Karen Curtis
Australian Privacy Commissioner

Speech to
Human Services Delivery
and Payment Reform Summit

Putting the Privacy into Service Delivery Reform

Canberra
29 June 2010
Thank you for the introduction. Firstly may I acknowledge the traditional owners of the land on which we meet, and pay my respects to their elders past and present.

I am pleased to have the opportunity to speak to you today and offer some privacy perspectives on what is a significant and very broad reform agenda.

But speaking of broad reform agendas, there are many exciting and important changes afoot in privacy law.

Last Thursday, Senator the Hon Joe Ludwig released an exposure draft for the new Australian Privacy Principles. The Australian Privacy Principles will replace the two existing sets of privacy principles in the Privacy Act: the IPPs which
regulate Australian and ACT government agencies, and the
NPPs which regulate the private sector.

This much needed reform, which flows from the extensive privacy inquiry undertaken by the Australian Law Reform Commission and the government’s first stage response to that report, aims to clarify and simplify the privacy obligations of agencies and organisations and introduce greater national consistency.

My view is that it is needlessly complicated applying similar but slightly different privacy principles to the public and private sectors. In some cases this leads to difficult situations where organisations or agencies have to take account of both sets of principles.
So this is a significant reform to privacy law and one that will be beneficial for both government agencies and private organisations which have to comply with the Privacy Act, and for individuals seeking to understand and exercise their privacy rights.

The reason I mention the release of the exposure draft Australian Privacy Principles in this forum is that a change in privacy law will have some effect on the operations and projects of agencies and organisations.

For example, the IPPs currently influence how privacy is built into Service Delivery Reform. However the IPPs will make way for the Australian Privacy Principles sometime later.
maybe 2012 or 2013, so we need to think through how we ensure a smooth transition.

The draft Australian Privacy Principles draw on the **existing standards** in the IPPs and NPPs. This is not a case of ‘out with the old, in with the new’ but rather a streamlining and harmonising of ‘the old’ into something new but familiar. The draft Australian Privacy Principles are intended to embody key tenets of the existing IPPs and NPPs.

When you read the Australian Privacy Principles you will see much that is recognisable and much of what we have come to know and expect when it comes to privacy regulation. For that reason, I believe that the Australian Privacy Principles will not
have a significant impact on the current work to transform government service delivery.

**Reforming service delivery**

So I offer a few reflections on the notion of ‘Service Delivery Reform’ that are relevant from a privacy perspective.

One phrase that has been adopted to help explain the Service Delivery Reform package is this: ‘Works For You’. It is a phrase that’s used often throughout the materials, and it is also the name of the website for these reforms.

The phrase ‘Works For You’ taps into the goals of Service Delivery Reform - to provide individuals with an improved experience in their dealings with government, and an
experience that is tailored towards the individual’s specific needs and circumstances.

This kind of approach could easily be described as ‘citizen-centric’ and ‘customer focused’.

Such an approach is, of course, highly desirable. Any project that keeps one eye firmly on the needs of its stakeholders is one which will go a long way to being successful.

The reform agenda includes customer focused improvements like:

- providing access to more government services in a single physical location – like co-locating offices such as Medicare, Centrelink and the Child Support Agency, so
that they are under the one roof – a kind of ‘one-stop shop’

- where a person (customer) agrees, a ‘tell us once’ approach in providing that customer’s information to government

- a single online access point for the convenience of customers, and

- making it easier for customers to be more self-sufficient in their interaction with service delivery agencies.

These are all appropriate and sensible outcomes – all focused on how government can better serve its citizens. But of course, we can’t just consider the ends in isolation.
Just because individuals have an interest in seeing these outcomes does not mean that people will necessarily forgo other things that they value and expect from government, like accountability and protection of their personal information.

Indeed, ‘Works for You’ could also easily be the catch cry for privacy law.

**Getting service delivery right**

To explore this a little further, I’ll refer to a couple of specific examples from the service delivery perspective:

1) The idea of a one-stop shop, or a well integrated set of services, has obvious appeal for people. They don’t want the hassle of going from office to office when the same set
of services can be more conveniently and efficiently provided in the one place.

2) Many people would of course be happy that if you changed your address, not to have to contact multiple agencies separately to advise them of the same news. People don’t want to waste time repeatedly filling out forms. As technology develops people actually have an expectation that government too will improve their services in a similar way.

This all makes sense. However, I note that many of these reforms hinge on the more efficient use of information, including personal information. While many of us welcome these developments, this is not the same as suggesting that
people would somehow consent to all arms of government having access to all of their personal information.

