Foreword:

Welcome to another packed edition of the Member Bulletin!

Echoing our President’s recent letter to Australia’s newly appointed privacy commissioner, the iappANZ welcomes Timothy Pilgrim to his exciting new role. Being a privacy commissioner during a time of sweeping change in privacy regulation is sure to be both challenging and immensely rewarding.

In this edition, the progress of privacy law reform has piqued the interest of our Editor-in-Chief, who tongue-in-cheekily reminds us that the journey itself can define a nation. A daring member takes the time to unpack the proposed new Australian Privacy Principles; our past Pres logs his blogs about APEC’s growing privacy reach and the notion of building privacy in (not bolting privacy on); and I weigh in on a topic that has made me bare my teeth in defence of my cubs – do people really “get” kids’ attitudes about privacy these days? Maybe a little reflection about “when we were that age” is in order…

Please take note of the call for submissions for the annual iappANZ conference, being held this year on Tuesday 30 November 2010 in Sydney. I encourage you to send the call to those in your network with an interest in the conference theme – to promote the conference, generally, as well as to introduce the iappANZ to the privacy professionals out there who do not yet have the benefit of linkages to our association.

All the best,

John Pane  
CIPP CIPP/IT  
Vice President  
iappANZ
Privacy reform in Australia – lessons from the… hare?

Found at number 226 in Perry’s Index to the Aesopica, the Tortoise and the Hare is one of Aesop’s better known fables about perseverance, patience and potential.

The story concerns a hare who mocks his slow moving peer, the tortoise. The tortoise takes exception to the teasing and challenges the hare to a race. The tortoise (plodding steadily) and the hare (blitzing the starting metres) set out on their course, with the hare calling behind to taunt the tortoise and even laying down beside the course to take a nap. The hare wakes from his nap to the sound of celebration. To his dismay, the hare realises that the tortoise passed him on the path to reach the finish line first.

Law of the handicap of a head start

Also called dialectics of progress, the law of the handicap of a head start describes a phenomenon where a perceived or actual initial advantage (the “head start”) eventually becomes a handicap when striving to progress or reach a new goal. When Society A dedicates itself to certain standards and there is a broader social, economic or technological move to change those standards, it is hard for Society A (which at one point had a “head start” over other societies) to adapt – possibly leaving them stuck with obsolete technology, laws or practices that impede further progress.

Dutch journalist and historian, Jan Romein, first discussed this phenomenon in his 1937 essay on technology called "The dialectics of progress", which was part of the series "The unfinished past". In his essay, Romein questioned why the London he observed on a recent trip was still lit by gas lamps and not electrical lamps, which were used by the majority of other European capitals. He then went on to explain that the “head start” of London (i.e. their possession of street lights before most other cities) was now holding them back from replacing them with the more modern electric lights. Their advantage in already having lit streets led to apathy in modernisation – after all, what was the great hurry?

This law is similarly illustrated by Aesop’s fable, which (along with its more obvious lesson) highlights the inescapably human flaw of arrogance: The hare is so certain of its racing prowess, and so confident that it has progressed further than the tortoise, that it wastes time, assumes (but does not verify) its advantage and does not take into account the steady progress of the tortoise. Eventually, the tortoise wins.
When it comes to privacy law reform in Australia, which is now reviewing, revisiting and revising the way the country has approached privacy regulation for years, it is quite impossible to ignore Aesop and Romein whispering in unison in the privacy professionals’ collective ear – “Maybe your head start has made it harder for you to adapt!”

**Mistaking ourselves for the tortoise**

In the 1980’s, being “first-in, best-dressed” in privacy regulation was a clear political advantage (the politicians didn’t really want the Australia Card, I’m sure…) with Australia running at the front of the Asia-Pacific pack. And now, times are changing… the privacy landscape we all knew then has morphed, due largely to a proliferation of technologies (particularly the ‘borderless’ internet-enabled ones) and a change in attitudes (particularly social and generational concepts) regarding when, where, how and about whom personal information ought to be protected.

Our race so far…

**Race Leg 1** - The [Australian Law Reform Commission](#) released its report on the review of privacy law in Australia in 2008, detailing sweeping changes that would usher Australia into the modern privacy age.

