Australian Government
Office of the Australian Information Commissioner

Protecting information rights – advancing information policy

Privacy law reform – getting the balance right

Timothy Pilgrim presentation to Communications and Media Law Association, 6 September 2011

I would like to begin by acknowledging the Gadigal peoples of the Eora Nation, the traditional owners of the land on which we meet today, and to pay my respects to their elders, both past and present.

Scott McNeally, co-founder of Sun-Microsystems famously said in 1999 that "You have zero privacy – get over it".

Every day there is a substantial growth in the amount of personal information that is available online, and technology continues to bring new opportunities for information sharing. The phenomenal growth of the internet, e-commerce and the international flow of vast amounts of personal information, able to occur in seconds, has created a brave new world for privacy.

It is interesting to look more recently at what some influential people in the field have said.

Mark Zuckerberg, the founder of Facebook, commented that:

"...when I got started in my dorm room at Harvard, the question a lot of people asked was why would I want to put any information on the Internet at all?"

But he then went on to say that:

"...people have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time."

And further that:

"You have one identity. The days of you having a different image for your work friends or co-workers and for the other people you know are probably coming to an end pretty quickly." And: "Having two identities for yourself is an example of a lack of integrity."

Eric Schmidt, the Executive Chairman of Google, said in 2010:

"I don't believe society understands what happens when everything is available, knowable and recorded by everyone all the time."

Today we are clearly in the midst of a social media revolution in which Facebook alone has 750 million users.

The fact that what you post today may cause grief tomorrow seems to elude many social media enthusiasts, so much so that Eric Schmidt also predicted in 2010 that:

"... every young person will be entitled automatically to change his or her name on reaching adulthood in order to disown youthful hijinks stored on their friends' social media sites."

So in 2011, this environment, why are we now looking at the potential for the introduction of a statutory cause of action to be enacted through the federal Parliament? Why on two occasions recently has Facebook announced changes to its privacy settings in response to its users' concerns?

Interestingly, in further elaborating on Facebook's role in the system, which he said is to reflect what the current social norms are, Mark Zuckerberg has also noted that:

"a lot of companies would be trapped by the conventions and their legacies of what they've built. Doing a privacy change – doing a privacy change for 350 million users, is not the kind of thing that a lot of companies would do."

"But we viewed that as a really important thing, to always keep a beginner's mind and what would we do if we were starting the company now and we decided that these would be the social norms now and we just went for it."

This evening, I'll ponder only some of these issues, as we wouldn't have time to work through all the possible answers, nor would I be silly enough to think that I even have "the answer".

I'll consider instead where we are now with privacy law in Australia in the context of the work we do in our office, looking at some of the cases that we have been involved with recently, and through developments in the law reform process.

But first a little history.

Warren and Brandeis

In 1890, Samuel D Warren and Louis D Brandeis (who later became a US Supreme Court judge) pioneered the idea of a right to privacy – a right to be "let alone"[1]. This was in response to the emergence of new technologies, such as instantaneous photographs, and the rise of the newspaper enterprise, which, in their words, "have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that what is whispered in the closet shall be proclaimed from the house-tops."

Jumping nearly a century later and across the Pacific to Australia, in 1969 Sir Zelman Cowen, an eminent Australian jurist and scholar who was later Governor-General of Australia, delivered the ABC's annual Boyer Lectures.

His series of six lectures – *The Private Man* – explored the serious threats to individuals arising from the emerging era of computerised information. Sir Zelman observed that:

" ... A man without privacy is a man without dignity; the fear that Big Brother is watching and listening threatens the freedom of the individual no less than prison bars."

In the late 1970s and 1980s, Australia made a conscious decision to consider the legal standing of privacy as a party to the International Covenant on Civil and Political Rights, of which Article 17 states**:**

No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

and

Everyone has the right to the protection of the law against such interference or attacks.

This recognition of privacy as a human right and deserving of the protection of law is one of the reasons why we have the *Privacy Act 1988*.

This was also the period that saw the then government attempt to introduce the "Australia Card" against much opposition within and outside the Parliament. There were even protest rallies against the proposal.

It is interesting to remember that while the Australia Card proposal was scrapped following a double dissolution election held over the issue, the accompanying Privacy Act was passed through the Parliament in 1988.