In delivering these outcomes, not all would be comfortable with unlimited information flows between the various agencies under the Department of Human Services (DHS) umbrella.

In a more integrated service delivery environment, people may have concerns about whether this might bring with it an increased risk that their personal information may be used for purposes they don’t know about and wouldn’t expect.

**Good government**

I want to refer to an observation made by the Minister for Human Services, Chris Bowen, in his speech launching these reforms late last year.
The Minister noted that it is often the case that people don’t necessarily view their dealings with government as dealing separately with a range of specific agencies (e.g. Medicare; Centrelink; Child Support Agency). Often, people instead conceive that they are dealing simply with ‘government’ – and they want a customer experience that reflects this.

While I accept this observation, every year my Office hears from people who expect their government to have the right systems in place so that only the relevant parts of that government will be able to appropriately access and use their personal information.

For example, for a number of years now my Office’s Annual Report has noted that the most common issue in complaints
against government agencies has been inappropriate disclosure.

So people still have an expectation that their personal information will be protected by government – and all the service delivery convenience in the world will be no consolation if they feel their personal information has been compromised.

This is really my key message today. No matter much how much the community wants and expects a simple and well integrated service delivery experience from government, people will also expect their personal information to be protected. So, good privacy is vital to Service Delivery Reform success.
**Ensuring success**

There are six key areas that need to be focused on to ensure this success. These six key areas are also underpinned by two fundamentals of privacy law – **balance**, and **choice and control**.

**Balance** – a balance between the free flow of information between the DHS portfolio agencies on the one hand, and individuals’ rights and expectations of privacy on the other.

**Choice** and **control** will be essential to getting this balance right. The more choice and control that individuals have over things such as:
• the personal information that one DHS agency can give to another agency (especially sensitive information such as health information), and

• when individuals can access and correct their own information held by individual DHS agencies, the better and more tailored the outcomes will be for individuals.

It is this, after all, that the Service Delivery Reform program is all about – making sure it ‘works for them’.

**Working with DHS to ensure success**

I want to be clear today that I am very confident that Service Delivery Reform can be undertaken successfully.
To assist with this, in February this year, my Office and DHS signed a funded one year Memorandum of Understanding (MOU).

The MOU aims to assist the SDR reforms progress with regard to the need to protect people’s personal information.

With the MOU in place, my Office has been in a better position to provide more detailed advice to DHS on the privacy aspects of the reforms.

MOUs such as this are positive because they recognise that privacy helps good policy development, and acknowledge the benefits of close cooperation between agencies and my Office on privacy issues. I am very optimistic that the reforms can achieve all the outcomes that they are expected to achieve.
Six privacy ‘must do’s’

Now to those six fundamental elements of getting SDR right from a privacy perspective. The first two I’ll discuss are fairly broad, but are fundamental to success.

Number One

Involve the community

The core rationale for Service Delivery Reform is to improve the experience of members of the community when they deal with government. It is about meeting the needs of citizens by delivering high quality public services seamlessly and efficiently, yet still handling people’s personal information in a way that is respectful of their privacy. It is about making service delivery ‘work for’ all Australians.
Of course, in any discussion about the public service and its effectiveness, we must return to the citizen, because they are at the centre of what we do.

One of the best ways to work out if we are meeting the needs of citizens is to consult widely, to gauge community needs and expectations, and then shape government services accordingly.

As you move from the design to the implementation phase, it is equally important to keep those lines of communication with community stakeholders open.

**Consultation leads to trust**

For individuals to get the most from public services, they need to be able to trust agencies to use, disclose, and protect their
information appropriately and respect their right to privacy.

When governments don’t get it right, citizens can suffer.

On the whole, Australians do tend to trust the public sector to handle their personal information appropriately.

My Office’s 2007 Community Attitudes Survey revealed that 73 percent of Australians considered government departments to be trustworthy when it came to handling their personal information.

Trust is a major factor in people’s decision-making processes.

In this survey, 36 per cent of people stated that they had decided not to deal with an organisation because of concerns about how their personal information would be handled. This shows that people’s perceptions about how their personal
information will be handled will impact on their consumer
decisions.

However, people often don’t have the choice **not** to deal with a
government department. For this reason, it is important that
government bodies handle personal information responsibly.

And trust can be eroded very quickly. In the event of a data
breach (and a sustained media attack) agencies cannot afford to
be complacent. Trust is an elusive commodity and should not
be taken for granted.

