Friday, 19 May 2017

As part of an address to the AGS FOI and Privacy Forum on May 19, Commissioner Pilgrim outlined the reasons and aspirations behind the introduction of the APS Privacy Code.

The relevant excerpts are provided here.

I'd like to begin by acknowledging the Ngunnawal people as the traditional custodians of our national capital, and offer my respects to elders past and present.

As part of Privacy Awareness Week, the OAIC has released the latest Australian Community Attitudes to Privacy Survey (ACAPs).

ACAPs is the longest standing privacy survey in the country, and one of the longest in the world.

In fact, it has been around almost as long as the Privacy Act, having commenced in 1990.

The survey has been undertaken every four years or thereabouts.

The ACAP's questions cover all industries and sectors of Australia, and once again the results are a mix of the predictable, and the unexpected.

The community and media interest in the survey has been quite evident this year.

This is because the survey has shown that while the majority of Australians are still reporting a growing concern about their privacy, particularly in the online context, they not embracing basic online privacy controls and tools.

Accordingly, I've been emphasising that we all have a role to play as individuals, to use the protections already available to us as best as we can.

The privacy protections my office is highlighting this week – like checking social media settings and clearing browsing histories – are simple steps that we can all take to reduce our privacy risk.

We're also telling consumers to insist that organisations they deal with treat their privacy rights seriously, and to vote with their feet if needed.

There is, in the commercial sector, a strong consumer choice driver available to send market signals to businesses on the importance of personal data protection.

However, that 'market signal' is inevitably modified by the unique operating environment of most government services and transactions.

This is because the limited choice dimension of Government transactions often shifts the power balance between the individual and entity when it comes to personal data choices.

At the end of the day, if someone wants to obtain a service from Medicare, they must deal with Medicare on the terms at hand.

If someone decides they do not like the data handling of the Australian Tax Office, for example, it is not as if an alternate tax office is an option.

Government agencies hold immense amounts of personal information, and they often have broad ranging powers to get it.

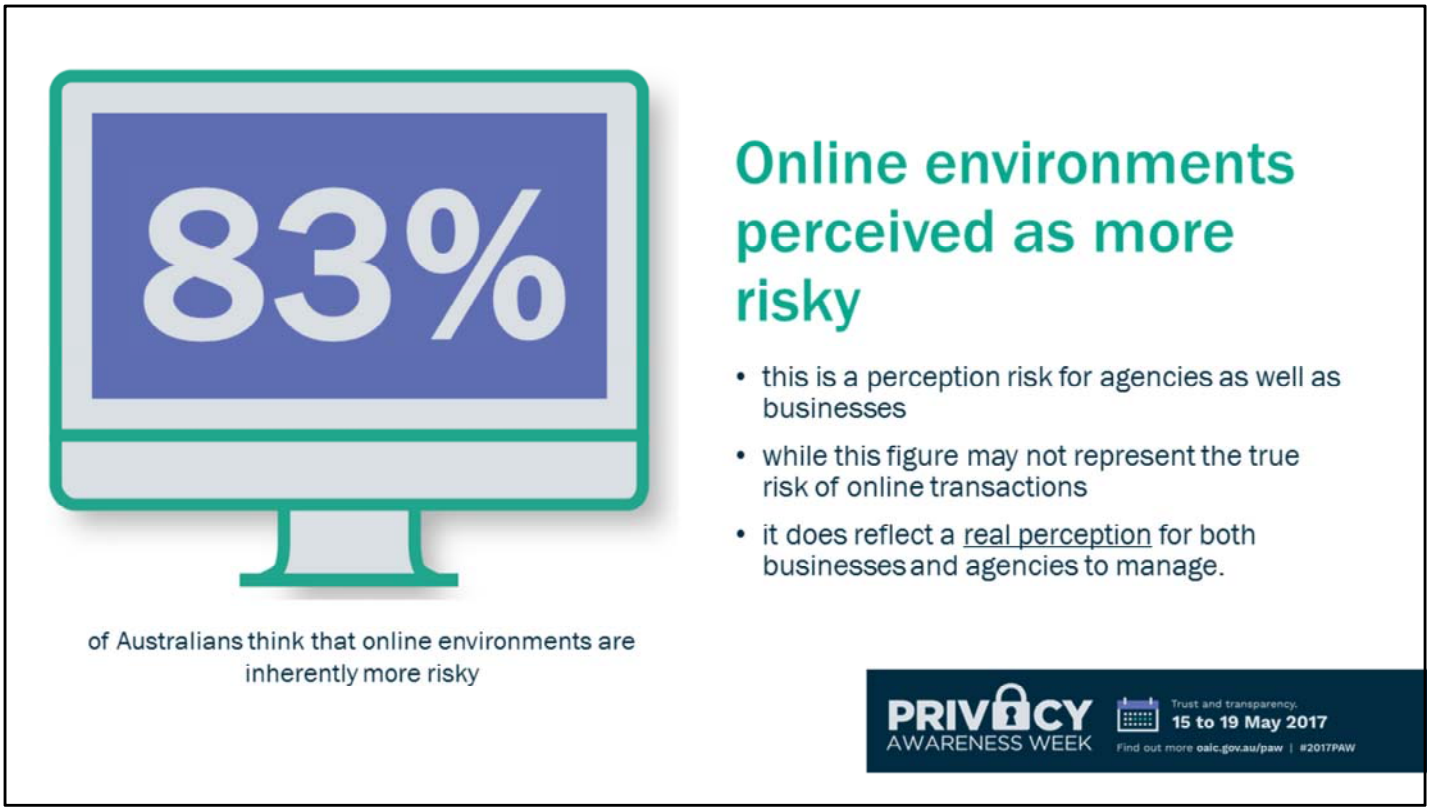
As we can see from our popular culture, Australians have a long and deep running suspicion about lack of choice.

