



Privacy Commissioner's speech at:

Open Data Forum

11 November 2013

(SLIDE 1)

Privacy and the NSW Government open data initiative

First, I'd like to pay my respects to the traditional custodians of this land and their elders, both past and present.

I'm sure many of you are wondering, 'a Privacy Commissioner at an 'open data' conference?'

The sub text being "is this 'lamb to the slaughter' or the 'kill joy at the party'?"

Neither view is apt for reasons that will become obvious as I speak.

Throughout 2012 and 2013, I have been working with the Department of Finance and Services and other agencies on the broader ICT Strategy encompassing, among other things, open government, the open data initiative and utilising cloud-based ICT services.

And yes today, I've been asked to speak from a privacy perspective on the NSW Government's open data initiative.

The best way to do this is to address what open data is, and, what it is not.

I will also spend some time on what is meant by 'personal information' under NSW privacy legislation, and the views of the community and their expectations when they entrust you with their personal information.

And, make no mistake about it, trust underpins the giving of personal information. And misuse of that personal information is seen as a betrayal of trust.

So, what is open data:

Open data is: a feature of a government that is open to its citizens. Open government and open data are intrinsically linked.

Providing the means to access information about, and from government, secures the accountability of government, public officials and public servants to the broader community.

When you add the protection of personal information, you have an even stronger accountability framework in which the principles of privacy and open government complement one another. And both are integral to the healthy functioning of a democracy.

In this open data context, privacy is an important consideration, not a barrier to the Government's aim of openness, transparency and accountability.

It is not the intention that the Open Data initiative releases information that leads to the identification of individuals. Let me go through some key documents to demonstrate this point:

In 'NSW 2021', the 10 year State Plan, Goal 31 promotes the community's right to openness, accountability and transparency when it comes to government decision-making.

The same goal also stresses that it is important to ensure appropriate safeguards are in place to protect privacy and confidentiality.

The ICT Strategy outlines the need to increase access to public information and facilitate engagement. **It also says and I quote "It will be essential that such sharing is conducted in a secure manner to protect privacy....."**

In the ICT strategy, 'Open Government' is described as engaging with the public through online and social media to enhance transparency and accountability. And to deliver better, more targeted services to the community.

'Open Data' is described as making government data available to industry and the community to stimulate the development of innovative approaches to service delivery and new tools for interacting with government anywhere, any time.

The 'Open Data' principles include the principle of 'protect where required'. That is, its clearly stated that data should not be released in full or in part, where privacy, security, confidentiality or legal privilege considerations preclude release. Particular care and in some cases further investigation may be required where disparate datasets, individually de-identified, could potentially be linked or combined, to re-identify individuals, or breach relevant privacy legislation or policies.

Lastly, 'Sharing Information Assets' is seen as capturing the better use of information both within government and industry to enhance cross-agency service delivery and co-production with the non-government sector to better meet community needs. **Again within privacy protection laws.**

To approach this from the other angle, 'Open Data' is not:

1. 'Open data' is not 'open slather'.

The NSW Government's open data initiative does not mean that the policy is to release personal information that identifies individuals, or groups of individuals, or communities or special interest groups. Or to release de-identified data that can be reconstructed to identify individuals.

There may be misperceptions that to achieve openness and transparency, agencies must release all information they hold, regardless of its nature. That is, whether it identifies individuals or not. The release of raw unprocessed data full of personal identifying information is not envisaged, nor is it necessary to achieve the aims outlined above.

2. 'Open Data' is also not a 'BOTPA'

'BOTPA's' are one of the banes of a Privacy Commissioner's life.

The spelling is B, O, T, P, A. Short for, 'Because Of The Privacy Act'.

When uttered, a BOTPA goes like this "we cannot do (whatever it is) but we really wanted to but "because of the privacy legislation it's not possible".

In this context, it would be "We really wanted to support the Open Data initiative but because of the privacy act ,we just couldn't".

A variation of a BOTPA at the policy level is to cast privacy legislation as a barrier to 'open government' and 'open data' without assessing objectively, the evidence either for or against this premise.

More often than not in the Open Data arena, the reasons behind the BOTPA involve other factors such as incomplete datasets, concerns about liability, concerns about the quality of the data, or the allocation of resources to identify and prepare data for posting.

It is possible to participate in the open data strategy and be compliant with NSW privacy legislation.

There is a significant amount of useful data that doesn't disclose personal information suitable for placement upon the NSW open data portal.

And, the provision of data (to the open data portal) that doesn't identify individuals is not prevented by privacy legislation.

Of course, we have to recognise that 'information' and 'data' may, in fact, be personal information or may contain personally identifying data.

If you perceive potential difficulties in providing data for privacy reasons adopt the 'privacy by design' approach and do a privacy impact assessment.

It's possible that those agencies experiencing the greatest difficulty in managing their information assets are those that do not have an adequate framework or processes in place to determine firstly what information they have and secondly the potential risks and opportunities posed by providing data access.

Without an appropriate governance approach or processes, the task of protecting the privacy of sensitive data while achieving greater openness and transparency can seem all too difficult, creating the inaccurate perception of privacy as a barrier.

(SLIDE 2 – Privacy by Design)

This brings me back to the concept of 'Privacy by Design'.

