Privacy Commissioner's Speech at:

National Media, Privacy & Entertainment Conference

13 June 2013

Privacy and Technology 2013 – The implications of new technologies, records management, and information governance practices as these relate to access to government information and the protection of privacy

Thank you Patrick.

Before I begin, I’d like to acknowledge the traditional owners of the land on which we are gathered today, and pay my respects to the elders, both past and present.

Notions of privacy, one’s own privacy and the ability to enforce our expectations have changed dramatically along with changes in technology.

The advent of new technologies, particularly social media, has posed challenges not seen before when we relied upon printing presses, faxes and snail mail to communicate. The ability to send a photo, a quote or a document around the world with one click has changed how we relate. And brought into focus a number of significant debates not least of which is the standing of privacy in the internet age.

In the information sphere, there has been a rapid convergence of technologies – telecommunications has merged with computerisation and other forms of communication, and with the creation and mining of huge databases. The speed, power, accessibility and storage capacity of technologies using personal information are hugely increased.¹

The individual now has a virtual existence in cyberspace in addition to a presence in what has been termed ‘meat space’.²
Each of us has a digital persona made up of a collection of previously unconnected information. Personal data has been described as the currency of the information economy. Analysts have likened it to the importance of oil in the industrial revolution.

I’m both a big fan and user of the internet. I’m not an IT expert, I don’t have the capacity of your average eight year old user, but I get by. I use the internet for the prosaic chores of checking train timetables through to researching obscure references to privacy law in Elizabethan Tudor England.

I also use social media but compared to the extent of my internet browsing, it’s limited. And I will admit to a little on-line shopping too. I mention these personal habits as some have a view that Privacy Commissioners will be automatically opposed to new technologies. I’m not. I think there are huge benefits to be gained from these technologies including data linkages but with, of course, appropriate privacy protections and practices.

One of the big pluses of the internet is that it is requiring all of us to think rigorously on the role and value that privacy plays in our society, and how it can be safeguarded in the internet age. Another benefit from the convergence of electronic technologies is the emergence of new forms and expressions of governance.

One of the down sides has been the sprouting of some oft quoted myths around privacy.

Let me move first to address myths; not the ones concerning a goldfish’s three-second memory, or that bulls get angry when they see the colour red – both false by the way – but those myths that exist regarding privacy and which are also false.

What are some of these myths?

First and foremost, that privacy is dead.

Secondly, then, the always prevalent, ‘If you’ve got nothing to hide you have nothing to fear’; and lastly, that ‘Privacy is the enemy of freedom of speech and of open government’.

There are more myths but, for relevance to the topic, these are my pick.

It’s important to address these myths. If they are not addressed; they continue to have a life unchallenged. There is value too in stating principles.

At the practical and operations end, the need to build privacy management into corporate governance will not be taken seriously if these myths prevail. And as a consequence,
corporate governance and key management practices such as information management and risk management will suffer, as will critical administrative functions, such as records management.

What does privacy have to do with records management, I hear you ask – well, a lot, but I’ll come back to that.

Our increasing usage and reliance on new technologies has most definitely spawned the first myth, ‘Privacy is not only dead but buried’.

(SLIDE)

“You have zero privacy anyway. Get over it”, CEO Scott McNealy, Sun Microsystems, (1999)

Way back in 1999, the CEO of Sun Microsystems – creator of Java software – made that oft quoted remark that privacy was dead and we should get over it.iii

He made the remarks in response to a question about what privacy safeguards his organisation would be considering for a new technology; one that was designed to allow various consumer devices to communicate and share processing resources with one another.

And it’s true that losses of privacy have been through the many voluntary and every day electronic transactions we all undertake. But it’s not as if it’s always been a real and informed choice. The media itself has identified many practices where policies and practices have changed without warning or consent.

Yet, at the same time, it is technology’s impacts that are increasing the desire for and value of privacy. It is also technology that can provide answers if we value our privacy sufficiently and make our privacy expectations known, including through use of our purchasing choices.

Technology is, for the majority of us, integral to our lives. In fact, our reliance on technology is so strong nowadays, that being “off the grid” is something many people strive towards at certain times.