So it is very important to involve the community in developing
and implementing a reform agenda, and to be flexible enough
to respond to community needs as a project develops. Taking
this step will set agencies on the course to developing a successful and privacy-friendly outcome.

**Number Two**

*Design privacy in*

It is important that privacy protections are built into a Service Delivery Reform program from the very beginning, rather than treated as an afterthought. Privacy should be **built in, not bolted on**.

By considering Service Delivery Reform projects in the context of privacy, and by building in privacy protections during the embryonic design phase, you can ensure that reforms can even enhance the privacy of individuals.
Enjoying the benefits of streamlined services does not mean that citizens have to give up other freedoms or rights.

Integrated service delivery has a lot to offer.

So let’s take responsibility to embed privacy in Service Delivery Reform initiatives so that they achieve not only efficiency gains, but also enhance protection of people’s privacy.

**How we can do this – PIAs**

To achieve this, I strongly encourage agencies to conduct **Privacy Impact Assessments** (PIAs) when commencing projects that are likely to impact on privacy.

A PIA is an assessment tool that describes in detail the personal information flows in a project, and analyses its possible privacy impacts.
A PIA can help agencies to identify when the collection of particular information is unnecessary for a given project, or where additional accountability or oversight processes may reduce privacy risks.

PIAs are becoming the norm now for new projects that involve the handling of personal information. They are an accepted assessment tool used in many countries across the world including Canada, the United States, the United Kingdom and New Zealand. Indeed, US President Barack Obama has mandated that PIAs be undertaken on federal projects involving significant personal information.

PIAs also help to gain community trust and confidence in new proposals.
My Office has recently produced an updated PIA Guide to help steer agencies through the PIA process. The Guide makes it clear that the best time to identify and address any privacy impacts is when you set out to develop a new project or product – that is, designing privacy in, and it’s available on our website.

Projects that have been through a comprehensive and transparent privacy impact analysis and planning process are more likely to achieve their aims, inspire the trust of the community and build an agency’s reputation.

If the core purpose of Service Delivery Reform is to ‘work for’ the Australian community, then agencies involved with these changes should tell the community:
• the **purpose** of the changes being made
• **what** the proposed changes are, and
• **how** personal information will be protected under the proposed changes.

Ensuring that clients are properly informed about the benefits of reform, and about the way their privacy is being safeguarded, will build community confidence.

Privacy complaints can arise when agencies use or disclose personal information in a way that an individual does not expect. If you are open and transparent with people about the way you handle their personal information from the first time they interact with you, you can avoid those misunderstandings.
Being open about your information-handling practices can lead to a win-win – your clients will be more confident in your ability to safeguard their information, and hopefully you should have fewer privacy complaints.

**Number Three**

*Choice and control*

Allow your clients to exercise choice and control over the way their information is handled.

Service Delivery Reform is a process driven by customers’ needs so individuals should be given the opportunity to decide whether or not their personal information will be shared between service providers for their convenience.
Imagine that a person who is simultaneously a client of Medicare, Centrelink and the Child Support Agency moves house. In the ‘pre-SDR’ environment, that individual would probably have to contact all three agencies to inform them of their change of address. This might involve significant inconvenience – filling in multiple forms with the same information.

Once Service Delivery Reform has been rolled out, if that person informs, for example, Medicare of their change of address, they could be asked whether they would like Medicare to alert the other DHS agencies that their details have changed.

If the client accepts this offer, they are saved the inconvenience of having to provide the same information to Centrelink and the Child Support Agency.
On the other hand, the client may want to deal with specific agencies separately.

If it is the client’s wish to inform each agency individually, then Medicare should respect that wish, and refrain from passing the information on. It will be up to the client to choose whether and when to update their address details with other DHS agencies.

This is just an example, but the key message is that you will gain individuals’ trust and confidence by empowering individuals to control the way their personal information is handled. And this will minimise the risk of misunderstandings, which can lead to privacy complaints.

Number Four

*Maintaining database integrity and compliance*
Another vital ingredient in an effective Service Delivery Reform program is an agency’s ability to maintain database integrity and appropriate segregation. There is no point offering customers the ability to control the way you handle their personal information if you cannot provide adequate security and information management.

Databases containing personal information collected for different programs need to maintain some form of separation. This is sometimes referred to as ‘siloing’. Each service provider maintains its own self-contained, independent database, or ‘silo’ of information, over which it has control. In this silo will be all the information that it collects in the course of delivering its services to the public.
Under privacy law, government service providers are not able to access any personal information in another service provider’s ‘silos’ except in limited circumstances, for example, if the individual has provided consent, if such a disclosure is authorised or required by law, or if it is within reasonable expectations.

We need to remember that the purpose of Service Delivery Reform is to improve the customer’s experience. A significant part of the customer’s experience is the security of knowing that their personal information will be appropriately handled and protected.

**IPP Compliance**

As I mentioned earlier, Australian Government agencies have to comply with the 11 Information Privacy Principles in the
Privacy Act. These principles govern how agencies handle personal information, including the way that they collect, use, disclose and secure that information.

The IPPs limit the circumstances in which agencies can use or disclose personal information. If an agency wishes to disclose personal information about a client to another service provider, the agency needs to be able to point to a reason for the disclosure under IPP 11.

IPP 11 states that an agency can only disclose an individual’s personal information in limited circumstances, including if:

- the individual is reasonably likely to be aware, or made aware, that it could be disclosed in those circumstances
- the individual consents to the disclosure
- the disclosure is required or authorised by or under law.
Further, IPP 4 requires agencies to take **reasonable** steps to ensure that the personal information they collect is protected against loss and unauthorised use, disclosure and modification.

Care needs to be taken about the way databases are structured, and the way that personal information is shared with others.

System design should be ‘privacy-friendly’ and should incorporate ‘need-to-know’ access protocols, while maximising customer convenience and efficiency.

Databases should be appropriately secured so that one service provider cannot access the information held in another service provider’s database unless the IPPs have been complied with.
By ensuring the integrity of databases and complying with the privacy principles, agencies can increase their clients’ confidence that their personal information is being properly protected.

**Number Five**

*Take extra care with sensitive information*

There is a subset of personal information known as ‘sensitive information’. Sensitive information includes information about an individual’s health, racial or ethnic origin, religious beliefs, sexual preferences or practices, and criminal record.

While the IPPs do not make specific reference to sensitive information, obviously agencies need to be particularly careful when handling sensitive information. So agencies should consider giving individuals a greater capacity to exercise control over the way their sensitive information is handled.
Imagine that one agency has collected a significant amount of health information about an individual. Another agency requires some information about a particular medical condition that the individual has, and seeks to access this information from the first agency.

The first agency should take particular care to ensure that it only discloses information relevant to the purposes of the second agency, and that the individual has consented to this information being disclosed.

So again, Service Delivery Reform must be mindful of and respect sensitive information. More specifically, it is our view that the reforms should not extend to particularly sensitive information such as clinical health or health claims information.
And so to Number Six

Leverage expertise

The final thing that I would like to emphasise today is that if you want to maximise the many benefits of ‘doing privacy well’ when implementing a Service Delivery Reform agenda – if you want to build community trust and confidence in your program while simultaneously minimising privacy risks – remember that other agencies have had to deal with similar issues.

Agencies engaging in Service Delivery Reform initiatives should look to local and international experience when designing and implementing SDR to reflect best practice information handling processes.
My Office was pleased to sign the MOU with DHS, to help DHS work with agencies to navigate the privacy issues associated with these changes.

We encourage agencies that have embarked on Service Delivery Reform projects to share their expertise with others. We arranged for a speaker from DHS to make a presentation at a recent Privacy Contact Officer network meeting in Canberra about this topic. This spirit of cooperation is one of the hallmarks of the Australian Public Service. There’s little to be gained from trying to reinvent the wheel!

And we heard yesterday about how Service Delivery Reform has been implemented in North America. Later today we will hear about SDR from a Danish perspective. So Australia is not
the only country pursuing a reform agenda, and there is much that we can learn from the experiences of other nations.

**Conclusion**

So my message is this: Properly implemented, service delivery reform is a good idea. **BUT**, it is important to build privacy in from the beginning and to get the balance right. Privacy is not a blocker to the business of good service delivery – protecting privacy is a key business requirement.

For service delivery reform to truly deliver on its motto of ‘Works For You’, it needs to produce not only good, efficient service delivery outcomes, but also positive privacy outcomes.

I don’t think the quote on the bottom of my date calendar a couple of years ago from *Unknown* was right:
Relying on the government to protect your privacy is like asking a peeping tom to install your window blinds.

But rather I’d like to leave you with Bill Clinton’s thoughts:

_We must protect our citizens’ privacy -- the bulwark of personal liberty, the safeguard of individual creativity._

And an Italian philosopher’s:

_Privacy is not something that I’m merely entitled to, it’s an absolute must._

Thank you.