The Act at that time only covered Commonwealth Government agencies and Tax File Numbers. It was amended in the early 1990s to cover credit information and then, more significantly, in 2000 the coverage of the Act was extended to cover much of the private sector. This was in recognition of the increasing consumer confidence in e-commerce, and also in an attempt to gain European Union adequacy.

However, the amendments to the private sector had some notable exceptions, including the media and political organisations. And this starts to raise the question of potential gaps in privacy protection.

Then, following a recommendation from the former Office of the Privacy Commissioner and a Parliamentary Committee in 2005, the then Government gave a reference to the Australian Law Reform Commission (ALRC) to review the whole Act in the context of a rapidly changing global and technological environment. This review made 295 recommendations for changing the Privacy Act. But a bit more of that later.

Before I consider why we are seeing a renewed interest in privacy, let's look at what privacy is. The type of privacy covered by the Privacy Act is the protection of people's personal information. However, this is just one aspect of privacy.

Other types of privacy can include territorial privacy, physical or bodily privacy and privacy of your communications. And as these are not covered by the Act, here we see some more potential gaps.

Our enquiries line, for instance, receives numerous calls relating to issues of bodily, territorial and informational privacy that are not covered.

What is privacy?

The Act defines personal information as "... information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion."

This is a deliberately broad definition and reflects the power holding such information can have on the day-to-day lives of people. In the business context, for example, personal information is often seen as an asset; however, I would say that it is a unique kind of asset.

Whereas an organisation may hold physical assets such as office equipment and photocopiers, if these are lost they are easily replaced. While personal information is undoubtedly an asset for business – it is profoundly different from other types of assets. When it is lost or misused, the consequences for individuals and businesses differ significantly.

For the individual there is:

- The potential loss of control over who knows what about an individual
- The risk that people can be using the information about them for unwanted contact – and this could be through relatively benign ways such as such as marketing through to more serious physical concerns
- Vulnerability to the threat of identity theft and fraud and the trouble of changing a raft of details – like credit cards and bank accounts.

There can also be significant problems for individuals in getting the integrity of their identity back.

And for businesses, there is the damage to their reputation.

Just to put identity theft in context:

Professor Iain Morrison, head of Bond University's IT School, recently predicted that more than one million Australians will fall victim to information and computer fraud this year, and that computer fraud will cost $3 trillion around the world in 2011.

Indeed, a Newspoll survey conducted in December last year found 23 per cent of Australian workers have received a phishing scam through a social networking site. Interestingly, another survey of 1200 consumers by technology company Unisys found that Australians are more concerned about identity theft and financial fraud than terrorist attacks.

People were asked if they were more or less concerned about security issues than they were 10 years ago (and remember that 2011 marks the 10th anniversary of the September 11 terrorist strikes in the US). While Australians remain concerned about terrorism, with 42 per cent saying they were more concerned about the risk of airline hijackings and 51 per cent were more concerned about suicide bombs, 76 per cent of Australians were even more concerned about their credit card data being stolen, and 59 per cent about companies losing their personal or financial details.

Unisys Security Program Director John Kendall commented that although concerns about "traditional" national security threats persist, "more contemporary issues... have greater potential immediacy" for most people.

So for the individual, personal information is not just like losing a physical asset that can be replaced. This is why the Privacy Act requires businesses and Australian Government agencies that handle personal information to have robust privacy practices in place. The benefits of having access to personal information come with responsibilities, such as a responsibility to use that information only in ways which the Act allows or the person has agreed to in order to get the service or the product they want.

Privacy in the headlines

There is no doubt that the *News of the World* events and the continuing incidents of data breach have sparked a growing interest in privacy. The Office of the Australian Information Commissioner (OAIC) has investigated a range of data breaches in recent years**.**

High-profile cases include:

- Google, who in May 2010 breached the Privacy Act by collecting unsecured WiFi payload data in Australia using Street View vehicles.
- Telstra, who in a mail-out in October 2010, breached the Privacy Act by misdirecting the personal information of 60,300 customers – a one-off, human error.
- Vodafone, who I investigated earlier this year and found did not have appropriate security measures in place to protect customer's personal information. I was particularly concerned by Vodafone's use of shared logins and passwords for staff and the broad range of detailed personal information available to them.
- Sony Playstation Network My own motion investigation into Sony began in April this year and continues as we examine what happened to the personal data, including credit card details, of more than 77million users when Sony was hacked into.
- Another case you may have heard about in July was an incident involving a medical laboratory, Medvet, which allegedly resulted in the online publication of the personal details of people seeking paternity and drug tests.