Some marketers are seeing this as an opportunity.
In London, in January this year, Selfridges opened a felt-covered ‘Silence Room’, where shoe-free, phone-free shoppers can retreat from the franticness of Oxford Street and the store itself.

No phones allowed. No loud talking. A bit of peace, quiet and the opportunity to take time out.

Originally due to run for a month or so, the Silence Room has been extended to run until the end of June; possibly later – such is its success.

You may think this was a new idea to keep up with the modern connected world, but interestingly enough, the concept of this ‘Silence Room’ goes back to 1909 when Selfridges’ founder, Harry Gordon Selfridge, included a Silence Room in the original store.iv

The ‘Silence Room’ and the notion of “being off the grid” reflect the notion of ‘privacy’ as the ability to be left alone, to be free from unwanted intrusion. It also underscores that no matter our reliance upon electronic tools and systems, privacy is an essential part of life.

Our need to preserve private spaces and private time in our lives, to reflect and enjoy moments of solitude is as relevant now as it has ever been.

It may seem a contradiction, but while people are out there sharing all sorts of information, and sometimes laying bare more than any of us ever wanted to know, their concerns about privacy have increased. But this is the case.

Enquiries to our office on privacy related matters have increased by more than 300% over the past four years. Privacy, and our right to privacy, touches the very core of our expectations of inalienable human rights. And it’s a fundamental part of a free society.

Our ability to exert our right to privacy speaks to our position of control and self-determination – the respect we have for ourselves, the respect we give to others and, the respect we receive from others, including government and business.

Because of the significance of privacy to our ability to function as respected members of society, we find it enshrined in some of the most powerful international conventions – the United Nation’s Universal Declaration of Human Rights (Article 12) and the International Covenant on Civil and Political Rights (Article 17).
Here we have Article 12, which says that:

“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”

Yet despite this United Nations recognition of privacy as a ‘right’, a prevalent myth we hear, and one that I as Privacy Commissioner most certainly do, is: “If you have nothing to hide, you have nothing to fear”.

This invidious saying was debunked comprehensively by the then Victorian Privacy Commissioner, Paul Chadwick in 2006, and I draw from his analysis and recommend his speech in full.† It’s on the Victorian Privacy Commission’s website.
Paul succinctly and elegantly pointed out that the sub-text here is that if you object to others having details of your life, or that of your family, you must be guilty of something, or possessing a shameful secret, or up to no good.

The focus upon the objector completely ignores the other half of the equation that is, “is the trustworthiness and intent of those collecting or using the information beyond question?”

And you need go no further than the 1992 ICAC inquiry into the unauthorised use of Government information to see what can occur without protections for personal information.

The point that the then Victorian Privacy Commissioner made well was that, the “nothing to hide, nothing to fear” imputation, should be turned around. Specifically, “No legitimate reason to know, no legitimate reason to ask”.

Coming now to the third myth, that privacy and privacy protections prevent free speech and restrict access to government information.

I work as an independent and equal Commissioner with my colleague the Information Commissioner, Deirdre O’Donnell, in the NSW Information and Privacy Commission. From this experience I say “freedom of speech and privacy are complementary and both are integral to a democratic way of life”.

information and privacy commission new south wales
www.ipc.nsw.gov.au  |  1800 IPC NSW (1800 472 679)
Privacy protections lie at the heart of a democratic state as they provide a way of constraining the power which people or organisations gain when they collect or monitor information about others.

Unreasonable incursions into our private lives erode our individual freedoms and autonomy irrespective of whether these incursions are undertaken by Government or other agencies. There is no obligation in a free society for individuals’ lives to become an open book for government or others to trawl through, especially when there is no public interest issue.

You will recall that Lord Justice Leveson spent a year and a half engaged in an inquiry into the culture, practices and ethics of the press in the United Kingdom. He spoke in Sydney in December 2012 at the invitation of the Communications Law Centre, University of Technology, on the subject of privacy and the internet.vi

Lord Leveson addressed the issue – whether in the age of the internet, privacy is dead: only freedom of expression, or “sharing” as Mark Zuckerberg would say.

