a complaint to the University, which was dealt with by Internal Review, oversighted by our Office.

The University concluded Mr Jones's conduct was such as to cause the University to breach the PPIP Act, by using personal information for a secondary purpose without lawful authority.

Mr Jones was also found to have breached the University's Privacy Policy, the University's Code of Conduct, and agreements to protect personal information signed by him when he commenced employment. In misusing information obtained in the course of duty, his conduct also constituted a category of corrupt conduct under the *Independent Commission Against Corruption Act 1988* (ICAC Act).

The University made a formal apology to Ms Smith, and undertook to implement measures to ensure that the conduct would not occur again. In relation to Mr Jones, the University referred the matter to their Manager of Industrial Relations to determine if any disciplinary action ought to be taken. The University also undertook to increase its privacy awareness training for staff that have access to student records.

Under Information Protection Principle 5 in the PPIP Act, agencies are obliged to implement security safeguards to ensure that personal information is protected against loss, unauthorised use, modification, disclosure or other misuse. However as this matter demonstrates, internal policies, staff contracts and IT systems alone cannot eliminate all risk.

This case highlights the increased privacy and corruption risks posed when people have a conflict of interest, such as where agencies engage staff members to deal with records that may relate to their own colleagues, friends or acquaintances. Organisations should be alert to this risk, and take preventive action.

So that concludes my overview of what privacy is, why it is important, and the particular challenges for you as record managers.

The HRIP Act

Now I turn to a very brief overview of the Health Records & Information Privacy Act 2002 (the HRIP Act).

Why a new Act?

The privacy of health information is a live topic, given recent progress towards the development of an integrated electronic health record. Over the last few years in NSW

there has been a flurry of activity in an attempt to ensure that strategies are in place to protect privacy standards before an electronic health records system is fully implemented.

The ability for an electronic health record to be linked and integrated with ease has the potential to diminish an individual's control over the flow of their health information. This can create apprehension in the minds of individuals as to who is accessing their health information, and for what purpose.

Now despite what you might think, privacy advocates are not anti-technology per se. On the contrary, advances in record-keeping technology can help ensure that an important privacy principle is met, namely that information is accurate, complete and up-to-date. So we believe that the electronic health record has much to recommend it, and many potential benefits. And although we believe strongly in the importance of privacy, we do not believe that privacy trumps all other interests.

The challenge, as we see it, in the development of electronic health records systems, is to maximise both the protection of individual privacy on the one hand, and positive health outcomes on the other. Controls and safeguards over electronic health records are important to ensure that there is maximum public confidence in the electronic health records system.

Therefore in 2002 the NSW Government passed a new law, the *Health Records and Information Privacy Act*, which introduces a comprehensive system for the regulation of health information in NSW. It applies to health information held by both the private and public sector. The Act is expected to commence in July this year.

The purpose of the HRIP Act is to promote fair and responsible handling of health information by:

- *protecting the privacy* of an individual's health information that is held in the public and private sectors, and
- enabling individuals to *gain access* to their health information, and
- providing an accessible framework for the *resolution of complaints* regarding the handling of health information.

The objects of the HRIP Act are to:

- *balance the public interest* in protecting the privacy of health information, with the public interest in the legitimate use of that information, and
- enhance the ability of individuals to be *informed* about their health care, and
- promote the provision of *quality health services*.

Who does the HRIP Act cover?

The HRIP Act applies to every organisation (public sector agency or private sector person) that is a health service provider *or* that collects, holds or uses health information.

So the coverage is quite broad. It is not only health service providers. It is not only the public sector.

It is every organisation that collects, holds, or uses health information. This can include, for example, gymnasiums, alternative therapists, counsellors, superannuation providers, insurance companies and so on.

There is a ‘small business’ exemption for private sector organisations, but it is not applicable to health service providers.

What is ‘health information’?

The definition of health information is set out in section 6 of the Act to include information or opinions about a person’s physical or mental health and information collected in relation to organ donation or genetic information.

It also includes any other personal information that is collected to provide, or in the course of providing, a health service, such as a person’s name and address.

What obligations are imposed on holders of health information?

The Act requires holders of health information to comply with 15 Health Privacy Principles. These principles form the core of the Act, and establish obligations in relation to the collection, retention, storage, use and disclosure of health information.

Health Privacy Principle 15 also ensures that patient information is not linked into a state-wide electronic health record unless the patient has expressly consented to participate in such a scheme.

We have published some Fact Sheets, which set out the 15 HPPs in plain language, and I would encourage you to use those documents. One set is written in terms of an organisation’s responsibilities, and the other in terms of an individual’s rights.

How will complaints about breaches of the Health Privacy Principles be handled?

Complaints about public sector agencies will be dealt with under the existing *Privacy and Personal Information Protection Act 1998*. Under the PPIP Act, agencies are required to conduct internal reviews of the conduct or decision complained of. For example, if a public sector agency refuses a person access to his or her own health information, the person is entitled to request an internal review of that decision. Where a complainant is unhappy with the results of an internal review, they are entitled to take their complaint to the Administrative Decisions Tribunal. The agency may be ordered by the Tribunal to change their practices, rectify any damage, or pay compensation of up to $40,000.

The complaints process for private sector organisations is a little different. Complaints will be made to Privacy NSW, and we will have the power to review, investigate and attempt to conciliate the complaint. Once this stage is complete, the complainant may choose to take their matter to the Administrative Decisions Tribunal. The Tribunal will be empowered to make the same range of orders as those available against public sector agencies, with the exception that if the defendant is a non-corporate entity, for example an individual GP, the compensation is limited to $10,000.

How you can prepare for the commencement of the HRIP Act

- **Familiarise yourself with what "health information" is, and what the HPPs say**
- Section 6 – "health info", Schedule 1 – HPPs
- See our Fact Sheets for a plain language explanation of the HPPs

- **Identify where your agency handles health information**
- Don't assume that if your agency is not a "health service provider", then it doesn't handle health information.
- Every agency will at the very least have sick leave records about their own employees.
- Local councils, for example, may collect and handle health information in the course of providing family day care, community care, or aged and disability support services such as 'meals on wheels'. You will need to think carefully about it.

- **Promote awareness of HRIPA within your agency**
- If possible, engage others in this process.
- The more people in the agency who know about the Act, the more likely it is that your agency will be operating in compliance with the Act, and the more chance privacy has of being ingrained into the culture of the agency.

- **Approach implementation of PPIPA and HRIPA in an integrated way**
- For health service providers, obviously most of the information you handle will be information "collected to provide, or in providing a health service", and thus come within the definition of "health information". So HRIPA will become the principal Act that you are covered by. There will be more for you to do.
- But every agency will need to identify the areas within their agency that handle health information, and then review existing policies and procedures, and where necessary, revise or develop those policies and procedures in order to comply with the new Act.
- Public sector agencies should then amend their Privacy Management Plans accordingly.

- **Training, guidance and assistance available**
- Privacy NSW is working on a training package now, which will be implemented later this year.
- In the meantime we have Fact Sheets and other FAQs, available on our website.
- Look to Victoria for examples – as they have a similar system: the Information Privacy Act (VIC) 2000 and the Health Records Act (VIC) 2001.