The concept was originally established by the Ontario Privacy Commissioner in relation to the life cycle of technologies, from the early design stage to their deployment, use and disposal.

But the 'privacy by design' approach has a far broader application. So as part of deciding what data to put on the Open Data website, assess upfront if personal information is involved and the consequent decision or actions that need to follow.

It's about building privacy protection into systems as they are created, thereby preventing breaches from occurring.

'Privacy by Design' recognises that privacy cannot be assured just by compliance with laws and regulations, but that privacy assurance is ideally an organisation's default mode of operation.

At a practical level it requires organisations to demonstrate their accountability by including privacy as part of their corporate governance, and valuing it as part of their corporate identity.

The need to do this is revealed by the recent survey on Community Attitudes to Privacy released by the Office of the Australian Information Commissioner (OAIC) this month. It shows that privacy is not dead in the minds of Australians.

By way of background, the OAIC conducts a survey on the public's attitudes towards privacy on a regular basis. It provides data not just on current attitudes but is a time series of changes in attitude. All of this data by the way, is available on the Federal open data website.

(SLIDE 3 – OAIC Privacy Attitude Survey Data)

As you can see on the slide, the most recent survey has found that almost all of the sample considered the following scenarios a mis-use of their personal information:

- An organisation revealing a customer's information to other customers
- Using information provided for a purpose other than for which it was provided, and
- An organisation you haven't dealt with, gets hold of your information

What is of great interest is the growth in the proportion of Australians not dealing with an organisation because of concerns over their use of personal information.

And this trend is strengthening such that, whereas in 2001, 14% of respondents decided not to deal with a government agency or public sector organisation due to privacy concerns; in 2013 this figure had grown to 23%. Given that frequently there are few alternatives to dealing with a government agency, this is a significant shift.

In the private sector, the trend was even greater with the proportion growing from 42% in 2001 to 60% in 2013.

For good reason then, the ICT strategy has identified government's obligation to protect personal information and commits to strengthening electronic information security measures across the NSW public sector.

NSW privacy legislation plays an important role for the NSW community. Over the past four years, the volume of privacy matters to the Privacy Commissioner has increased by 300%.

The role of Privacy Commissioner is an acknowledgement that people need an independent voice or champion to promote their rights. And an independent body which can investigate privacy matters, and help protect the privacy of their personal information.

As Privacy Commissioner I am responsible for administering two Privacy Acts.

(SLIDE 4 – NSW Privacy Legislation)

The first 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. The Act also provides for the Privacy Commissioner to undertake inquiries and investigations, and provides the power to obtain information.

In addition, there is the:

- *NSW Health Records and Information Privacy Act 2002* (HRIP Act)

The HRIP Act covers NSW organisations, both public and private, that provide health services or deal with health-related information.

The major focus of the NSW legislation is upon the protection of personal information, rather than the more generally accepted concept of privacy which includes physical seclusion or solitude.

Under NSW privacy legislation, 'personal information' is information or opinion (which can be part of a database) about an individual whose identity is apparent or can be reasonably ascertained from the information or opinion. Personal information can include such things as an individual's fingerprints, retina prints, body samples or genetic characteristics.

But 'personal information' does not include, amongst other things:

- information about a person who has been dead for more than 30 years, or
- information about an individual that is contained in a publicly available publication.

Both pieces of legislation (PPIPA and HRIPA), like the Commonwealth legislation, are principle based.

The Information Protection Principles in the PPIP Act and the Health Privacy Principles in the HRIP Act focus on the collecting, holding, using or disclosing of personal information.

It's critical to embed these privacy principles in operations and to consider them when deciding when data is appropriate for placement upon the open data portal.

In the open data policy, there are guiding principles that agencies should follow when implementing an open data practice. And as I outlined earlier these include the need to protect personal information.

Agencies need to consider the privacy implications of releasing the data and satisfy themselves that the privacy requirements are met. De-identification of datasets may be necessary to ensure that personal information is not compromised.

Currently my office is in the process of developing a Privacy Governance Framework document.

This framework document will complement the open data policy by mapping out the elements of the privacy law regime. It will also outline the role and responsibility of agencies to consider privacy in the context of their projects and governance framework.

This will strengthen agency understanding of the privacy legislative framework in NSW and assist them when considering the open data policy.

Obviously from a privacy perspective, good record management is essential to both protecting personal information and providing appropriate data for access. I mention this as so often the importance of records management is overlooked. It underpins both providing 'open data' and protecting personal information.

In conclusion, I'd like to leave you today with some key messages:

- At the big picture level, the protection of personal information and public access to information are characteristics of a democratic system of government.
- It is possible for agencies to actively participate in the 'Open Data' initiative while complying with the letter and spirit of privacy legislation
- Far from privacy being a barrier to open government, and open data, privacy requirements help drive the need to identify information assets, to understand the type of information held and to develop appropriate governance arrangements.
- The key to managing privacy considerations lies in implementing 'privacy by design' principles and best practice in open data initiatives.

The Open Data vision requires commitment from us all to make it a reality. If you or your agency needs assistance to determine if your information assets include personal information and how to deal with this, don't hesitate to contact my office. We will be happy to assist.

Thank you for your attention.

(SLIDE 5 – IPC Contact Details)