SPEECH

Australian Government
Office of the Australian Information Commissioner

AMSRO Leaders forum 2014

Presentation by Timothy Pilgrim to AMSRO, Sydney, 20 March 2014

Good afternoon. I'd like firstly to acknowledge the Traditional owners of the land that we meet on today, the Gadigal peoples of the Eora nation, and pay my respects to their elders, both past and present.

Well, the last week has been a big one for us in the Office of the Australian Information Commissioner (OAIC). Over the last few weeks we have been working at full steam getting everything ready for the commencement of the reformed Privacy Act, and here we are, so far so good!

But 12 March was by no means an end date. There is still much more for us to do in terms of further guidance and educative material to produce. In that regard, you may have seen several new consultations go up on our website, including the OAIC's revised privacy policy, our privacy regulatory action policy, e-Alerts providing updates on our consultations and guidance, as well as the broader updating of all our website content to reflect the reforms.

In the last 14 months we have been working on over 50 different types of guidance, including:

- the comprehensive APP guidelines
- the APP quick reference tool
- checklists for both agencies and organisations
- comparison guides between the new and old principles
- guidelines around external dispute resolution schemes and developing codes.

The continuing development of guidance and educative material is a key function of the OAIC and we will be looking to gather information from consumers and entities covered by the Act to help us prioritise our efforts in this area into the future.

AMSRO code consultation

The construct of the Privacy Act is in part to facilitate a co-regulatory approach to the handling of the community's personal information. One way in which it does that is to provide a mechanism by which entities can develop a Privacy Code to reflect the business practices of a particular sector or even the use of a particular technology. I believe that this is an opportunity for organisations in particular to demonstrate to their customers, or the people they interact with that they take the protection of the personal information in which they entrusted, seriously.

In that regard, I was pleased to see that yesterday AMSRO launched the consultation on its draft industry APP code, the Privacy (Market and Social Research) Code 2014, and I thought I would take a moment to talk about that.

For the last 14 months, we have been saying the OAIC doesn't want to see organisations quickly making the absolute minimum changes, and then sitting back in the knowledge that they have just met compliance requirements.

There is no deadline for compliance and continuous improvement. Organisations should be striving for continual improvement in the privacy space.

It's up to businesses to continue to lead and implement changes to process, procedures and, in some cases, workplace culture, to build in everyday compliance with the new requirements. Privacy Codes are a tool that can help do this in the right circumstances.

I say this because the AMSRO APP code is a good example of an industry taking the necessary steps to rise above minimum compliance.

As you know, the AMSRO Code has been one of only two industries that had established and maintained a code under the previous National Privacy Principles that remained current until 12 March 2014, and I am particularly pleased to see that AMSRO and the industry are continuing this drive to reach above minimal compliance with a new code under the Australian Privacy Principles (APPs) in relation to identifiable research information.

We are also very pleased to have been involved with AMSRO from the outset in the processes of developing this new code, and we hope that this will provide added value to the code for AMSRO members.

We're also pleased to see AMSRO working so closely with industry and consumers on the code and engaging more broadly through the 6 week consultation process that started yesterday. I'm sure that there will be some valuable feedback through that consultation process.

Of course you know that this code is likely to be the first voluntary code to be developed under the new privacy laws, and we're hoping that it will be an example to other industries of the value of taking those extra steps.

As previously indicated we have published a comprehensive set of guidelines on the APPs – and these should be very useful to you in meeting both your obligations under the new code as well as in those situations where you are dealing with other personal information.

As was the case previously, the OAIC will handle complaints in relation to any alleged breaches of the new code.

New enforcement powers

As of last Wednesday, the OAIC now has a range of new powers and remedies. These new powers give us a bigger tool kit in resolving complaints, conducting investigations, and promoting privacy compliance.

The OAIC previously had the power to conduct audits of Government agencies and credit reporting agencies and providers — these audits are now called 'assessments', and we can now assess 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 like your new code.

These assessments may be conducted at any time, whether the organisation has had a previous privacy breach or not, so businesses need to have their systems and processes in place to be ready at all times for an assessment.

The Commissioners' will also now be able to make a determination on a Commissioner initiated investigation (as can already be done with a complaint lodged by an individual), accept written undertakings that will be enforceable through the courts, or apply for civil penalty orders of up to $340,000 for individuals and up to $1.7 million for companies.

Over the last 14 months a lot has been made of the potential $1.7 million penalty, especially in media coverage. But adhering to the law is not just about penalties, it is about building in a culture of compliance, about knowing what is expected of your business and making sure that others know what to expect from you.

The OAIC recognises that agencies and businesses have been working hard to implement the changes — our focus over the next 12 months is on working with you to ensure compliance.

We will continue to follow the escalation model that has always been our approach — we will always attempt conciliation of complaints in the first instance. However, where conciliation is not effective we may use our other enforcement tools.

We recently released a consultation draft of the *OAIC Privacy regulatory action policy*. We have developed this policy to outline and explain our approach to using out privacy regulatory powers. The regulatory action policy will be supported by a *Guide to the*

OAIC's privacy regulatory action, which will give more detailed and practical guidance on how the OAIC will exercise its powers.

Consultation on the *OAIC Privacy regulatory action policy* is designed to find out if the policy is clearly expressed and comprehensive — we would like it to be as useful as possible to stakeholders.

Privacy policy tool

Earlier I touched on a range of guidance material that we have produced and will be producing. One of these resources you may be interested in is a tool for developing privacy policies.

