information and privacy commission new south wales

Privacy Commissioner's speech at:

Privacy Reform and Compliance Forum

12 June 2013

Roles and Responsibilities as a Privacy Commissioner

Thank you Professor Greenleaf. 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 elders both past and present.

I'm delighted to be speaking to you as part of the Privacy Reform and Compliance Forum, where the new Federal privacy reforms will be covered, including how they will impact upon us all.

Today I'm addressing the roles and responsibilities of a Privacy Commissioner in our society, primarily at a State level but also with some reference to the Federal role. With the Victorian and Queensland Privacy Commissioners here, there will be opportunity in the roundtable to clarify any differences in their roles and perspectives. I'll look at the framework within which the NSW Privacy Commissioner works, the new Commonwealth amendments, and the future challenges ahead.

I'll also address some privacy myths frequently put to Privacy Commissioners.

But first, 'privacy'…

What is privacy, why does it matter to us, and what are some of the common misconceptions about privacy?

(SLIDE)

Many people over many decades have attempted to define privacy. Ultimately, definitions tend to include one or all of the following elements listed on this slide:

- The right to be left alone, to enjoy solitude

- The ability to exercise control over one's personal information, or
- A set of conditions necessary to protect individual dignity and autonomy and for a democratic society.

We often think about privacy in different ways, for example:

- Physical privacy – such as bag searching, or use of our DNA;
- Information privacy – the way in which our personal information such as our age, address, sexual preference and other details are handled; or as
- Freedom from excessive surveillance – our right to go about our daily lives without being watched or having our actions recorded. Issues which are currently featuring in the media.

In different situations we may prefer one or another of these definitions. We may also choose to emphasise different aspects of privacy depending on the reasons why we think that privacy is important.

Privacy protections are critical because they:

- provide a way of controlling the power which people or organisations gain through collecting and storing information about others;
- because they require conditions, such as data security which people expect when providing personal information about themselves; and
- because privacy protections are a necessary condition for a democratic society which truly values freedom and diversity.

General rights to privacy

Privacy as a value, or as a right, is not something dreamt up by Privacy Commissioners.

Privacy – and our right to privacy – is an inherent human right to which we are all entitled. It was recognised as a basic human right in some of the most powerful international conventions, the Universal Declaration of Human Rights (Article 12) and the International Covenant on Civil and Political Rights (Article 17).

(SLIDE)

As you can read on this slide, Article 12 of the Declaration of Human Rights 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.[i]

Yet amid this background of recognising human rights, we hear some declaring "Privacy is dead".

The first widely publicised remark came in 1999, when then CEO Scott McNealy of Sun Microsystems – the creator of Java – infamously declared, "You have zero privacy anyway. Get over it."[ii]

He made the remarks in response to a question about what privacy safeguards his organisation would be considering for the design of a new technology.

Then, during a keynote session in October 2001, after the terrorist attacks on September 11, he predicted that while the attacks would usher in greater attention to security technology, privacy would suffer more than ever at the hands of technology.[iii]

(SLIDE)

This conclusion, that privacy is dead, was also reached by security technologist Bruce Schneier in an article he wrote for CNN in March this year about the privacy dangers with new online technology.[iv]

He described the Internet as a surveillance, saying:

"Whether we admit it to ourselves or not, and whether we like it or not, we're being tracked all the time".

Google tracks us, as does Facebook, which even tracks non-Facebook users. Our iPhones and iPads allow Apple to track us. And so does the US Government if certain media reports are to be believed.

Schneier cited a reporter who used a tool called Collusion to discover that 105 companies tracked his internet use during one 36-hour period.

Yet despite such claims, and examples, I am pleased to confirm that privacy isn't dead. Yes, it has been put in the spotlight and sorely interrogated, but these challenges may yet have a positive effect. Particularly if they initiate public debate about what is acceptable, the

accountability to be demonstrated for any trade-off in privacy and the public is kept informed of changes.