He pointed out that views that privacy is dead, or no longer “a social norm” (Mark Zuckerberg 2010) are not new. He traced the history of the birth of the popular press and how it gave rise to similar privacy concerns.

While we have been here before, Lord Leveson acknowledged that the historical analogy may not hold in relation to the internet, the ‘global megaphone’.vii The nature of the internet with its ease and speed of disseminating information, its wide distribution and digital permanence, combined with an element of ‘mob rule’ that can prevail in blogging, twittering and other social media, may pose particular challenges.

He was hopeful however, that as with the rise of the penny press in the 19th Century, that time and proper application of the law will, over time, “civilize the internet”.viii

What he thought more likely was not the question of how to protect private information, but what was it that we as a free society seek to protect.

As a Privacy Commissioner, I certainly want to believe he will be proven correct.

I said earlier that personal information is the oil of the information economy. When I was researching this address, I came across a reference to a company that sells deleted Facebook posts going back seven years, to recruitment agencies. And there are many other such examples of how the commercial incentive and technological capacity can enable the
determined and resourceful to trawl and use the internet and social media in “privacy invasive” ways. Will the internet be civilised, privacy wise? Will there be the development of “cyber manners”, as some commentators have asked?

It is an aspect of freedom of expression that an individual can properly choose not to publicly disclose certain things about his or herself whether it is facts, views or personality. Lord Leveson saw the right to be silent as exercising not only a right to privacy but also a form of freedom of speech.

If we accept this connection between privacy and freedom of speech, it follows then that to have concerns about the access others have to your information is not only a desire for the protection of privacy, but also for the protection of freedom of speech. That is the choice not to publicise your details.

As the following slide demonstrates, his words capture this better than mine.

(SLIDE)

“Privacy is in itself both an aspect of freedom of expression and necessary for freedom of expression to be fully realised.” The Rt. Hon. Lord Justice Leveson, December 2012

I’ll just point out the obvious – totalitarian regimes are not known for freedom for their citizens, neither for freedom of the press nor for the privacy rights of individuals.

While society obviously needs to be safeguarded from clearly antisocial forces, there are strong arguments for protecting and preserving privacy. It can be a fine balance.

There is also a fine balance between the ‘public’s right to know’ and the ‘public’s right to privacy’.

I’ve been asked to address the connection between access to government information and protection of privacy. And, I thought it might be helpful to do this by examining the rationale behind the formation of the Information and Privacy Commission in 2011.

The merger of Privacy NSW with the Office of the Information Commissioner created an independent body for individuals and agencies seeking advice and redress in relation to the protection of personal information and access to Government information.
Both privacy and access involve rights, and both impose obligations on the public sector in the way that it deals with information. And they are both concerned with transparency and holding Government accountable.

Sometimes it’s not clear cut. For example, where a person seeks access to Government information which includes a third party's personal information. There is then a need to strike a balance between the importance of disclosure, in the interests of open Government, and the importance of protecting individuals' privacy. The test that is applied is ‘the public interest test’.

The single office gave effect to the view of the NSW Law Reform Commission that, administratively, it makes sense to have a single body as agencies’ questions about protecting personal information and access to Government information frequently overlap.

Both Commissioners are independent and report to the Parliament. The NSW Parliament’s Joint Committee on the Office of the Ombudsman, the Police Integrity Commission and the Crime Commission oversees both Commissioners.

The legislative framework requires consultation between the Commissioners on certain matters. Before I issue guidelines that limit the disclosure of personal information by a public sector agency, I must consult with the Information Commissioner. Conversely, when the Information Commissioner issues guidelines with privacy implications or recommends disclosure of privacy-related information, consultation with the Privacy Commissioner is required.

The tension between the ‘right to privacy’ and the ‘right to know’ has existed for a long time and will continue. It is not possible to be prescriptive. Each matter typically has to be assessed on its own facts and circumstances.

There is recognition within the NSW Government that increasing access to public information requires an obligation to protect personal information. The 2012 NSW Information Communications Technology Strategy commits to strengthening electronic information security measures across the NSW public sector.