Most of you will be aware of the changes that APP 1 brings — seeking to ensure that entities manage personal information in an open and transparent way and take a proactive approach to informing individuals about how their personal information will be handled. This includes a requirement to have a clearly expressed and up-to-date privacy policy outlining the way they handle personal information.

However, our 2013 Community attitudes to privacy survey results show that 51% of Australians don't read privacy policies on websites, although this number is decreasing. Among people who don't read privacy policies, the biggest reason by far is that they are too long (52%) or too complex (20%).

You may also remember that the OAIC participated in the Global Privacy Enforcement Network internet sweep last year. For the sweep we assessed website policies against APP1 — you would have seen the results, which showed that many of the websites most accessed by Australians had quite a way to go in bringing their privacy policies up to best practice.

We have been meeting with business and government over the last year, and one of the messages we have received is that entities across the public and private sectors would be keen to see some more guidance on writing effective privacy policies.

We will be releasing an APP privacy policy tool to give entities covered by the Act some practical assistance in ensuring that their privacy policies are as clear and accessible as possible. Whatever stage your privacy policy is at, the privacy policy tool will help you to check that it achieves compliance with the APPs, meets best practice, or if it needs more work in certain areas.

Guide to undertaking privacy impact assessments

I am often talking about the value of conducting privacy impact assessments (PIA), and today is no different. The changes to privacy processes that are needed to make them compliant with the new laws are the biggest we have seen in two decades. That means that the importance of conducting privacy impact assessments should remain at the forefront of our awareness.

I always recommend conducting a PIA whenever you institute any new business process or commence a new project that may involve the handling of personal information. With such substantial changes to the law, if you have not already done so, I would recommend approaching all your 'business-as-usual processes' as 'new'. Projects and processes that you have used for years have never been used under the new laws, and the last thing you want is an embedded practice that you have overlooked to let you down when it comes to compliance.

The OAIC has just updated our Guide to undertaking privacy impact assessments, and it is currently out for consultation. While you may need to adjust your approach to conducting a privacy impact assessment slightly to take account of those areas covered by the AMSRO code, the PIA guide is a methodological approach and will still be both relevant and applicable to your industry. An interesting aspect of the new laws is that we will be able to require Australian Government Agencies to undertake PIAs and that there will be a review of these provisions in 5 years to determine whether that power should be extended to cover organisations.

De-identification resources

As an industry that deals with a lot of de-identified information, you may also be interested in our recently released "De-identification of data and information" privacy business resource. With our open government mandate, the OAIC is very interested in the use and sharing of open data, but any process whereby data is made publically available also contains risks to privacy. The de-identification resource is designed to help organisations minimise this risk, providing information on when, why and how to de-identify personal information. It also provides some guidance on how to assess the risk of re-identification.

Complaints and awareness

Community concern about and awareness of privacy is by no means decreasing, regardless of what some people may think. Privacy is not 'dead' as some commentators suggest.

The OAIC's Community attitudes to privacy survey showed a steady increase in awareness of Federal privacy laws among Australians, with a jump to 82% awareness from 69% in 2007. There is also a number of areas where people show an increasing level of concern about the handling of their personal information:

- Australians continue to be concerned about their personal information being sent overseas (90%)
- Australian are extremely concerned about information security and data breach notification, with approximately 95% of people saying that they should be informed how their information is handled and protected, and if it is lost
- 74% of Australians are more concerned about the privacy of their personal information in the online environment than they were 5 years ago
- 48% of Australians listed the greatest privacy risk as online services and social media, and only 9% of respondents felt that the social media industry was trustworthy

- And 63% of Australians have chosen to not deal with a public or private sector organisation due to concerns about the way their personal information is used or protected.

This heightened public awareness is supported in the volume of complaints and enquiries that we receive.

In the 2012-13 financial year we received 1496 privacy complaints. In the 2013-14 financial year, just so far, we have already received over 2,000!

In the second week of March last year we received approximately 400 enquiries — in just the last week we have received nearly 700 enquiries to our office.

There are also a number of alternative dispute resolution bodies such as the TIO, FOS who handle privacy complaints and they are also seeing an increase. And this of course does not take into account the huge number that are dealt with successfully by the entities that people have an issue with.

PAW

I want to finish up today by talking about Privacy Awareness Week (PAW).

Over the last few weeks and months there has been a considerable amount of media attention focussed on law reform, on the level of public awareness or concern, and a lot of discussion of the how the laws would be changing.

As far as the OAIC is concerned, we will be using this awareness of the law reform process as an opportunity to raise public awareness of privacy, and we encourage you to do so too.

Privacy Awareness Week this year runs from 4 to 10 May and we will be speaking at a lot of events, and increasing our media and social media presence, building on last year.

Our PAW campaign website is up and running, and we have started listing our partners on it. This year, for the first time, we will be

displaying the logos of those who sign on as partners, which will give our PAW partners that extra bit of public recognition of their commitment to privacy. If your organisation hasn't signed up as a partner yet, I strongly encourage you to do so.

We will be sending out updates to our partners in the weeks leading up to PAW, to keep them up to date on events and campaign issues. This year, as part of our plan to spread the privacy message as far and wide as possible we are encouraging our partners to take an active and public role — we'd love to see organisations doing internal communications, but we'd also be really interested to see our partners holding their own PAW events. If your organisation is planning an event for PAW, we'd be really interested in hearing about it.

We will also be getting very active on social media this year. We will be live tweeting from our events, and we'll be using #PAW2014 all week, as well as in the lead up to 4 May. We'd be keen to engage with our partners on twitter during PAW, so I encourage you to use the hashtag.

With the public already focussed on law reform, organisations have a captive audience, already listening to what they have to say about their commitment to privacy.

Thank you!