Lord Justice Leveson (who oversighted the 2011 UK inquiry into the ethics and behaviour of the UK media) last year in Sydney put forward the view that, while new technology has raised fears about privacy, the passage of time, application of law and public pressure will introduce and reinforce social norms acceptable to the community.[v]

While many social commentators will continue to proclaim the death of privacy, the public's concern for privacy is clearly not dead.

Enquiries to our office on privacy related matters have increased by more than 300% in the past four years.

(SLIDE)

According to the latest Unisys Security Index[vi] released in May this year, the security concerns of the Australian public have hit their highest level in five years, with data privacy issues remaining the top security concern.

The Unisys Security Index is an annual global study into the attitudes of consumers.

As you can see on the slide, these concerns cover a range of issues such as unauthorised access to, or misuse of, their personal information, the unlawful use of credit and debit card details, unauthorised access or misuse of personal information, and data breaches at financial institutions.

Reality

Not only are privacy concerns growing, the reality is that privacy is essential to us all. As human beings we need to preserve our private spaces and enjoy private time in our lives, to reflect and enjoy moments of solitude.[vii]

Given the real dangers of such issues as identity theft and cyber fraud, the need to protect the privacy of our personal and financial information is greater than ever.

It seems contradictory, that while people seem to be sharing everything they do and think on the internet, their concerns about privacy have increased. But this is the case.

(SLIDE)

This concern for privacy is reflected across Australia's jurisdictions and internationally. Statistics collated by the Asia Pacific Privacy Authorities highlight some interesting numbers.[viii]

An illustrative sample:

- 78% of Australians refusing to provide personal information online;
- 92% of Canada's population believing companies should ask permission to track them online; and
- 88% of New Zealanders supporting punishment for businesses that misuse personal information.

The role of the Privacy Commissioner in our society

Against that background, my task today is to outline the role of a Privacy Commissioner. I'll also touch on our participation in the national law reform process.

But firstly, to the role of Privacy Commissioner…

As Privacy Commissioner of NSW I work under two Privacy Acts. There are other pieces of legislation in NSW that have privacy aspects such as the NSW *Workplace Surveillance Act,* and, in addition, a number of agencies such as the Roads and Maritime Services have privacy provisions in their own legislation.

The first Act that I work to is the:

NSW Privacy and Personal Information Protection Act 1998 (PPIP Act)

The PPIP Act covers NSW public sector agencies, that is, NSW Government agencies, local councils and universities. Unlike the Federal legislation it does not cover the private sector, although the functions of the Privacy Commissioner do provide a broader reach, which can be utilised when required.

My functions under the PPIP Act are listed in Section 36(2), and include (*it's rather a long list, so bear with me*):

- Undertaking inquiries and investigations as I find appropriate;
- Making public statements about the privacy of individuals;

- Reporting and recommending the need for legislative, administrative or other action;
- Initiating and recommending the making of privacy codes of practice;
- Promoting the adoption and compliance with the privacy principles, privacy codes of practice, public interest directions and privacy plans;
- Developing privacy guidelines;
- Investigating and conciliating complaints;
- Responding to enquiries and educating the community about privacy issues; and lastly
- Researching any matter that may impact on privacy, (including developments in technology) and making reports and recommendations to relevant authorities.

The Act also provides for the Privacy Commissioner, when undertaking inquiries and investigations, to have the powers conferred on Royal Commissions.

In addition, there is specific health privacy legislation, the:

NSW Health Records and Information Privacy Act 2002

The HRIP Act covers NSW organisations, both public and private, that deal with health-related information. There is some jurisdictional overlap here with the Federal Act.

Both pieces of legislation (the PPIP Act and the HRIP Act), like the Commonwealth legislation, are principle based. Both NSW Acts are concerned with the protection of personal (and health) information, not the generally broader concept of privacy as freedom from intrusion or of solitude.

Simply put, the role of a Privacy Commissioner is an acknowledgement that Parliament and citizens need an independent voice or champion to promote privacy rights, investigate privacy matters, and provide expert advice on privacy issues.

The championing of privacy rights is the paramount focus. But on some occasions, the Privacy Commissioner's role is frequently about striking a balance. For example, between protection of personal information and public access to information, between the privacy of individuals and the public interest issues in, for example, public safety.

Independence of the Privacy Commissioner

When agencies or individuals bring matters to the Privacy Commissioner, they need to know that it will be considered impartially. This is an important point because I am dealing with the government, community and business sectors. And people need to know that, whether I

am advising on policy matters, alleged breaches of the privacy principles or dealing with privacy enquiries, it will be done independently, without favour and according to the law.

I work within the NSW model of the Information and Privacy Commission, where the Privacy Commissioner and Information Commissioner have equal status in championing and administering their specific legislation, while working under one roof. The Information Commissioner is concerned with access to government information.

While our roles are independent, sometimes complementary and sometimes in tension, together we endorse strong information governance as a part of corporate governance.

It frequently comes as a surprise to some to realise that, as Privacy Commissioner, I have a strong interest in people being able to access information. This is because both NSW Privacy Acts allow people to actively check what is on public sector records about themselves and have that information corrected if it is inaccurate or irrelevant. Many applications under the former *Freedom of Information Act* and the current Government Information Access legislation have been from members of the public seeking information about their records.

The principles of privacy and open government complement each other, as they are integral to the healthy functioning of a democracy. They also secure the accountability of government, public officials and public servants to members of the public.

I and the Information Commissioner, Deirdre O'Donnell, are oversighted by a Parliamentary Committee – the Committee on the Ombudsman, the Police Integrity Commission and the Crime Commission. This is a joint statutory Committee and its functions, in relation to the Privacy Commissioner, are set out in Section 44A of the PPIP Act.

The Committee's functions include:

- Review of how I exercise the functions of Privacy Commissioner;
- Examination of the reports I release; and
- Recommending to Parliament any changes to the functions of the Privacy Commissioner that the Joint Committee thinks desirable.

The Committee's oversight does not extend to:

- Investigating a matter; or
- Re-considering a decision I make to investigate or not, a matter brought to my attention; or

- Reconsidering the findings, recommendations, determinations or decisions I make in relation to a particular investigation, complaint or matter.

We, the Information Commissioner and I, have appeared before the Committee on a number of occasions. Most recently the Committee has been addressing the accountability of the integrity agencies as demonstrated by performance measurement data.

Information and Privacy Advisory Committee (IPAC)

It is important that I also mention the NSW Information and Privacy Advisory Committee, which was established in March this year. The Committee provides advice to myself and the Information Commissioner on privacy and information access matters. The Attorney General also has the capacity to refer issues to the Committee.

The Advisory Committee's role in relation to privacy includes:

- Providing expert knowledge and experience;
- Strategic input to key projects undertaken by the Privacy Commissioner;
- Fostering communication with key stakeholders to promote the protection of privacy; and
- Promoting the value of privacy to the community.

Peter Timmins who spoke earlier this morning, Teresa Corbin from the Australian Communications Consumer Action Network and Samantha Yorke, who is speaking on privacy policies and social media tomorrow, are all members of our advisory committee.

There is a similar Committee Federally, the Privacy Advisory Committee, which assists and advises the Australian Privacy Commissioner on matters relating to privacy, and the Information Advisory Committee which advises the Federal Information Commissioner on matters relating to Information policy.

Collaboration

While it might be desirable to have one set of privacy principles that apply across Australia to both government and private sectors, currently there are both State and Federal privacy laws. And a Privacy Commissioner at each level charged with the responsibility of oversighting these different pieces of legislation.

There are differences between the Commonwealth and State legislation, and in the case of the health privacy legislation some overlap in jurisdiction.

Interaction between State and Federal Commissioners is vital – both in terms of working together to ensure that people have their privacy complaints dealt with quickly, and also in addressing the potential privacy impacts of either State or national initiatives. There has been considerable liaison, for example, between Commissioners and our offices on the national personally controlled electronic health record system.

In my experience, the Privacy Commissioners work well together on privacy matters affecting both complainants and emerging policy issues.

We meet under the auspices of the Privacy Authorities of Australia on a regular basis to share information and canvass privacy issues. This interaction complements and strengthens our knowledge base, highlights emerging issues, and provides a forum to discuss strategies and effective outcomes.

This interaction is complemented also by our membership of the international Asia Pacific Privacy Authorities network. A body supported and coordinated currently by the Office of the Australian Privacy Commissioner. There are, I recall, around fifteen member countries in this network.

The relationship between the Office of the Australian Privacy Commissioner and my office is based upon collaborative principles.

These principles enable the two jurisdictions to work well together. Our combined focus is on ensuring the best outcome for the applicant. This is a key principle based on a customer and service focus.

Other specific collaborative principles relate to:

- Sharing information about any projects, activities or developments that may affect each other's responsibilities;
- Undertaking joint investigations where appropriate; and
- Sharing knowledge and resources.

Working relations are strong with the Federal Commissioner. Essentially we protect the same privacy rights for different sectors of the Australian population.

Privacy Law Reform

Another part of my role is to advise the NSW Parliament and NSW Attorney General on Privacy Law Reform in NSW.

My office also contributes to consideration of proposals for new Federal privacy legislation or other initiatives or legislation with privacy impacts across the States and Territories. Typically, such submissions address the alignment of proposed reforms with State legislation.

The Federal privacy law reform process commenced in 2006 with the referral from the Federal Attorney General to the Australian Law Reform Commission for an inquiry into the extent to which the Privacy Act and related laws provided an effective framework for the protection of privacy in Australia. The State and Territory Privacy Commissioners had the opportunity, with others, to provide submissions to the committees throughout the process.[ix]

For example, our office provided submissions to the Senate Finance and Public Administration Legislation Committee. Our submissions considered the definition of personal information and consent, and the proposed Australian Privacy Principles (or APPs).[x]

On the latter we particularly sought the simplification of the complex wording so these principles could be more easily understood by the general public.

We also made specific recommendations concerning certain Privacy principles:

In APP 1 (open and transparent management of personal information) we recommended the requirement to disclose the provision of personal information when it goes outside the jurisdiction in which the person resides.

In APP 6 (use or disclosure of personal information) we suggested extending the principle to any circumstances in which personal information is used or disclosed for a secondary purpose.

We also expressed a view on including an APP on reporting data breaches. It was good to see the Mandatory Data Breach Bill introduced on 29 May to Federal Parliament. The expectation is that the breach notification changes, if passed, will take effect at the same time as the privacy law reforms in March 2014[xi].

A statutory cause of action for serious invasion of privacy

We broadly support the development of a statutory cause of action for serious invasion of privacy. Our preference is that any such privacy cause of action is based in legislation in the States and Territories rather than left to judicial development by case law or common law.

Legislation can provide greater consistency and access to the cause of action than might be the case if it is left to be developed by the Courts.[xii]

The wish to see a statutory tort is prompted by the rise of technology and its application to our daily lives with its increased potential for privacy invasions. Basically, to give the means to address the situation where, as Lord Leveson has described it, "There is not only a danger of trial by Twitter, but also of unending punishment, and no prospect of rehabilitation, by Google".[xiii]

(SLIDE)

It is important when the Federal privacy law reforms commence in March 2014, that the community understands what these changes mean for their privacy rights, as well as Government and business addressing the new requirements.

The benefits of the main changes include:

- More transparency from all business and federal government agencies in identifying the minimum information that must be contained in a privacy policy. This includes how they use, store and dispose of personal information, and making it clear how to make a complaint.

  Building privacy in from the outset (known as 'Privacy by Design') is part of good governance and should be a matter of protocol. It's a proactive approach that can prevent breaches and other issues arising later.

- Changes to direct marketing such as the provision of an "opt-out" option. (We would have preferred an "opt in" system as we consider this best practice for protecting privacy for individuals.)
- Changes to the credit reporting system will include, in most circumstances, the ability to request a copy of your credit reporting file at no cost.

Enhanced powers of Federal Privacy Commissioner

Another significant legislative change is the enhanced powers of the Federal Privacy Commissioner.

This will include the ability to:

- conduct performance assessments at any time on private sector organisations;
- approve and register enforceable codes; and
- impose penalties on organisations of up to $1.7 million, and the provision of enforcement powers and remedies in regards to own motion investigations.

As NSW Privacy Commissioner, I do not have determinative powers. Complainants, if they are unhappy with the outcome of internal reviews undertaken by NSW public sector agencies, can take matters to the NSW Administrative Decisions Tribunal for determination.

The way forward

The Federal law reforms are an important turning point for privacy in Australia. It is sensible that government agencies and the private sector work under a common set of national privacy principles. This will make it easier also for the community to understand their rights and to exercise these.

Our shared future challenge will be to make sure the community is aware of the changes, where they apply and where they don't, to closely monitor how the changes work, where refinement might be needed and how emerging privacy challenges can be met. My specific interest will also be in monitoring the changes for the provision of advice as to if, and how, NSW legislation could be improved.

(SLIDE)

Conclusion

I think I can speak for other State and Territory Privacy Commissioners when I say that we welcome the privacy law reforms.

Thank you for your time today. I look forward to further discussing the privacy law reforms and their impact during the round table discussion.

[i] United Nations, *Universal Declaration of Human Rights*. The Declaration is the basic international pronouncement of the inalienable and inviolable rights of all members of the human family. The Declaration was proclaimed in a resolution of the General Assembly on 10 December 1948 as the "common standard of achievement for all peoples and all nations" in respect for human rights.

[ii] www.wired.com/politics/law/news/1999/01/17538

[iii] www.computerworld.com/s/article/64729/McNealy_calls_for_smart_cards_to_help_security

[iv] edition.cnn.com/2013/03/16/opinion/schneier-internet-surveillance

[v] The Right Honourable Lord Justice Leveson, "Privacy and the Internet", Communications Law Centre, University of Technology, Sydney, Australia, 7 December 2012.

[vi] www.unisyssecurityindex.com/usi/australia
http://www.businessspectator.com.au/news/2013/5/27/technology/data-breaches-leave-australian-public-fuming

[vii] Ontario Information and Privacy Commissioner, Ann Cavoukian, PhD, Ontario Canada.

[viii] Asia Pacific Privacy Authorities (APPA) Infographic, April 2013 – www.privacyawarenessweek.org/resources.html

[ix] The Australian Law Reform Commission's final report was released in 2008 following submission from a range of bodies including the Federal and State and Territory Privacy Commissioners. In 2009, the Australian Government released the first stage of its response to the report. This response addressed 197 of the 295 recommendations made by the Australian Law Reform Commission. In mid 2010, Government released Exposure Draft Legislation upon its first stage response. The Senate Finance and Public Administration Committee received draft legislation for review and report. The Senate Committee released reports into the draft Australian Privacy Principles and the draft credit reporting provisions in 2011. In September 2011, the Government released an issues paper on the right to sue for serious invasion of personal privacy. Again, Privacy Commissioners at State and Territory level had the opportunity to make submissions. This time to the house Standing Committee on Social Policy and Legal Affairs, and the Senate Legal and Constitutional Affairs Legislation Committee for inquiry and report. Both Committees reported in September 2012. The Reform Bill passed Parliament in November 2012 and received Royal Assent in December 2012.

[x] www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/vwFiles/s100853.pdf/$file/s100853.pdf

[xi] dataguidance.com/news.asp?id=2034

[xii] Our preference is that there are two separate causes of action. They are misuse of private information; and Intrusion upon seclusion.

[xiii] The Right Honourable Lord Justice Leveson, "Privacy and the Internet", Communications Law Centre, University of Technology, Sydney, Australia, 7 December 2012.