Similarly, the NSW State Plan’s commitment to promote the community’s right to open Government has recognised that it is important to ensure appropriate safeguards are in place to protect privacy.
I indicated earlier that the evolution of information communication technologies have given rise to new forms and expressions of governance – one of which is information governance.

In the past, some of the chief protections for privacy were that it was just so difficult to collate and link personal information. ‘Big data’ has changed that.

(SLIDE)

“Some of the chief protections for privacy arose from the sheer costs of retrieving personal information, the impermanency of the forms in which that information was stored; and the inconvenience experienced in procuring access (assuming its existence was known).”

– The Hon Michael Kirby, 1996, p4

I’ll ask you to note the date when that was said – 1996 – and to consider the advances in technology since then.

Now changes in technology, and particularly convergence, have removed this unintentional safeguard completely. So much so that privacy, data protection, and identity theft have become issues of interest for records managers. And the role of records managers has grown to aid in the protection of an organisation’s records against such risks.

(SLIDE)

Information governance

So, what does privacy have to do with information governance and specifically, records management?

Information governance sets out the organisational requirements for the valuation, creation, storage, use, archiving and deletion of information across the business. Its primary aim is the smart uses of information to assist an organisation to achieve its goals. It’s also about accountability and encouraging the right behaviours.

Taking an enterprise-wide view gives ‘information’ value as an ‘asset’ that needs to be managed. It draws together the responsibility for managing this asset from sometimes disparate parts of the organisation. It also provides the opportunity to identify and capitalise on good privacy practices, to build in appropriate privacy protections, and to address risks of inadequate data security (amongst other things).
If you have difficulties relating information governance with privacy and records management, it can be helpful to think of privacy and records management as tools of information governance.

Records management is a practical example of privacy in practice. Under NSW Legislation there are Information Protection Principles that enable people to actively obtain access to records containing information about them. Records are to be accessible to the individual for viewing. Changes can be requested if the information is inaccurate or irrelevant. If record management is such that a record cannot be located, the individual cannot exert their privacy right to see their information, and correct it, if appropriate.

The reform of the Commonwealth Privacy Act is adding pressure to establish information governance as a recognised part of corporate governance. And to review its adequacy. I note that many companies and professional bodies, such as the Australian Institute of Company Directors, are urging Directors to understand the new obligations under these reforms.

These Federal privacy law changes will take effect from March 2014. Thirteen new Australian Privacy Principles will replace the existing Information Privacy Principles and National Privacy Principles that apply to Commonwealth government agencies and businesses respectively.

These new principles or APPs as they are known, more closely reflect the information life cycle from ensuring transparency in information collection through to use and disclosure, quality and security, access and correction.

They will have significant implications for information governance. Most, if not all of the information protection principles have a linkage to records management actions.

Take APP 4 – ‘dealing with unsolicited information’ – where an agency comes into possession of unsolicited personal information, it must now consider whether the information is something it could have collected itself under the APPs. If not, and the information is not in a Commonwealth Record, the information must be destroyed or de-identified.

The important things to note are that unsolicited personal information is afforded privacy protections, and in addition, that the need to ensure irrelevant information about individuals is not retained, bringing greater focus to records retention schedules and records destruction.
Another example, APP 8 relates to cross border disclosure of personal information, requiring an agency to take reasonable steps to ensure that the overseas recipient does not breach the APPs.

APP 11 refers to security of personal information. While security is currently a principle under both the NPPs and IPPs, from March 2014 there will be an additional requirement for agencies to protect personal information from *interference*. This APP also sets out that an agency has obligations to destroy or de-identify personal information in certain circumstances.

The Australian Privacy Commissioner’s powers will be expanded. The Commissioner will have the power to:

- conduct, at any time, compliance assessments of an entity’s information maintenance practices;
- accept written undertakings that may be enforced in court; and
- seek civil penalties of up to $1.7 million for serious or repeated breaches, and the provision of enforcement powers and other remedies in regards to own motion investigations.

The new Australian Privacy Principles are similar to those that apply at the State level in the alignment with the life cycle of information from collection through to access and correction.