These cases provide an insight into how data breaches can occur. It could be because of:

- human error
- a failure to comply with obligations in regard to the use and disclosure of personal information
- a failure to take reasonable steps to protect personal information from misuse and loss or from unauthorised access, modification or disclosure
- or something more insidious, such as when personal information held by a company is stolen or 'hacked' into.

The investigations I have just mentioned are notable because of the large numbers of people affected and the sensitivity of the information disclosed.

As you would expect, there are many other cases of data breach that do not make news headlines.

Data breaches you won't have read about in the press that we have investigated include:

- incidents involving the loss or theft of data sticks, documents and computers containing personal information
- mail misdirection, particularly mistakes made using email
- unauthorised employee access to and misuse of customer information.

We have even had a case where documents containing personal information turned up in the drawers of used furniture sold at auction.

In the last financial year, the OAIC received 56 voluntary data breach notifications (or DBNs), up from 44 in the previous year.

We also initiated 59 own motion investigations – and it is highly likely that among these are matters that should well have been DBNs.

Collectively, these incidents have highlighted the issue of mandatory data breach notification or DBN, one of many of the ALRC's recommendations for reform of Australia's privacy regime.

While there is much public attention given to DBN through media reporting, it is useful to put these kinds of incidents in the context of the OAIC's broader compliance workload. Each year we receive around 1200 complaints and more than 20,000 enquiries – either by phone or in writing.

Current law and DBN

By way of getting into discussion of the privacy law reform process, I'll just mention where the law stands now for data breaches.

The Information Privacy Principles (IPPs) and the National Privacy Principles (NPPs) in the Privacy Act do not impose an obligation on agencies or organisations to notify individuals whose personal information has been compromised.

However, the Act does require that agencies and organisations take reasonable steps to maintain the security of the personal information they hold. Failure to do so constitutes a breach of our current laws. The OAIC recommends notification to affected individuals, and in certain cases, to the Privacy Commissioner, as one of the steps in our best-practice guide to data breach handling that you can find on our website.

Despite the current absence of a legal requirement, it is my view that prompt notification should be considered as a matter of course in any situation where a data breach gives rise to a risk of real and serious harm to the individuals whose information has been disclosed.

It's worth mentioning that calls for mandatory data breach reporting are not new: they go back several years, with the Australian Democrats Senator Natasha Stott-Despoja calling for reform through a Private Member's Bill in 2007.

There is no doubt that data breaches cause concern in the mind of the public and lead to calls for tougher regulation, particularly if there is a perception that organisations are not

treating them seriously – or worse, trying to cover them up. Consequently, data breaches pose a serious reputational risk to business.

However, an even greater reputational risk confronts organisations found to be either hiding a breach, or doing nothing about it. This will ultimately impact on consumer trust and make people reluctant to deal with them in the future. This is perhaps one of the reasons why the organisations involved in those high-profile cases I mentioned have been extremely cooperative in working with us to resolve the issues.

Law reform process

Data Breach Notification was among 295 recommendations for amendments to the Privacy Act in the 2008 Australian Law Reform Commission *Report 108 – For Your Information: Australian Privacy Law and Practice*, the extensive review into Australia's privacy laws.

Other amendments recommended by this review included:

- a new set of harmonised privacy principles to cover both the public and private sectors
- provisions introducing comprehensive credit reporting to improve individual credit assessments and supplement responsible lending practices
- provisions relating to the protection of health information
- a statutory right to privacy
- a review of the exemptions to the Act, including clearer definitions around the scope of the journalism exemption.

Given the size of the ALRC's report, the Government decided to respond in a two-stage process.

A first stage response to 197 of the 295 recommendations contained in the ALRC report was released in October 2009 and the Government is still in the process of implementing these changes.

The first stage covers:

- New privacy principles
- Credit reporting provisions
- Health provisions
- Additional powers for the Commissioner.

Australian Privacy Principles (APP)

We are currently in the process of moving towards a single set of privacy principles covering both the public and private sectors in Australia and an exposure draft of these was released by the Australian Government earlier this year.

The proposed 13 APPs are structured to reflect the information life cycle – from collection, through to use and disclosure and access and correction.

Currently, there is one set of principles covering the Australian, ACT and Norfolk Island Governments and a separate set of principles covering business. A single set of principles will simplify privacy obligations in Australia and reduce confusion and duplication.

This is not without its challenges.

Australian Government agencies have been working with the Information Privacy Principles (or IPPs) for 23 years, while the private sector has been covered by the National Privacy Principles (or NPPs) for only 10.

The new draft principles more closely reflect the wording of the NPPs, so the change for government agencies will be potentially bigger.

They also introduce concepts that government agencies haven't had to consider as part of the IPPs – such as sensitive information and the associated need for consent, and a specific trans-border data flow principle.

Sensitive information

For the first time, for example, there will be specific requirements on the way government agencies can collect sensitive information. Sensitive information is a subset of personal information and is defined to include information relating to:

- Race or ethnic origins
- Political opinions and membership of political associations
- Religious or philosophical beliefs
- Membership of a trade union or of a professional or trade association
- Sexual preferences or practices
- Criminal record
- Health information.

Sensitive information is a particular class of personal information that, if misused, can be particularly damaging to the individual concerned.

Cross border information

While this will be a new concept for the Government sector, the new principle also represents some significant changes to the existing cross border principle that the private sector has been used to for the last 10 years. The new draft principle introduces the concept of accountability. This means that entities will remain accountable for any disclosure of personal information outside Australia, unless one of a number of exceptions applies.

Some organisations have raised concerns about how far this 'chain of accountability' would extend. For example, if an organisation contracted a function to an overseas entity, and so made a cross border disclosure, and that overseas entity then engaged a subcontractor, should the organisation be accountable for the way the subcontractor handles the personal information?

In order to give effect to this provision's intent, it is my view is that the chain of accountability would not be broken simply because the overseas entity engaged a subcontractor. The intent of this Principle is to ensure that people can enforce their privacy rights, even when organisations send their personal information offshore.

New credit reporting provisions

Credit reporting has been regulated under the Privacy Act since the early 1990s. In February this year, the Government released an exposure draft of the new credit reporting provisions, and we support the move to simplify these and make them more user-friendly.

Additional powers

The Government has indicated that it will introduce new laws to strengthen the powers of the Privacy Commissioner.

Under the current Privacy Act, we are unable to impose a penalty on an agency or organisation when we have initiated an investigation on our own motion, without a complainant. Our role is to work with the agency or organisation to ensure ongoing compliance and better privacy practice.

The Government has not yet released exposure draft legislation in this area, but it has stated that it intends to make amendments so that the Privacy Commissioner can:

- make an enforceable determination on an own motion investigation
- accept undertakings from agencies or organisations and, if necessary, enforce those (through a court)
- seek (through a court) a civil penalty for serious or repeated offences.

At the end of the day, I would rather not have to use such powers. Our recent experience in relation to the Google Street View and Vodafone cases show how agreed undertakings can operate successfully.

Nevertheless, overseas experience has indicated that regulators with the power to pursue large penalties will often do so. The United States is perhaps the best example of this.

One of the most notorious data breaches in the US was the disclosure by ChoicePoint, a large identification and credential verification organisation, of sensitive information it had collected on 145,000 individuals. In this case, a Federal Trade Commission (FTC) investigation led to the imposition of a $15 million fine.

More recently, the FTC investigated Google when Gmail users were opted in to the new social networking platform 'Buzz' by default and their personal information – including which other Gmail users they interact with most – was made public.

As a result of its investigation and as part of its settlement, the FTC now requires Google to enact a consumer privacy protection program by implementing a comprehensive privacy policy and submitting to privacy audits by independent parties every second year for the next two decades.

Additional powers for the Privacy Commissioner will provide added credibility for enforcement of privacy law, reinforce the significance of privacy compliance, and give everyone an even greater incentive to take privacy more seriously.

Current exemptions from the Privacy Act

As you are no doubt aware, there are a number of exemptions from the Privacy Act, and this again raises the question of gaps in the system.

I'll now touch on some of these and mention some of the recommendations for reform made by the ALRC – and I should note here that Government is yet to respond to these.

Small business exemption

Generally speaking, small businesses – namely, those with an annual turnover of $3 million or less – are exempt from the operation of the Privacy Act, and it has been estimated that up to 94% of Australian businesses may fall under this exemption.

The small business exemption has been scrutinised by four separate inquiries since 2000, when the Privacy Act was extended to the private sector. The ALRC recommended that the small business exemption should be removed, noting that there would be a need to minimise unnecessary compliance costs on small businesses.