**Race Leg 2** - The Government announced its first stage response to that report in October 2009 (a staged approach being required due to the sheer number of ALRC recommendations spanning all aspects of privacy regulation in this country). In June 2010, the Government released draft legislation that would implement part of the first stage response – that being a set of new Australian Privacy Principles (APPs) based on the ALRC’s suggested Unified Privacy Principles.

**Race Legs 2 (continued) and 3** - On the last sitting day of the Federal Parliament before the Federal Election was called, two separate Senate Committees were given references to review privacy in Australia.

<table>
<thead>
<tr>
<th>Race Leg 2 (continued) – Senate Committee re: implementing legislation responsive to ALRC recommendations</th>
<th>Race Leg 3 – Senate Committee re: looking at online privacy protections</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Race Leg 2(a)</strong></td>
<td><strong>Race Leg 3</strong></td>
</tr>
<tr>
<td>First, the Senate referred the exposure drafts of Australian privacy amendment legislation (as arising from the 2008 ALRC recommendations and the Government’s subsequent response) for report and inquiry by 1 July 2011. This referral went to the Senate Finance and Public Administration Committee. As a first phase in this inquiry, the Committee will inquire into and report on the APPs exposure draft by 21 September 2010. The Committee has invited written submissions from the public addressing any issues in relation to the APPs exposure draft by 27 July 2010. The Committee expects to receive 3 more blocks of draft legislation and to call for submissions in corresponding stages, all the way up to June 2011. There may even be a fifth round of submissions.</td>
<td></td>
</tr>
<tr>
<td>On 24 June 2010 the Senate also referred “The adequacy of protections for the privacy of Australians online” to the <a href="#">Senate Standing Committee on Environment, Communications and the Arts</a> for inquiry and report. The Committee is seeking written submissions for its online privacy inquiry by 23 July 2010. The reporting date is 20 October 2010.</td>
<td></td>
</tr>
</tbody>
</table>
calling for views on the package as a whole.

<table>
<thead>
<tr>
<th>Race Leg 2(b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remember, after all that, the <strong>second stage response</strong> to the ALRC’s recommendations is still due from the Government covering such issues as data breach notification, removal of exemptions in the current Act and a statutory cause of action for breach of privacy and other issues believed to be more controversial.</td>
</tr>
<tr>
<td>I’m sensing the Senate Committee will be busy for some time to come…</td>
</tr>
</tbody>
</table>

Discreet queries made by a fellow Boardie to the Committee Secretariats indicate that the calling of the Federal Election will not likely alter the dates of the inquiries relevant to Race Legs 2 (continued) and 3. However a delay of a week or two for lodging submissions may be possible on request.

By now, anyone reading this could be forgiven for thinking we are the tortoise (“slow and steady wins the race”)… but I would argue that we are, in fact, the hare. Hamstrung by the requirement to reform all the privacy regulation we’ve put in place since 1988, the hare is faced with the difficult tasks of

1. taking what was a good thing;
2. assessing where it could be made better (and where we can confidently retain the status quo);
3. showing stakeholders, including the community, how making it better will improve how privacy (legislatively and conceptually) is done in Australia;
4. agreeing to the actions necessary to make it better;
5. taking those actions; and
6. getting back in the race.

Of course, getting back in the race means resisting the urge to continue to be a hare (e.g. racing ahead, failing to look back, taking a nap/ resting on our laurels/ doing what we’ve always done), in favour of taking the (slightly faster than a) tortoise approach of steadily and meaningfully achieving the goal of being a world leader in privacy protection and regulation.

**Nicole Stephensen**  
Editor-in-Chief (Member Bulletin)  
iappANZ Board

**Ed’s Note** - *Thanks to Malcolm Crompton (iappANZ Board) for providing me with a digestible synopsis of the “race” to date for use in this article.*

**The APPs are here!!! (... in draft)**

On July 24 2010, Senator Joe Ludwig announced the release of the first exposure draft of the new Australian Privacy Principles (APPs). The announcement was somewhat overshadowed in the media by two other events of the day: the political assassination of increasingly unpopular Prime Minister Kevin Rudd and the television elimination of equally unpopular Masterchef contestant Joanne.

The APPs will be part of a new Privacy Act (Act) and are the latest step towards implementing the recommendations made in 2008’s Australian Law Reform Commission (ALRC) report, *For Your Information: Australian Privacy Law and Practice*. 
While much anticipated by the privacy professional community, the draft APPs could use a little unpacking… and probably a good measure of discussion before (and during!) the review process.

**The Australian Privacy Principles**

Thirteen APPs will replace both the Information Privacy Principles (IPPs) (for the Commonwealth public sector) and the National Privacy Principles (NPPs) (for the private sector), although there are some areas where public and private sector obligations will differ. The collective term ‘entities’ has been introduced to cover both ‘agencies’ and ‘organisations’. The APPs are relatively closer to the NPPs than the older IPPs, with the effect that the changes will be more extensive for the public sector.

The APPs do not include a number of health-related provisions which may have been expected from their inclusion in the IPPs and NPPs. This is because the Government is separately reviewing health privacy (and other areas referred to below) for later release. It is possible that consequential changes may be made to the APPs to reflect those other reviews.

As well as the APPs, the exposure draft includes some definitions and provisions relevant to the interpretation of the APPs.

The Australian Information Commissioner – a new position which will oversee the Privacy Commissioner from 1 November 2010 – will be expected to issue guidance materials to assist entities to comply with the APPs.

**Offshore data transfers and activities**

Currently the Act extends to the offshore activities of private sector organisations in relation to Australian citizens and permanent residents. The exposure draft will extend this to apply to public sector agencies as well, and to protect all individuals, not just Australians.

APP 8 will regulate ‘cross-border disclosure’, where NPP 9 regulates ‘transborder data flows’. The Government has sought to make it clear that:

- there will be a cross-border disclosure where a third party offshore has access to personal information that remains in Australia; and
- there will not be a cross-border disclosure where personal information is merely routed through servers outside Australia.

The new cross-border disclosure regime will mean that Australian entities that disclose personal information to third parties overseas will generally be liable for privacy breaches committed by those third parties – although the Australian entities may have recourse through their contracts. Some exceptions will apply. There will be a consent exception, as there is in NPP 9, however consent will only be valid where the individual is told that the entity will not be accountable for any APP breach by the foreign recipient.

Another notable change from the NPPs is that the exception relating to foreign laws and binding schemes will only require substantial similarity to the APPs ‘overall’. This relaxation of the requirement may go some way to opening up that exception for greater use by entities transferring personal information to other countries with robust privacy regimes. Furthermore, the Government announced last year that it accepts the ALRC’s recommendation that the Government publish a list of approved foreign laws and schemes for this purpose.

**Privacy policies and notices**

The requirements for privacy policies and notices will be expanded to require additional details about matters including the following:
Privacy policies

| How individuals can access and seek correction of their personal information | The fact and circumstances of data collection where not apparent |
| Complaint processes | Reference to privacy policy regarding complaint processes |
| Cross-border disclosures | Cross-border disclosures |

Identification of specific laws or orders requiring the personal information to be collected

Direct marketing

The new APP 7 on direct marketing applies to private sector organisations only, and is subject to the Spam Act and the Do Not Call Register Act. Accordingly APP 7 will primarily apply to direct mail.

Use or disclosure of sensitive information (such as health information) in connection with direct marketing will generally require consent. Where other personal information is involved, organisations will need to provide a simple and effective opt-out.

Where an organisation has collected personal information from an individual, the organisation may use and disclose that information for direct marketing where the individual would reasonably expect it. Where the individual would not reasonably expect it, or the information was collected from a third party, the organisation would need consent (unless impracticable) and would need to prominently draw attention to the opt-out.

Individuals will also have the ability to contact an organisation to:
- opt out of third party marketing facilitated by the organisation; or
- request the source of their personal information.

Security

An intriguing addition to APP 11 is the word ‘interference’. That is, entities will be required to protect personal information from misuse, interference and loss and from unauthorised access, modification and disclosure. This addition was not one of the ALRC’s recommendations and was not mentioned in the Companion Guide released with the APPs. It is unclear how ‘interference” will add to the other words, which are used in both the NPPs and IPPs.

Other changes

Other notable changes from the current Act include:
- specifically requiring entities to implement privacy compliance, for example through appropriate procedures and systems (APP 1);
- allowing individuals to identify themselves by pseudonym where appropriate (APP 2);
- allowing entities to destroy or de-identify unsolicited personal information as an alternative to complying with the APPs (APP 4);
- allowing collection of sensitive information without consent by the Defence Force in connection with war, aid and certain other offshore operations (APP 6);
- allowing some collection, use and disclosure of personal information (including sensitive information) in connection with missing persons or diplomatic processes (APP 6);
• extending the exception for use and disclosure in connection with suspected unlawful activity to cover serious misconduct (APP 6);
• allowing some use or disclosure of personal information in connection with alternative dispute resolution (APP 6);
• extending the principle on government identifiers to State and Territory identifiers as well as Federal identifiers (APP 9);
• extending the data quality principle to require entities to take steps to ensure that personal information used and disclosed is ‘relevant’ (APP 10);
• where personal information is corrected, requiring entities to inform previous recipients of the incorrect information, where requested (APP 13);
• extending the definition of ‘sensitive information’ to include certain biometric information; and
• removing the requirement for Government agencies to submit annual Personal Information Digests to the Privacy Commissioner each year.

Senate Committee

The APPs and their Companion Guide have been referred to a Senate Committee (Committee) for review. Submissions were due by 27 July 2010. The Committee is due to report on these matters on 21 September 2010.

The Committee’s final report is due on 1 July 2011 and is also expected to consider the following additional components which the Government plans to release in the interim:
• consumer credit reporting reforms;
• health privacy reforms; and
• reforms to the powers of the Australian Information Commissioner.

I’m interested to see what happens next – not just in terms of the Senate Committee review, but in terms of the general uptake of this new (but not too new) direction in privacy regulation.

Kaman Tsoi
iappANZ member

Kaman is a Senior Associate with Freehills in Melbourne, specialising in privacy, technology and telecommunications law.

BLOGGED: APEC’s clear privacy message: actions speak louder than words

The Asia-Pacific Economic Cooperation (APEC) has launched an initiative to help boost consumer trust in e-commerce by fortifying enforcement of regional data privacy laws.

The APEC Cross-border Privacy Enforcement Arrangement (CPEA) will serve as a platform for authorities to engage in information sharing, evidence collection and complaints handling, among other imperatives. The formal commencement day was 16 July 2010. Initial participants include the Office of the Privacy Commissioner of Australia, the Office of the Privacy Commissioner of New Zealand, and others.

The CPEA is a structured regional arrangement, setting out specific procedures and mechanisms for cooperation among participating privacy enforcement authorities in APEC member economies. As such, it is a world first for privacy regulators.

Here is a clear case where actions are speaking louder than words!

Agreeing on the APEC Privacy Guidelines in 2004 was significant in itself. Endorsement was achieved in record time in no small part through the remarkable efforts of Peter Ford who was in the Attorney-General's Department of Australia at the time.

But some of us felt that more needed to be done: how could the framework be given life?

After a series of informal discussions, we developed a formal proposal for technical assistance seminars which APEC agreed to fund. Peter Ford and I organised and facilitated the first seminars in 2005: Hong Kong in May and Korea in September.

These seminars and the meetings of the Data Privacy Subgroup of the APEC Electronic Commerce Steering Group culminated in the Data Privacy Pathfinder. The Pathfinder was developed during the 2007 seminars and meetings when Australia hosted APEC. The Pathfinder was made up of 9 projects. These included the projects leading to the CPEA.

And now we have a real and formal CPEA in place. The step by step development of the Pathfinder projects are due to the effort and persistence of a large number of people from all round the APEC region, but particularly from Canada, Chinese Taipei, Korea, Japan, Mexico, the US as well as Australia; both in government, business and non government organisations.

Congratulations to all who have been part of this journey.

Even though the journey is not yet over, with some Pathfinder projects still not quite complete, at the risk of repetition, we are clearly seeing actions speaking louder than words!

Malcolm Crompton CIPP
iappANZ Board

Malcolm is Managing Director of Information Integrity Solutions (IIS), a globally connected company that works with public and private sector organisations to help them build customer trust through respect for the customer and their personal information. He was also foundation President of the iappANZ.


BLOGGED: Privacy by Design: An oxymoron, an impossibility or the way to go?

What is privacy, REALLY?

What is 'Privacy by Design'?

After the concept was first developed by the Information and Privacy Commissioner of Ontario, it has become the new framework for thinking globally: Leaders in the European Commission; the European Data Protection Supervisor; the UK Information Commissioner and interests in the US such
as the [Department of Commerce](http://www.commerce.gov.au) all see great promise in this way of ensuring privacy is 'built in' not 'built on' later as a compromise.

A number of recent initiatives in Australia have included Privacy by Design as part of more comprehensive strategies to respect privacy. These include the health identifier being issued for all Australians.

I was asked to speak on this topic at a [Big Picture Seminar](http://www.bigpicture.com.au) organised by [NICTA (National ICT Australia)](http://www.nicta.com.au) in Brisbane.

Now it is [out on video](http://www.youtube.com/watch?v=example_video) and is based on a [PPT that is complete with links to wider references](http://www.ppt.com) and includes a short [video of UProve being used in Germany](http://www.uprove.com). The talk went over well and I hear is being sought for replay on local TV.

Since then, Privacy by Design has come up again in the debate about Facebook and privacy, with regulators asking questions and a court case in Canada. It was the subject of a short segment on the Channel 7 Morning show earlier in July which you can see (after a short ad) at "[Facebook privacy policy poked](http://www.facebook.com/privacy_policy_poked)".

The jury might be out, but in my view Privacy by Design is not an oxymoron. It does take a clear mind and persistence to achieve, with rewards for all, including the financial bottom line. But we have more to do!

**Malcolm Crompton**  
CIPP  
iappANZ Board

Malcolm is Managing Director of [Information Integrity Solutions (IIS)](http://www.iis.com), a globally connected company that works with public and private sector organisations to help them build customer trust through respect for the customer and their personal information. He was also foundation President of the iappANZ.


---

**The boundaries of babes**

I read a really interesting article in The Age recently. At the start of the month the St James Ethics Centre held their IQ2 debate on the topic of ‘Young People and Privacy’.

The former Victorian police commissioner Christine Nixon posited this view for the negative: “Young people do not care about their privacy and there is little reason to protect it. They use Twitter and Facebook. They appear on Big Brother. There has been a generational shift”.

"These arguments about protecting people's privacy: in many cases people don't care about their privacy being protected," she said.

That is an interesting position. It appears to be a fair observation. But is it really? Now, I would have thought, especially having had the benefit of a long career in law enforcement, Ms Nixon may have observed that the behaviour of young people, particularly being able to gauge, understand and take *risks*, changes with time. Indeed many young people will look back in 10 years time and shake their heads in disbelief at some of the things that they have done. (Sorry to disappoint you but my numerous skeletons remain firmly entrenched in their respective closets!)

In the context of adolescence and young people, the term *risk* all too often has alarming associations: unprotected sex, experimenting with drug use, drinking and driving, and more.
Many of the risks we expect young persons to take—creating romantic relationships, finding and keeping a responsible job, perhaps travelling far from home for schooling or to live on their own for the first time—obviously are positive, major steps toward independence. At the same time, from the adult perspective, other risks, involving physical recklessness (say, drink driving) or flouting the law (for example, experimenting with drugs), may appear not only dangerous but foolish. It’s often said that young people embrace this kind of risk because “they think they’re immortal,” or at least immune from the consequences of their actions. But what may really be at work here is a crucial gap between what young people rationally know and what knowledge they use in making decisions—a gap that fills in gradually as they learn more from the outcome of each decision (experience).

Let’s look at social media for a minute. MySpace and Facebook have been very successful because they matched social media technology to adolescent and youth behavioural traits and in particular, their desire to connect with other young people in their own ‘private’ space. There they can be free to interact and ‘hang out’. A bit like a digital cubby house, isn’t it?

But what happened as some of these (predominantly Gen Y) users grew older and the social media companies started to shift the boundaries on how personal data was to be used? They objected. They balked. And they let those objections be known. (By the way, have you ever seen the reaction of a young person when a parent tries to ‘friend’ them on a social networking site?)