A key governance concept in the privacy sphere is ‘Privacy by Design’, a term coined by the Ontario Information and Privacy Commissioner, Dr Ann Cavoukian.

‘Privacy by Design’ essentially involves proactively (rather than reactively) addressing privacy. With technology, it involves planning privacy protections from the outset; when creating any system designed to collect, use and store or share personal information. It embeds privacy and data protection throughout the entire life cycle of technologies, from the early design stage to their deployment, use and disposal.

‘Privacy by Design’ is a critical concept for information governance.

When applied to assessing readiness for the Federal privacy changes, it would entail conducting a privacy audit of the organisation – to identify what personal information is collected and how it is collected, stored, used and disclosed.
As well as undertaking an assessment of compliance against the new APPs and developing a strategy to address any shortfalls.

It may be necessary to revise and update privacy policies and practices, and undertake staff training. Forms may need to be reviewed for compliance with the new credit reporting and credit information requirements.

Outsourcing and other practices should not be forgotten when reviewing compliance against APP 8 for personal information transferred out of Australia. New contractual arrangements may be required with any overseas recipients of personal information. Cloud computing is an obvious outsourced arrangement that will need to be included.

In this readiness program, don’t forget records management and the role it plays.

Records management is often seen as an unnecessary or low priority administrative task that can be performed at the lowest levels within an organisation. However, records management is primarily concerned with the evidence of an organisation’s activities. That’s not an inconsequential activity.

Like work-place health and safety, like privacy protection, information management is the responsibility of everyone within an organisation.

Good records management practice is about the creation, management, protection and ultimate retention or disposal of the records that are generated in the course of everyday business – whether those records are paper or electronic. And electronic records can include x-rays, scanned office documents, databases, application data and e-mail.

Another Federal privacy reform to watch is the proposed mandatory data breach requirements.

If the current Bill before the Senate is passed, notification of serious data breaches that will cause “real harm” will become mandatory. It is expected that this legislation, if passed, will also come into effect in March 2014.

Additional governance issues are triggered. What is your organisation’s policy on data breaches? Do employees know who to inform if a serious breach occurs, what processes will be followed, and by whom? Who will inform the Office of the Australian Information Commissioner?

Some governance questions you might care to consider in relation to cloud computing are:
• can my organisation audit the cloud provider to ensure they are complying with obligations?; and
• what reports do we require to ensure that our compliance requirements are being met? 

Good governance practices lead to good management of clients’ personal information. This in turn builds consumer confidence and influences consumer preferences which can lead to a competitive advantage. It’s not too hard to imagine that, far from being dead, privacy could become an element in an organisation’s competitive arsenal.

I urge organisations to demonstrate their accountability by including privacy as part of their corporate governance, and valuing it as part of their corporate identity.

I mentioned earlier the advent of ‘big data’ – vast databases holding vast amounts of information. Highly personal ‘big data sets’ are a prime target for hackers, or leakers or criminal elements. More regularly, data breaches arise from within an organisation – either from human or computer error (even technology can fail sometimes).

If you have the capability and resourcing to undertake testing of your information technology for possible privacy breaches, then it is a good risk management strategy. It is no excuse to say “we didn’t know about it”. It is the organisation’s responsibility to ensure personal details are safely secured.

From my perspective, it is imperative for organisations handling personal data to have effective strategies in place, which brings us back to governance and Privacy by Design.

“Prevention will always be better than cure”, if I can use that saying. This is even more important as technology continues to evolve and social norms or ‘cyber manners’ and legal frameworks are slow to keep up.

I encourage you to implement a Privacy by Design approach to build privacy into your organisation, from the ground up.

Privacy by Design will provide the foundation stone for good information governance and will help your organisation effectively adopt new technologies, as well as giving you confidence in your organisation’s management of privacy.
We’ve traversed a considerable amount of territory today, from the UN Declaration of Human Rights to the workings of records management. I’ve found it a valuable exercise to compose my thoughts on those topics, and I trust it has also been of interest to you.

Thank you for your attention.

References:


