SPEECH

Australian Government
Office of the Australian Information Commissioner

Update your privacy settings

Privacy Law Reform 2014

Presentation by Australian Privacy Commissioner Timothy Pilgrim to CAMLA, Henry Davis York Level 10, 44 Martin Place, Sydney [7 March 2013]

Introduction

I would like to begin by acknowledging the Gadigal people 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.

Thanks for having me here tonight. I last spoke to you about 18 months ago, in September 2011. Much has changed in the privacy environment since that time — 18 months ago the News of the World scandal was in the headlines and there was much discussion about a statutory right to privacy.

Privacy in the headlines

Not surprisingly privacy has rarely been out of the news since that time. In the UK, we have seen the release of Lord Justice Leveson's report on the culture and ethics of media in which privacy featured heavily.

In North America, we have seen the release of guidance and draft legislation on mobile apps and privacy. And the Federal Trade Commission has finalised settlements with mobile app developers and online companies involving significant amounts of money.

In Europe the EU is considering changes to European data protection laws to reflect changes in technology, and on behalf of the European Data Protection authorities the French DPA continues to monitor the activities of Google.

Here, we've seen some significant data breaches involving some well-known brands — LinkedIn, Telstra, Dell, Sony, not to mention, the hack by Anonymous of the ABC website just last week. The Australian Government introduced a discussion paper on Mandatory Data Breach Notification and the privacy law reform bill passed Parliament. We have also seen the rise of drone technology and the increasing frequency of media outlets using these devices, and the ease with which individuals can purchase them. This is an emerging area and we still don't know what privacy impacts it will have.

The continuing level of public interest in privacy confirms the importance of enhanced privacy protections for individuals, and embedding privacy-by-design in 'business as usual' processes. Privacy issues continue to make front page news and many high profile organisations have come under public scrutiny.

In 2011–12, our office received 285 media requests, a 28% increase on the previous year. Over 90% of these enquiries related to privacy.

And in the 2011–12 financial year, the office received:

- 1357 privacy complaints (an increase of 11% from the previous year)
- around, 9000 telephone enquiries
- 1541 written enquiries.

We are also seeing figures from the current financial year showing that we are on track to receive even more complaints this year.

And it is important to note that it's not just the OAIC that receives privacy-related complaints:

- the Telecommunications Industry Ombudsman and the Financial Services Ombudsman each get close to 1,000 privacy specific complaints a year
- some large Australian Government agencies also receive around 500 privacy complaints per year

- and of course there are privacy regulators at the state and territory level, handling privacy complaints in their jurisdictions.

These figures indicate that people are actively looking to exercise their privacy rights.

Of course, privacy is also increasingly of concern to businesses. Recent high profile data breaches not only demonstrate the importance of privacy protection to individuals, but also to businesses, particularly in terms of customer trust and reputation.

It is therefore no surprise that privacy law reform has become a priority for the Government as well as the public. It is fair to say that the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* will bring about the most significant changes in privacy regulation and compliance for over two decades.

I was very pleased to see it reported in *Lawyers Weekly* last week that privacy reform is the chief concern for corporate counsel in 2013, according to an Allens survey of in-house lawyers. As I will explain, it is important that lawyers pay attention to these reforms as they will play a key role in assisting their clients to understand and comply with these new requirements.

The law reform process started several years ago, and it feels as though we have been talking about it for quite a while but on 12 March 2014 the new law will commence. So today we are almost 12 months to the day when we will have the new law in place.

Outline

In the time I have with you this evening, I would like to set out some of the key changes to the Privacy Act and how they may affect your role as a legal practitioner, as well as your role within an organisation that handles personal information.

In particular, I will talk about two significant areas of reform:

- the new Australian Privacy Principles (or APPs)

- the enhanced powers of the Commissioner

And I will let you know how we will assist you and your clients prepare for the changes.

I would also like to briefly touch on some other important developments in privacy including:

- our new *Guide to Information Security* on 'reasonable steps' that can be taken to protect personal information, and
- the mandatory data breach notification discussion paper.

Let's look now at law reform. The APPs are one of the most important changes that you will need to be aware of as legal practitioners.

APPs

The 13 new privacy principles will apply to both Commonwealth agencies and private sector organisations. Under the APPs, government agencies and businesses are referred to as 'APP entities'.

These unified principles replace the existing Information Privacy Principles (or IPPs) and National Privacy Principles (or NPPs) that apply to government agencies and businesses respectively. As lawyers you will no doubt welcome the simplicity of working with one set of principles, particularly when advising clients that provide contracted services to government.

The APPs are structured to more closely reflect the information lifecycle — from notification and collection, through use and disclosure, quality and security, to access and correction. They aim to simplify privacy obligations and reduce confusion and duplication.