Which brings me to my point: Most young people may well do things that they would not otherwise do when they are older. A young person’s perception of privacy risks, the value attached to privacy and how to protect it are comparatively underdeveloped to that of an older person. This perception will change, evolve and deepen with both experience (positive or negative) and age.

To say young people do not value privacy may have some limited currency now… but the answer will not be the same in a decade or less.

John Pane CIPP CIPP/IT
Vice President
iappANZ

 Privacy After Hours

Melbourne

Join us monthly for a free “Privacy After Hours” event!

iappANZ members and their guests are invited to mix socially at one of Melbourne’s best lounge bars – Chi. No agenda – just great conversation!

Date: The last Thursday of every month
Coming up: Thursday 29 July 2010 and Thursday 26 August 2010

Time: 5:30 to 8:30pm

Venue: Chi Lounge – Level 2, 195 Little Bourke Street, Melbourne (near the corner of Little Bourke and Russell)

Cost: Free – you pay for your own drinks (happy hour prices to 8pm, $3 bubbles, $5 wine, $10 cocktails).

Enquiries: 03 9895 4475

RSVP: You can simply turn up or let us know you intend to come by emailing us at admin@iappanz.org or telephoning the Enquiries number above.
What’s new in privacy?

Experienced deputy earns top privacy job

Timothy Pilgrim, Australia’s deputy privacy commissioner since 1998, has been appointed to a five-year term as Australia’s new privacy commissioner. Senator Joe Ludwig announced the appointment in a press release issued Thursday 22 July.

Pilgrim replaces former commissioner Karen Curtis, whose six-year term expired this month. Ludwig praised Curtis for her significant contributions to privacy in Australia and said that Pilgrim’s "experience and operational knowledge of the office will be of great assistance when the office transitions to form part of the new Office of the Australian Information Commissioner, which will open its doors on 1 November 2010."

iappANZ President, Kevin Shaw, wrote to the newly appointed privacy commissioner on 26 July to congratulate him on behalf of the association and its members. A copy of Kevin’s letter is attached.

CALLING FOR PARTICIPATION:

iappANZ annual conference – Tuesday 30 November 2010 in Sydney

Building on the sell-out success of our 2009 conference, the annual International Association of Privacy Professionals Australia and New Zealand (iappANZ) conference will be held in Sydney on Tuesday 30 November 2010.

With a theme of Silver Lining: The Privacy Umbrella of Cloud Computing, the conference the only dedicated privacy and cloud computing event in the ASEAN region – bringing together privacy professionals from all sectors.

This focused one-day conference will be an opportunity to not only network with other privacy professionals but learn from others, including leaders in the cloud computing, privacy, legal, information security, compliance and government fields. The day will feature a stimulating mix of international keynote speakers, “lightning talks”, expert led forums and exhibitions.

Forum proposals

The iappANZ is looking for speakers to participate in expert forums on key topics associated with privacy and cloud computing. Our aim is to offer different perspectives and points of view, and to truly engage those attending the conference.

Be a standout presenter and raise your profile among colleagues, competitors, clients and hundreds of others in the privacy profession!
Interested? Please review the call for participation and fill out the required details.

**Sponsorship opportunities**

The conference will be attended by various legal, privacy, compliance, government and corporate stakeholders who advise top executives on the identification and management of privacy risks and the protection of your organisation’s reputation and brand.

By sponsoring an international speaker or a forum/ conference segment the spotlight will be on your organisation in front of a captive audience.

Major sponsors receive prominent recognition in a variety of printed materials, on the iappANZ website and much more. Sponsorships are available at a wide range of levels for this annual event.

**Want to learn more about sponsorship opportunities?** Contact: John Pane at john.pane@iappanz.org

---

**Top mag has cloudy chat with iappANZ President**

iappANZ President, Kevin Shaw, spoke with CIO magazine this month about cloud computing and the necessary uptake of adequate privacy and security controls. He also spoke about the iappANZ conference coming up in November, which will be a stellar opportunity for CIOs and other key operators within the public and private sectors to learn about privacy and security savvy approaches to conducting business in the cloud.