It’s not every nation that can make the rather arcane topic of compulsory land acquisition into a hit film and a cultural catchphrase – I refer here of course to *The Castle*.

For all its legal fiction –*The Castle* is underpinned by longstanding jurisprudential themes on the tension between individual liberty and social benefit, which struck a chord with Australian notions of ‘the fair go’.

And, if Australians could take compulsory acquisition of land to heart in this way, why would we assume they treat compulsory acquisition of our personal information with any less regard?

It’s a signal to those who work in Government that it’s in our interest to be seen as preferred custodians of personal data, and as being at the forefront of personal data protection.



After all, Government agencies have a lot to gain from improving community confidence in personal data management – because the ACAPs survey shows do we have some issues to overcome.

One of these is that 83% of Australians think that online environments are inherently more risky than offline.

Now, I can assure you from my perspective as Commissioner that many of the privacy breaches that my Office deals with are decidedly offline and low tech.

Nevertheless, while this figure may not represent the true risk of online transactions, it does reflect a real perception for agencies to manage.

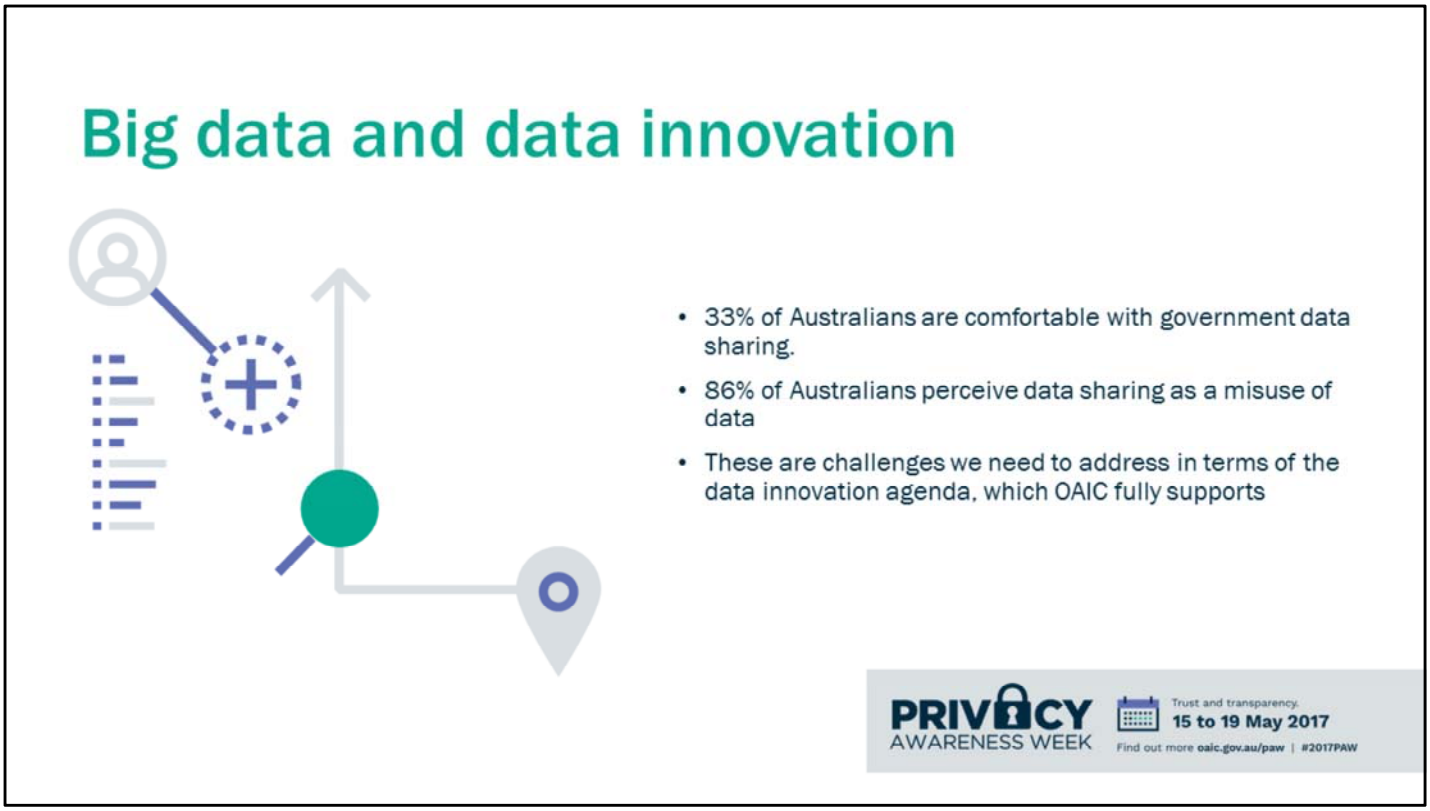
Given the desirability – for efficiency, policy and service delivery – of promoting online transactions, building greater community comfort with online environments is vital.

The other issue we need to tackle is the low level of comfort with agency-to-agency data sharing – something which is critical to the Government's data innovation agenda.

Only 33% of people are comfortable with the idea of agencies sharing data while 49% are uncomfortable.

The good news for the APS is, these results are vastly better than then the private sector figures where only 10% of people are comfortable with businesses sharing their personal information while 79% are uncomfortable.

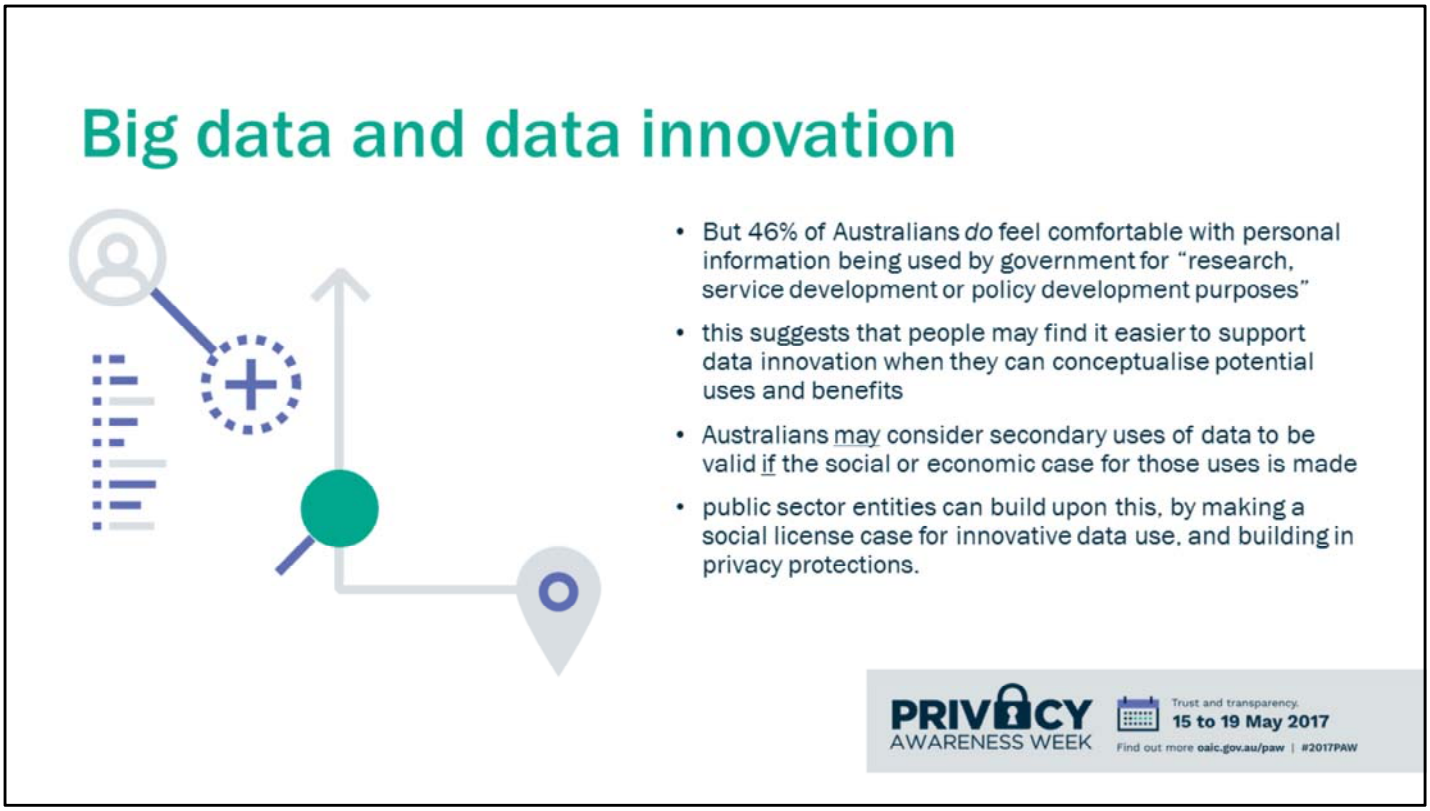
However, this is clearly still a challenge for the APS.