I want to cover some of the detail on a few of the APPs for you so I have selected some that I think will be of interest.

APP 1 Manage personal information in an open and transparent way

The intention of APP 1 is to promote a 'privacy by design' approach — to ensure that privacy compliance is included in the design of information systems and practices from inception.

Under APP 1 an entity must take such steps as are reasonable in the circumstances to ensure compliance with the APPs or a registered APP code that binds the entity.

According to the Explanatory Memorandum, the phrase 'such steps as are reasonable in the circumstances' requires an objective assessment of the specific circumstances of each case that must be considered. Policies and practices under APP 1 could include:

- training staff and communicating to staff information about the agency or organisation's policies and practices
- establishing procedures to receive and respond to complaints and inquiries
- developing information to explain the agency or organisation's policies and procedures
- establishing procedures to identify and manage privacy risks and compliance issues.

APP 1 also requires agencies and organisations covered by the Privacy Act to have a clearly expressed and up-to-date privacy policy about the way they handle personal information. This privacy policy must contain certain information relating to the:

- kinds of personal information collected and held
- how such information is collected and held
- the purposes for which the entity collects, holds, uses and discloses personal information
- access and correction procedures

- complaint-handling procedures, and
- information about any cross-border disclosure of personal information that might occur.

This APP is a bedrock principle for all APP entities — by complying with this APP you will be establishing a workplace culture and processes that will assist you in complying with all the other APPs, right from the start.

APP 7 Direct marketing

The new direct marketing principle (APP 7) will replace the direct marketing provisions that are currently within NPP 2 on 'Use and Disclosure' of personal information. This principle applies to all personal information, regardless of whether it was initially collected for the purpose of direct marketing or for another purpose.

Direct marketing continues to be an area of increasing community concern, particularly in the online environment where behavioural advertising targets users according to their online activity.

In privacy research conducted by the University of Queensland last year, more than half of respondents — 56 per cent — disapproved of having advertising targeted to them based on their personal information. There is also evidence to suggest that with the growing prevalence of tracking and aggregation, some consumers are choosing not to use services due to privacy concerns.

APP 7.1 prohibits the use or disclosure of personal information for a direct marketing purpose, except under specific conditions. For example, if the organisation collected the information from the individual and the individual would reasonably expect the organisation to use or disclose the information for that purpose.

However, where the individual wouldn't reasonably expect the organisation to use or disclose the information for that purpose, or it collected the information from a third party, then the organisation

would need to get the consent of the individual unless that wasn't practicable.

In each of these scenarios the organisation will be required to provide a **'simple means'** by which the individual can request not to receive any marketing. Further in the case of the second scenario the organisation must also generally include a **'prominent statement'** that the individual can make such a request in each direct marketing communication.

APP 7 also proscribes against direct marketing of sensitive information, unless the individual has consented.

Importantly, the principle will provide that individuals may ask organisations who hold their personal information to stop sending direct marketing, or to not use or disclose their personal information to facilitate direct marketing by other organisations. Individuals may also ask organisations to disclose the source of their information. Organisations must comply with such requests free of charge within a reasonable period.

A welcome reform for legal practitioners is the clarification in APP 7's application. For example, the *Spam Act 2003*, which contain specific provisions regarding direct marketing, will displace the more general provisions under the principle. In other words, APP 7 will be displaced where another Act specifically provides for a particular type of direct marketing or direct marketing by a particular technology. But, APP 7 will still apply to organisations involved in direct marketing relating to electronic messages and other acts and practices not covered by such instruments.

APP 8

APP 8 is an important new principle on the cross-border disclosure of personal information to an overseas recipient.

APP 8.1 requires an entity to take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information, subject to limited exceptions set out in 8.2.

In considering APP 8.1, s 16C of the Act is also relevant. In short, APP 8.1 and s 16C create a framework for the cross-border disclosure of personal information under which the disclosing entity remains accountable for the subsequent handling of that personal information by the overseas recipient. In some circumstances, the disclosing entity will be liable for an act or practice of the overseas recipient where that act or practice would breach the APPs.

So, even if an APP entity takes reasonable steps to ensure that the overseas recipient complies with the APPs, where the overseas recipient does not comply with the APPs, the disclosing entity may still be liable.

As I mentioned, this is subject to exceptions in 8.2 which includes where:

- the organisation reasonably believe that the overseas organisation is subject to a law or binding scheme substantially similar to the APPs and there is a mechanism that allows an individual to seek redress, or
- the organisation expressly informs the individual that if they consent to the disclosure overseas then the organisation will not be required to take reasonable steps to ensure that the overseas recipient does not breach the APPs, and will not remain accountable for what happens to that information, and the individual consents.

This new accountability approach does not seek to prevent the cross-border disclosure of personal information. Rather the approach facilitates cross-border disclosure in a manner that ensures appropriate privacy protections are in place and that individuals will be able to seek redress if their information is mishandled.

APP 11

APP 11 relates to an entity's obligation to protect the personal information it holds. You will be happy to know that the obligations largely remain the same as those under IPP 4 and NPP 4. However, there are some differences to note.

Under APP 11, an entity must take reasonable steps to protect personal information it holds from misuse, **interference** and loss, and from unauthorised access, modification or disclosure.

The inclusion of 'interference' is new and recognises that attacks on personal information may not be limited to misuse or loss and may include interference that doesn't amount to modification of the content or information.

According to the Explanatory Memorandum, this new element may require **additional measures** to be taken to protect against computer attacks and other interferences of this nature, but the requirement is conditional on steps being 'reasonable in the circumstances'.

APP 11 also provides that if an entity no longer needs personal information for any purpose for which it may be used or disclosed under the APPs, and if the information is not contained in a Commonwealth record, or legally required to be retained by the entity, an entity is required to destroy or de-identify the information.

Just as a side note, what I'm seeing in data breaches resulting from hacking both here and overseas is that some organisations have not taken reasonable steps to protect the personal information they hold. For example they have not been regularly updating their security systems.

To assist organisations understand their information security requirements we will be releasing a new guide that will help clarify what 'reasonable steps' should be taken under the Privacy Act. The guide won't be binding but it will send a clear message about my expectations in this area, so naturally we intend to refer to the guide

when assessing compliance with the data security obligations in the Privacy Act. We are expecting to release this during Privacy Awareness Week in late April.

Commissioner's new powers

Let's turn now to look at the Commissioner's new powers.

The reforms introduce enhanced powers of resolution and mediation to the role of the Commissioner, including more power to resolve complaints, conduct investigations and promote privacy compliance. These changes will also strengthen my enforcement powers.

From the date of commencement, I will be able to conduct Performance Assessments of private sector organisations to determine whether they are handling personal information in accordance with the new APPs, the new credit reporting provisions and other rules and codes.

The power will consolidate the existing discretion to conduct audits of Australian Government Agencies, tax file number recipients, credit reporting agencies, credit providers and extend it to include organisations.

These assessments may be conducted at any time — an added incentive for organisations to ensure they are handling personal information in accordance with the Privacy Act. So I will be putting businesses on notice that they need to have their systems and processes in place to be ready at all times for a Performance Assessment.

I also have enhanced code making powers under Part IIIB of the reformed Act and these have been a bit of a sleeper. In summary the code making powers will allow me to approve and register enforceable codes which are developed by entities, on their own initiative or on request from the Commissioner, or by the Commissioner directly.

APP entities are able to develop written codes of practice for the handling of personal information, called APP codes, that set out how one or more of the APPs are to be applied or complied with, and the APP entities that are bound by the code. The Act also requires the development of a code of practice about credit reporting, called the CR code. This code will set out how the Privacy Act's credit reporting provisions are to be applied or complied with by credit reporting bodies and providers. I have asked the Australasian Retail Credit Association (ARCA) to develop this.

Another important new addition to the privacy compliance model is that from the first day of operation, the privacy reforms will provide me with enforcement powers and remedies in regards to investigations that I have commenced on my own initiative — we refer to them as own motion investigations. I will be able to make a determination – as I can already with a complaint lodged by an individual, accept written undertakings that will be enforceable through the courts, or apply for civil penalty orders which can be up to $340,000 for individuals and up to $1.7 million for companies. These powers also extend to certain entities' handling of credit information, tax file number information and health information.

As I have been telling businesses and government since I became Privacy Commissioner in mid-2010, my focus will always be on resolving the majority of complaints via conciliation. However, I will not shy away from using new and existing powers where it is appropriate to do so.

I have been asked about what my enforcement approach will be, specifically will I be taking a 'softly, softly' approach after implementation of the reforms. Well I have never been known to be subtle so the answer to that question is probably 'no'. Now before people get too excited about the bluntness of that response remember that I said I would always start by trying to resolve matters through conciliation. Having said that, let's remember that the public sector have been working with the Act for nearly 25 years

and the private sector for over 12 years, these concepts are not new. Fundamentally the principles remain the same. If we take the security principle IPP 4/NPP 4 or what will be the new APP 11 as an example, organisations are required to take reasonable steps to protect the personal information they hold. This is not a new requirement and in my view it should already be happening.

Let's now look at the resources our office is working on for you to use in your work.

OAIC guidance and resources

Our Office has a role to educate all organisations and agencies, as well as the community more generally, about the changes that are coming under the reforms, including the APPs, credit reporting and our new functions and powers. We are doing this on a very limited budget, having received no additional funding from Government, so it is encouraging to see that a number of law firms are already producing and disseminating helpful guidance on these important changes.

We have already commenced developing guidance to assist agencies and businesses.

The upcoming resources will include:

- a comparison guide between the IPPs/NPPs and APPs
- Guidelines on the APPs
- Code-making guidelines (which will be released for consultation next week) and
- revised Privacy Impact Assessment and Data Breach Notification guides

Reference to these resources will be essential when advising clients on what the new law require, and what changes clients need to make to their personal information handling policies and practices.

To ensure compliance, businesses and government agencies need to start thinking **now** about what these changes mean in terms of current privacy policies and business processes and practices.

Some key issues that lawyers should be raising with clients include:

- the review and updating of privacy policies and notices
- outsourcing arrangements, particularly if these involve the disclosure of personal information outside Australia
- the circumstances where personal information can be used for direct marketing, sent overseas, or for credit reporting purposes.
- direct marketing practices, including the availability of 'opt out' mechanisms.

We also have a range of other important responsibilities in the lead up to the commencement of the reforms, including the drafting of binding rules and statutory instruments. We are planning for this material to be ready over the next few months.

We will be conducting targeted public consultation processes to assist us in developing this guidance. I would encourage you to contribute to these consultations, so we can arrive at guidance that is practical and meets the needs of business.

As I mentioned before, we have very limited resources for this task so we will be relying on partnering with peak bodies, agencies and businesses to assist us to get the message out. If you have any suggestions on how we can engage with agencies, business and the community then we would be more than happy to hear from you.

We'll be using our various existing communication channels to get the word out and if you haven't already, I encourage you to sign up with the Privacy Connections Network, our network for private sector privacy professionals.

Although the bulk of our guidance materials are not available just yet, I would strongly encourage you to take advantage of the resources as they do become available.

Mandatory data breach notification

I mentioned to you earlier that we had seen the Government publish a discussion paper on mandatory data breach notification in October 2012. This was a parallel development not covered by the law reform Bill.

As many of you know, I support the amendment of the Privacy Act to require mandatory data breach notification in certain circumstances. The OAIC made a submission in response to the Government's issues paper and it will be very interesting to see how this issue develops. As I have noted, there is no doubt that data breaches cause concern in the minds of the public and lead to calls for tougher regulation.

In addition to the risks to individuals, data breaches also pose a serious reputational risk to business. This 'cost' is in addition to other costs associated with data breaches. Some research estimates the costs of data breaches to be in the millions of dollars. An even greater reputational risk confronts organisations perceived to be either hiding a breach, or not acting on it. Ultimately, this affects consumer trust and the number of return customers. This is perhaps one of the reasons why organisations I have previously investigated have been extremely cooperative in working with us to resolve the issues.

Privacy Awareness Week 2013

On a final note and with such a large number of changes imminent, this is also a great time for you to get involved with Privacy Awareness Week this year.

Every year, we celebrate Privacy Awareness Week (or PAW) as part of the Asia Pacific Privacy Authorities forum initiative to promote the importance of protecting personal information and data security in

the information age. In 2013 Privacy Awareness Week will be held from 28 April to 4 May.

The theme for PAW this year will focus on privacy law reform, and there will be a number of events held and publications released around this time.

To mark the launch of the week, the federal Attorney–General will launch our new *Guide to Information Security* at a business breakfast here in Sydney. We are expecting over 180 privacy professionals to gather and listen to expert speakers discussing their industry experiences in the information security field. I encourage you to get together with your colleagues and buy tickets for a table.

We also invite you to become a PAW partner. Last year we had over 140 partners, almost double the number of partners we had in the previous year. This is a non-financial arrangement and is a great way to demonstrate to your stakeholders the importance that your firm places on privacy. More information about getting involved, and resources to help you participate in PAW will be available on our website soon so please take a look and help spread awareness on the importance of data security and protecting personal information.

Conclusion

I will conclude by saying that it is an exciting time to be working in the privacy field — the large scale of these reforms present interesting challenges and opportunities for all of us as privacy laws are brought up to date with technology and contemporary international approaches to privacy regulation. It also means that it is more important than ever for organisations to be vigilant when handling personal information.

I'm certain that this will be a busy year for all of us. It's been a pleasure speaking to you all this evening and I hope that you will join us in getting the message out about the challenges and opportunities that the privacy reforms present. Thank you.