---

**On-line learning – exclusive invitation for iappANZ members**

iappANZ is delighted to invite members to access SAI Global’s Privacy Awareness on-line learning, a course designed to provide general awareness of privacy regulation to staff within your organisation who may have no background in privacy or compliance. It assists your organisation ensure that staff have the privacy basics, which is especially important for any staff who handle customer information.

iappANZ has negotiated with SAI Global to enable iappANZ members to receive a 7.5% discount off the cost of the learning module. When you purchase the on-line learning you also help the iappANZ. On each sale, iappANZ also receives 7.5% of the normal price (regardless of the number of staff you need to train), which will help iappANZ improve its member services.

SAI Global’s e-learning has just won a Platinum Award for Best Compliance Training Programme at the prestigious LearnX Asia-Pacific Awards for the second consecutive year.

For further details please contact Ross Millar, Regional Sales Manager, SAI Global: ross.millar@saiglobal.com

---

**APEC - a longer arm for privacy enforcement**

Senator Joe Ludwig has welcomed enhanced global privacy enforcement made possible through cooperation between Asia-Pacific Economic Cooperation (APEC) members,

The APEC Cross-Border Privacy Enforcement Arrangement, which came into effect on 16 July, will enable participants to give and obtain assistance from foreign privacy enforcement authorities to resolve complaints against overseas companies.
Key participants in this cooperative arrangement include the Australian Office of the Privacy Commissioner, the United States Federal Trade Commission and the New Zealand Office of the Privacy Commissioner, with other authorities in APEC member economies expected to join as participants in the future.

“The Government’s proposed Australian Privacy Principles include a principle dealing with cross-border disclosures of personal information”, said Sen Ludwig in his recent media release.

“This is the first part of a package of significant reforms to Australia’s Privacy Act that will be referred to the Senate Finance and Public Administration Committee for consultation and report.”

“The APEC Arrangement will enhance these reforms by making it possible for privacy enforcement authorities to call upon their international colleagues for assistance.”

Don’t be shy… certify!

Interested in attaining a Certified Information Privacy Professional (CIPP) credential? Please visit the certification page on our website for more information.

ANZ DashBoard Digest

Members and other privacy professionals are able to view the ANZ Dashboard Digest on a weekly basis – a wonderful result of the collaborative spirit and generosity of the IAPP (our affiliates in the northern hemisphere)!

Interested in privacy news specific to our part of the world? Subscribe to the ANZ Dashboard Digest when you visit here or check out the iappANZ website for more information!

Two sides of the same coin: Queensland celebrates Right to Information

Just over a year ago, the Queensland Government commenced legislation giving effect to a series of information reforms for improved access to information held by public sector agencies. The Right to Information Act 2009 and Information Privacy Act 2009 are key features of these reforms and, together, they strike a balance between open, accountable, transparent government and the fair handling of personal information.

The Queensland Office of the Information Commissioner, in partnership with the Queensland Government, will soon celebrate Right to Information Day.

On 27 September, the second annual Solomon Lecture will be held at Brisbane’s Gallery of Modern Art (GoMA). This evening event will include admission to two GoMA exhibitions and refreshments.

On 28 September, the Right To Information Forum will be held at the Sofitel Hotel in Brisbane with a program featuring Queensland’s Attorney General, Beth Noveck (Leader of US President Obama’s open government reforms) and Bernard Salt (social commentator and futurist).
Visit the [OIC website](http://oic.org.au) to obtain a copy of the Right to Information Day program and registration details.

**Brisbane-bound… for WCC 2010**

**World Computer Congress 2010** - Held every 2 years by a host nation, this is the International Federation for Information Processing's main global event!

<table>
<thead>
<tr>
<th>Host City:</th>
<th>Brisbane</th>
</tr>
</thead>
<tbody>
<tr>
<td>When:</td>
<td>20-23 September 2010</td>
</tr>
<tr>
<td>Venue:</td>
<td>Brisbane Convention and Exhibition Centre</td>
</tr>
</tbody>
</table>

The congress combines content from commercial, industry, association and research sectors offering an opportunity to showcase and discover innovative ideas. The content will range from the latest international research, to leading commercial and industry-focused insights and thought pieces, of interest to a wide audience.

The congress attracts expert presenters and thousands of delegates from around the globe. For more information: [http://www.wcc2010.com](http://www.wcc2010.com)