Employee records exemption

While the employee records of public servants have been covered by the Act since 1988, other employee records are not covered by the Act.

These kinds of records contain a great deal of personal information that could cause harm to someone if used or disclosed inappropriately – things like the terms and conditions of employment, salary and leave details, taxation, banking or superannuation affairs as well as the employee's trade union membership.

The ALRC was particularly concerned about the lack of adequate privacy protection for employee records in the private sector. So the ALRC recommended that the employee records exemption should go.

The former Office of the Privacy Commissioner (or OPC) supported this proposal because it strengthens the protection of employees' rights as private citizens and creates greater certainty about rights and obligations for both employers and employees.

We also saw value in eliminating the regulatory difficulties an organisation might face in interpreting the exemption, and also opening up our conciliation-based complaints processes to employees.

Political exemption

The ALRC has called for the removal of the exemption for registered political parties and the partial exemption currently applicable to Australian Government Ministers. The former OPC submitted that privacy protection may be enhanced by requiring political parties to comply with key privacy principles, but, as with the other exemptions, it remains to be seen what the Government will do on this issue.

The ALRC also recommended amending the Privacy Act to provide that the Act does not apply to the extent, if any, that it would infringe any constitutional doctrine of implied freedom of political communication or parliamentary privilege.

Journalism exemption

And now to the journalism exemption, which will probably be of most interest to you tonight. As you will be aware, the practices engaged in by media organisations in the course of journalism are exempt from the operation of the Privacy Act, provided the organisation meets certain requirements, including being publicly committed to standards that deal with privacy. This exemption is said to promote the public interest in freedom of expression and the free flow of information critical to the maintenance of a democratic society.

However, the ALRC's consultation raised some concerns about the nature and operation of the journalism exemption. Some of these include:

- The broad scope of the exemption
- The lack of criteria and independent assessment of media privacy standards
- The adequacy of the regulatory model
- The lack of strong enforcement mechanisms in some media sectors.

While the ALRC supported the journalism exemption, it recommended a number of improvements to its application, and I'll now consider some of these.

The ALRC noted that self-regulatory mechanisms do not provide the complete answer to the task of balancing competing public interests in privacy and freedom of expression. The ALRC considered that, unlike for other professionals – for example, financial advisers and lawyers – journalists have no *requirement* for formal educational. Nor are there compulsory requirements for accreditation or registration.

In this context the ALRC has recommended that components of the journalism exemption be more clearly defined. First, the ALRC noted that the lack of definition of the term 'journalism' was problematic. It suggested that 'journalism' be defined to limit the scope of the exemption to acts and practices that are associated with a clear public interest in freedom of expression.

Similarly, the ALRC suggested amendments to the definition of the term 'media organisation' – to avoid unnecessary circularity with the 'journalism' definition and to allow flexibility in the provisions as new media platforms continue to evolve.

The ALRC believes these new and changed definitions would address comments made by a number of stakeholders, who in their submissions, questioned whether the proposed definitions would exclude emerging mediums for conducting journalism, such as blogs.

For example:

The Australian Library and Information Association commented that the concept of 'the media' is changing rapidly, and suggested that protection might need to be widened to encompass this broad range of mediums.

The Australian Press Council noted that journalism

"... is something more than just the straight reporting of, and commentary on, matters of economics, politics and social developments. Sports, travel, food and leisure, film, music and books, and popular culture are all as worthy of coverage, in the public interest."

The Right to Know Coalition also questioned whether advertisements could be excluded from the definition of journalism, noting that this approach could result in material presented in a news or current affairs story falling within the journalism exemption, but the exemption not applying where the same material is presented in an advertisement for the story.

These are interesting discussions that I am sure will continue as the reform process progresses.

Media privacy standards

Another recommendation by the ALRC was a new requirement that media privacy standards must deal 'adequately' with privacy in the context of a media organisation's activities.

In light of the events around the *News of the World*, this is a salient point.

The public's right to know must continue to be balanced against individuals' right to privacy – and we know that what the public is *interested in* is not necessarily the same as what is in the public interest.

During the ALRC consultation process, some people questioned whether the media privacy standards that exist today are sufficient to guard against breaches of privacy if media organisations or journalists behave irresponsibly.

Most media organisations are subject to a range of **voluntary** industry standards – for example, those developed by the Australian Press Council for the print media – and to regulations made under law – such as codes of practice approved and registered by the Australian Communications and Media Authority (ACMA) in respect of the broadcast media.

However, it has been argued that this regulation does not provide real remedies for individuals whose privacy rights have been affected. In this context, the ALRC has identified a range of options for enhancing the operation of the 'commitment to privacy standards' requirement, including the requirement that media privacy standards deal with privacy in an 'adequate' way.

The ALRC's view is that in order to qualify for the journalism exemption, organisations should be publicly committed to 'adequate' privacy standards that relate to the particular activities undertaken by a media organisation. Public commitment is regarded as an important mechanism to ensure that any standards being relied upon will be robust – while respecting the need for a high degree of media autonomy in order to protect freedom of expression.

To promote regulatory certainty, the ALRC also recommended that clear guidance explaining how the requirement for adequacy would be assessed should be developed by the OAIC in conjunction with the ACMA.

A statutory cause of action for serious breach of privacy

Another significant recommendation proposed by the ALRC that you have probably heard about is a statutory cause of action for breach of privacy. This would give individuals, in certain circumstances, a right to sue for serious invasion of privacy.

The ALRC's proposed statutory cause of action would be applicable in situations where there was a serious invasion of privacy and there was a reasonable expectation of privacy.

The ALRC also proposed that the court should take into account whether the public interest in maintaining the claimant's privacy outweighs other matters of public interest or public concern and the public interest in allowing freedom of expression.

Although initially scheduled for consideration during the second stage of the law reform process, the Government has announced that it intends to release an issues paper on this matter in the near future.

In terms of my own view, I welcome this debate.

The former Office of the Privacy Commissioner supported this recommendation in its submission to the ALRC. I believe that a statutory right to privacy would clearly establish that privacy is a human right that warrants specific recognition and protection within the Australian community – and also in a way that accords with community expectations and understanding of the meaning of 'privacy'. A statutory cause of action could also complement the existing, legislative-based privacy protections afforded to individuals and address some of the gaps that presently exist in both the common law and legislation.

However, could other approaches address these same gaps?

For example, if the Privacy Act were to be amended in the following ways, this may address the gaps in a similar manner to the proposed statutory cause of action:

- to introduce mandatory data breach notification
- to remove all the exemptions that I mentioned earlier
- to extend coverage to individuals and to interferences with territorial and bodily privacy
- to strengthen the Commissioner's powers.

But would this be an appropriate role for the Privacy Act, and indeed for the Australian Information and Privacy Commissioners?

These are just ideas for consideration. But going back to the statutory cause of action, I stress here this evening (as I have done throughout all media discussions I have had on this issue) that the right to privacy is not absolute: it should always be balanced with other human rights and social interests. One of these is freedom of expression. The public interest in continuing to allow the public to be informed about matters of public concern is an important consideration to balance against the right to privacy.

Exemptions and statutory right

So how would exemptions sit with the proposed statutory right to privacy? The ALRC has proposed that the journalism exemption in the Privacy Act should not extend to the recommended statutory cause of action.

The Government is yet to respond to this suggestion and it is one that will no doubt be considered in the forthcoming issues paper when it is released for community consultation and comment. Many media organisations have campaigned vigorously against the application of a statutory cause of action to acts and practices that fall within the journalism exemption in the Privacy Act.

It is very important that Australia has an independent and active media, and that Australians continue to enjoy freedom of expression. Any changes to the law will need to strike a balance between privacy and freedom of expression.

Through its issues paper, I expect that the Government will be consulting extensively to ensure that the views of the media and the wider community are heard as these reforms progress.

It's important to remember as we consider privacy reform and the statutory cause of action, that these proposals stem not just from the events surrounding the *News of the World*, but from a lengthy law reform process.

This process was based on a comprehensive review of the Privacy Act, undertaken in the context of a rapidly changing technological environment and changing community expectations.

Conclusion

So to wrap up, why does privacy continue to be an issue for people?

Well, it could be put this way: at the end of the day, privacy is about what we think, what we believe and value, what we want and what we want to do ... basically, who we are – it is the detail of what makes us unique.

It is also about having the greatest ability to control who gets to know these things about us.

But it can't be an absolute in the society in which we live – and in that sense, privacy law reform is about trying to find the balance.

Thank you.

---

[1] Louis Brandeis & Samuel Warren, "The Right to Privacy," 4 Harvard Law Review 193-220 (1890-91)