Another challenge thrown to our data innovation agenda is the finding that secondary use of personal information is perceived, in concept, as a misuse of personal information by the majority of Australians (86%)

Both these figures have ramifications for innovative data uses, which rely on both data sharing, and secondary use.

We need to find ways to address these perceptions in order to build a broad social license for data innovation work – which the OAIC fully supports as a long-term champion of open government and maximising the public benefit of public data.



But all is not lost, and with that in mind, and with a desire to better understand what lies behind these community concerns, we added a new question to the ACAPS this year.

This question specifically tested the idea of personal information being used by government for "*research, service development or policy development purposes.*"

Responding to this question is 46% said they were comfortable with their personal information being used for these purposes.

Those who can hold figures in their heads will note that this is higher than either figures for data sharing when considered generically – suggesting that people find it easier to support a public data purpose when they can conceptualise potential uses.

This finding also may offer a contradiction to the broad objection to secondary uses I just highlighted – as the question implies this.

Again, it does suggest that Australians are prepared to support data sharing and re use, when there is transparency in terms of use and a clear social license case is sought.

Interestingly, a further 21% of respondents were neither comfortable nor uncomfortable, and 19% were only "somewhat uncomfortable".

This may suggest that 40% of respondents have not yet formed hard views against the proposition, but are yet to be convinced.

So, these are all findings with potential for public and private sector entities to build upon, by communicating the public case for innovative data use.

Trust = innovation mandate

- agencies that move beyond compliance and into privacy by design will have a distinct advantage in addressing this concern
- clients can feel overwhelmed by the issue
- agencies that make privacy choices easy to control and understand will be more trusted
- that community confidence is vital to creating social license for data innovation

PRIVACY AWARENESS WEEK
Trust and transparency
15 to 19 May 2017
Find out more oaic.gov.au/paw | #2017PAW

Therefore, the link between being a *trusted* sector in personal information, and being an *effective* sector in data innovation, is clear.

And as we see from the private sector, organisations that move beyond basic compliance and into "privacy by design" can gain a distinct advantage in addressing consumer and community concern.

A key of the 'privacy by design' ethos is the principle of transparency. This is what I mean when I say, as I often have, that privacy is more about transparency than secrecy.

It's about being clear about the what, why, how and who of personal information management.

This allows clients to make informed choices, where they are available, and for there to be transparency and accountability in transactions in all cases.

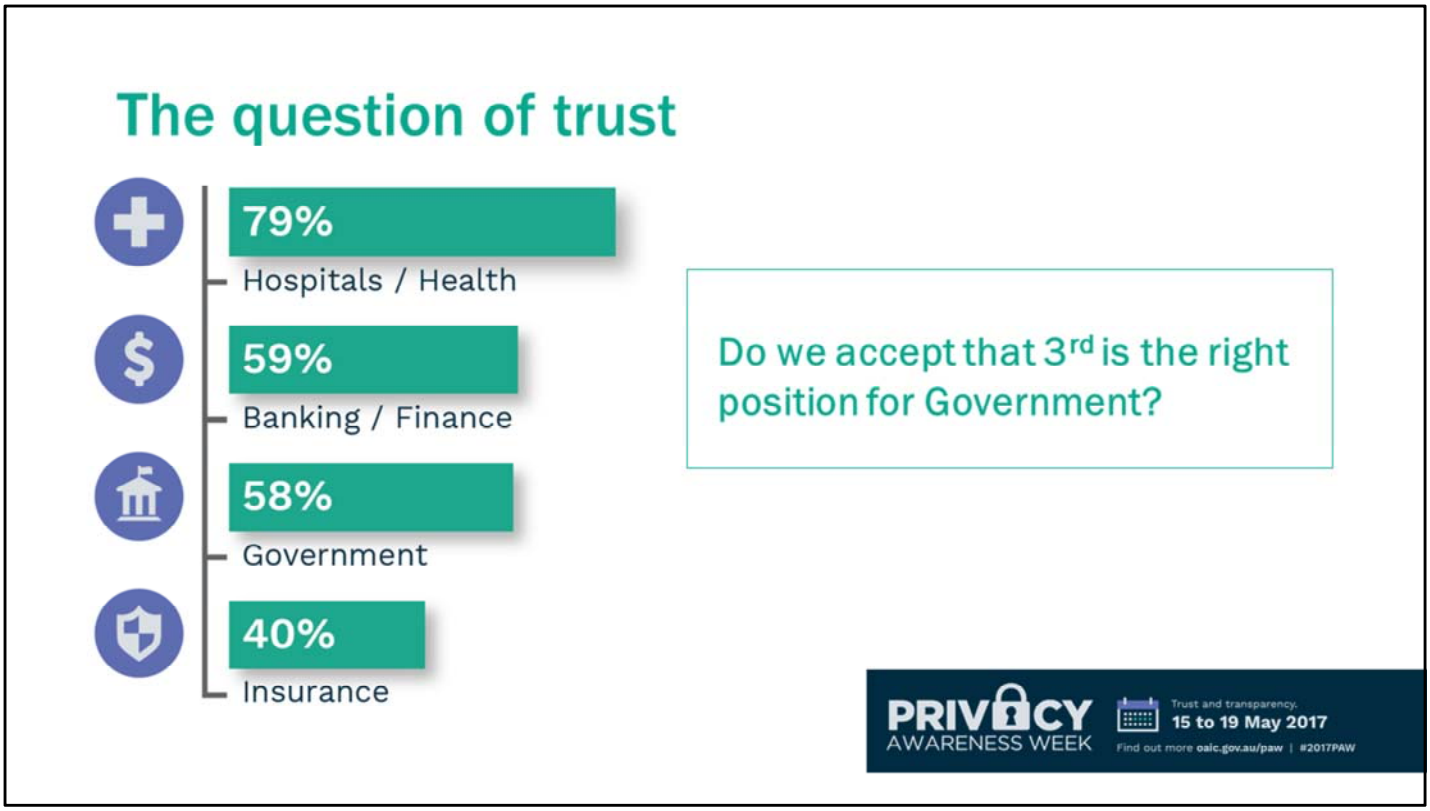
Also, if you make it easy to understand and manage privacy, people tend to feel more empowered about the transaction.

And the apparent contradiction I highlighted earlier – between rising concern but static action – is in part due to a sense of being overwhelmed by the issue.

So, agencies that make privacy transparent and easy will be more trusted – building the community confidence that we need for data innovation projects.

Now, "surely" you may ask, "Government is already the trusted source on data protection?"

Well, let's see….



The ACAPS survey does measure net trust by sector, and in 2017 we see that all sectors have held their 2013 rankings.

Health, financial and government are once again the top 3, and the net trustworthy score for government is 58% (albeit just 1 percentage point behind Banking and Finance).

While that keeps us in the top three – and that is positive – my view is we need to be at number 1.

If there's any doubt about that then I suggest that we ask ourselves why we would accept that the banking sector, or the health sector, should inherently be more trusted with personal information than the APS?

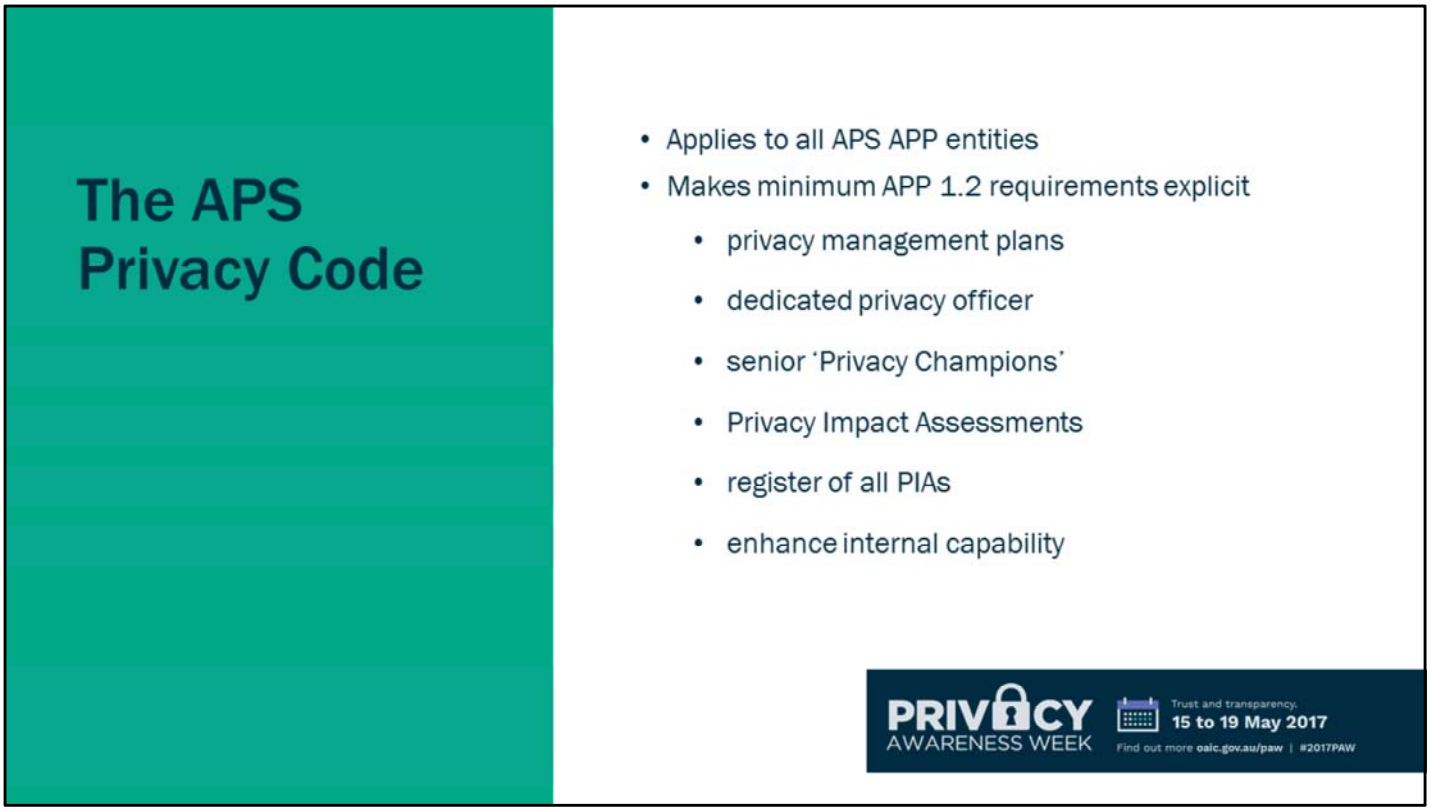
In fact, in the 2007 survey the Government sector was rated second, above Banking and Finance, a position lost in 2013.

Those are sectors, like the APS, with immense transactional volume and hold some of the most sensitive data of individuals. And, they are not immune to data breaches and incidents. So, in terms of environment, all three sectors operate on similar playing field.

Therefore, trust and transparency, as I have said on many occasions, will be the defining aspects of any successful policy, project or system (or organisation for that matter) that is built on personal information.

And, it was with that in mind, that yesterday I jointly announced with the Secretary of the Department of Prime Minister and Cabinet (PM&C) that I would be developing an APS wide Privacy Code for the Australian Public Service, to take effect on July 1 2018.

So it's great that we have this opportunity today to unpack that announcement a little, to explore what the Code means to Agencies and why we're implementing it.



First, to the formalities.

The Privacy Code is a binding instrument created under the Privacy Act.

It will apply to all Australian Government entities currently subject to the Australian Privacy Principles.

And it will make explicit minimum expectations of all agencies under Australian Privacy Principle 1.2 (APP 1.2), which requires reasonable practices, procedures and systems in place to comply with the APPs.

More specifically, the Code will require agencies to:

- Have a privacy management plan
- Appoint a dedicated privacy officer
- Appoint a senior official as a 'Privacy Champion' to provide cultural leadership and promote the value of personal information
- Undertake a written Privacy Impact Assessment for all 'high risk' projects or initiatives that involve personal information
- Keep a register of all Privacy Impact Assessments conducted and make this available to the OAIC on request
- And take steps to enhance internal privacy capability, including by undertaking any necessary training.

As you may note, the Privacy Code makes requirements of practices that many agencies, and businesses for that matter, already have in place.

Indeed, if you're in an agency that has a privacy-by-design approach, and has been implementing our guidance around Privacy Management Plans, PIAs and so on, then the Code will mean little net change.

And I stress, my implementation of the Code is not a negative reflection on any APS agency or their privacy management.

But it is about ensuring that a single, clear, high standard is created across the APS.

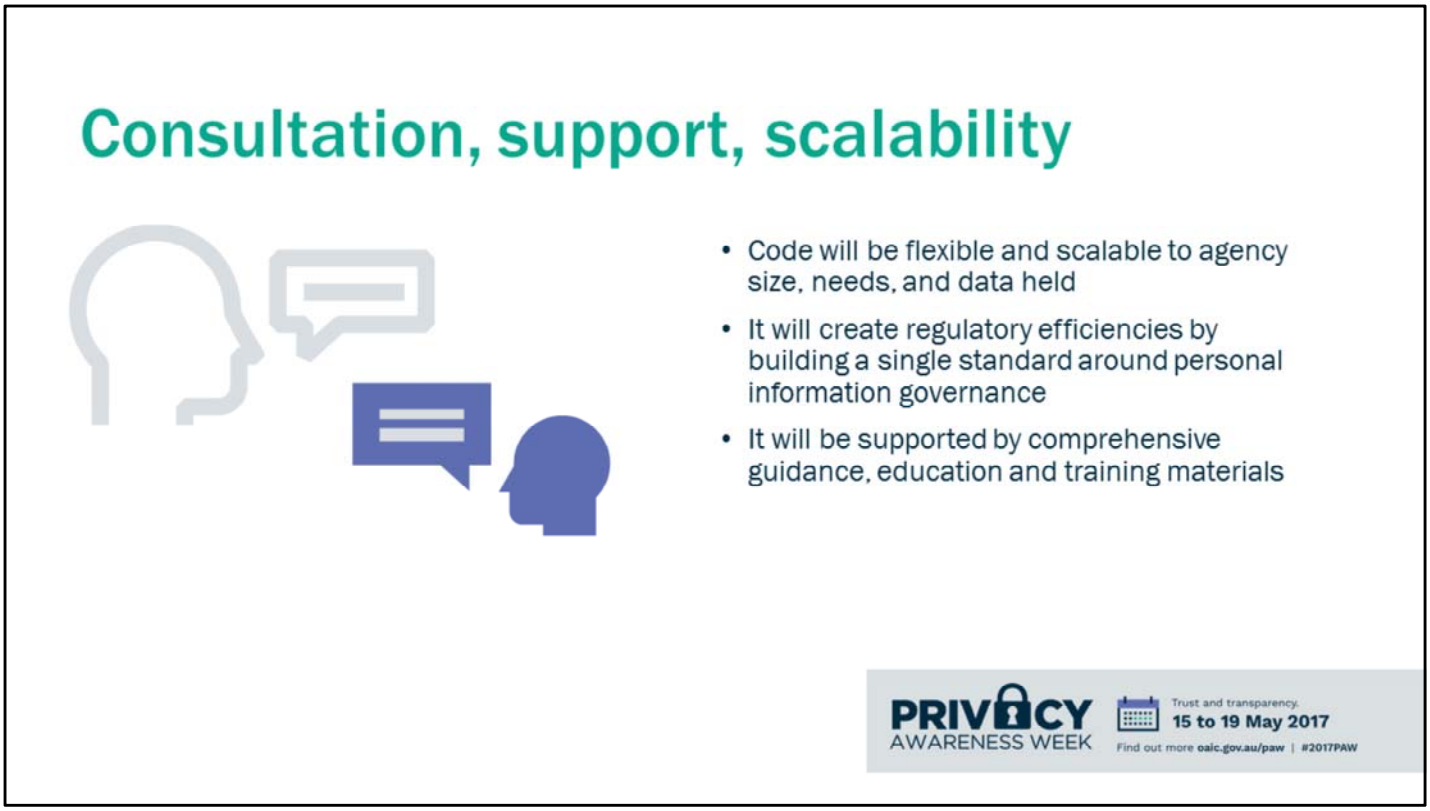
It is about making best practice, the only practice for the APS.

That single high standard across all agencies is vital to improving community buy-in for data sharing.

It is also decidedly in the interest of agencies who already do manage personal information to high standards.

After all, we know that the distinction between tiers of Government, let alone specific agencies, is not well understood by the average Australian (nor should we expect it to be). And therefore, a fall in standards by any agency is a risk to the public confidence in all agencies.

The good news is that, equally, public assurance that personal information provided to any agency will be protected no matter where it travels within government, will enhance community support for shared services, data sharing and other innovations.



Accordingly, my office wants every agency to succeed in this endeavour, and will support you in both design and transition to the Code.

The Code will be flexible and scalable, and will take account of the agency's size, and the sensitivity and amount of personal information it handles.

Its implementation will create regulatory efficiencies by building clear minimum expectations around information governance.

And its transition will be supported by comprehensive guidance and educational materials developed by the OAIC, to assist agencies to comply.

As is the case with our Notifiable Data Breaches page on our website – we will shortly establish a dedicated resource point for updates, events and draft materials in the development of the Code.

This will be live before the end of June.

We will also be establishing a dedicated Privacy Officer Contact network to act as the primary conduit for agencies on code development, transition and accountability.

Turning then to some of the key milestones ahead of us:

- We expect the Draft Code to be published for consultation in June 2017
- Consultation on the draft Code will occur, including making the draft available for public comment in June and July
- The OAIC will be developing supporting resources, in consultation with agencies from now until December this year
- Code documentation and supporting resources will be in published December
- Training course for privacy contact officers will be available from February 2018 onwards
- And the Code takes effect on 1 July 2018.

And of course, the Code being a binding instrument does mean that failure to comply will be a breach of the Privacy Act.

- This is about a national leadership position
- APS should be seen as the leader in personal data protection
- This is commensurate with our unique personal data assets and unique powers to obtain data
- The 'single high standard' supports data sharing and re-use that maximises data value
- This in turn is supported by public confidence that the whole APS is a "privacy-by-design" entity

I'm fairly confident that the many privacy professionals and officers in this room already understand the desirability of a privacy-by-design approach across the APS.

But the Code is about instilling that understanding across all levels and critical roles which handle personal information across the APS. It ensures visibility of personal information risks and opportunities at senior levels.

Above all, this is about a leadership position for the APS in the field of personal data protection.

We need a Privacy Code because the APS needs to be, and needs to be seen to be, the national leader in this field.

A binding whole-of-government Code telegraphs this within Government and out to the community.

It also creates a fair response to that question of "just terms".

Because of the unique position Australian Government agencies are in, in terms of their ability to collect and hold vast amounts of personal information, it is only fair that they demonstrate the highest standards of personal information protection.

And, because the value of government data may be best realised when it can be shared and built upon, that standard needs to be consistent right across the APS.

The APS Privacy Code takes best-practice tools and processes – which are already used by many agencies – and makes them requirements for all agencies.

That provides assurance – both across the public service and in the community – that Australian Government data sharing and innovation has privacy built in, by design.

On that note, thank you for your attention today.

I think we have some immense opportunities ahead to reshape the capability and personal information performance of the APS.

I look forward to working with you on what we believe will be an exciting and transformative year ahead.