Foreword:

This month is a treat… a bumper edition of the Member Bulletin! Our Editor in Chief recently joked with me that our membership would see through the thinly veiled attempt at ‘wow’ing them with privacy content in advance of the November iappANZ conference… until we both agreed that there is no ‘thin veil’ about it!

The annual iappANZ conference is being held on Tuesday 30 November 2010 in Sydney. To compliment the great work being done by our Communications Partner, the cword, I encourage all iappANZ members to make the conference details known to those in your network with an interest in this year’s theme. This is the only conference of its kind in the Asia Pacific region, and attending will be time well spent.

Also, take a moment to browse our new website! This has been an important undertaking for the Board this year, and we are pleased to provide iappANZ members with increased opportunities to meaningfully engage with the association and its resources.

All the best,

John Pane CIPP CIPP/IT
Vice President
iappANZ
**CMather.com talks privacy and delivery of virtual IT services through ‘the cloud’**

Virtualisation and the delivery of virtual IT services through “the cloud” is the major subject of discussion in IT circles today. It’s actually hard to avoid the discussion because on some levels, the concept of virtualisation is so attractive. The idea of delivering IT services without having to build, manage and maintain IT infrastructure is incredibly appealing, especially to small and medium-sized business enterprises that are looking to manage the ever-present cost of information technology. But how did we even get here?

Virtualised computing is nothing new. The earliest enterprise computers, designed and built in the 1960s, provided a compartmentalised computing experience. By design, these earliest enterprise-level mainframes could generate entirely distinct virtual operating spaces complete with discrete operating systems and virtual machines that completely segregated the processes and operations of one user from those of another. This secure virtualisation architecture was based on “protection rings” that determined which users and operating system processes could do and access what at which security levels.

The move toward decentralised computing originated with the dawn of the personal computer. Small and medium-sized enterprises recognised the value of business computing but had neither the monetary or human resources to introduce centralised computing into their business processes. The comparatively low entry costs of personal and small computers, combined with the growing sophistication of business applications meant that smaller enterprises could take advantage of low-cost technologies.

The inherent limit of decentralised computing, however, is scalability. It turns out that there are limits to the number of servers a business can add without incurring significant costs for data center space, disaster recovery capabilities, maintenance, licensing and support. Business computing is a critical component of most organisations’ business models, but sustaining decentralised computing appears to be both impractical and unwise.
Centralised computing didn’t go away because small businesses adopted a decentralised approach to computing. In fact, quite the opposite occurred. Today’s virtualisation giants quietly improved their products, targeting large enterprises as their primary market share. Today, they’ve increased the processing power and memory capabilities of centralised servers, designed centralised services that appeal to enterprises of all sizes and made products that address the “server sprawl” that SMEs (Small and Medium Enterprise) must contend with daily. By making virtualisation both technologically and financially accessible to the small and medium-sized enterprises, virtualised IT infrastructure providers can help SMEs deliver better IT services at a lower overall cost.

**What are the major benefits of cloud computing?**

Far and away, the benefit of virtualisation is a significant reduction in the cost of information technology infrastructure for a given computing environment. By divorcing the software server from the hardware server, and similarly separating the desktop client from the desktop computer, businesses can spend less on their IT infrastructure. That means fewer servers on-site, “thin” clients on desktops, virtualised data storage, better license management and even virtual networks.

Businesses spend less because they don’t add new hardware each time they want to add a new server. At the same time, virtualisation means that individual users can have the operating system environments that they need (or prefer) without the individual expense associated with purchasing a complete desktop unit and licensing individual software copies.

Businesses spend less on disaster recovery and business continuity infrastructure. Instead, they rely on a common infrastructure partitioned (and instantly reconfigurable) to meet their exact needs. Adding more storage space doesn’t mean adding more disks, and IT infrastructure resources don’t always need to be dedicated to a particular business function.

*All well and good, but does virtualisation work?*

**What are the major disadvantages of virtualised IT infrastructure?**

The impact of a physical hardware failure cannot be underestimated. Hardware can and does fail, and when it fails, it can cripple the servers and processes running on it. If you operate your own virtual IT infrastructure, you may or may not be equipped to respond to the problem immediately. If you contract for virtual IT services through a provider, you need to know what their capacity is to respond to physical failures. Ask for service level guarantees and develop a back-up plan for your most critical business processes and data.

In addition to the impact of physical failure, troubleshooting problems within the cloud can be complicated. With part of your infrastructure outside of your control, you’ll need to rely on the skills and expertise of your virtual IT infrastructure provider.

The freedom to create servers and other virtual machines on an as-needed basis can be tempting because you can create them virtually instantly. Without prudent guidelines on what justifies having a new server, you could end up with a lot of under-utilised (or just plain unnecessary) virtual machines. The justification process for creating a new virtual server
should be similar to the process your organisation used to justify the purchase of server hardware, if only because creating virtual machines does absorb resources.

**Is privacy possible in cloud computing?**

One of the biggest questions about virtual IT infrastructure (which is, by definition, shared) is whether or not the controls in place provide the levels of data security and user privacy that may be required either as a matter of law or a matter of best business practices. **Are your data – created and stored on someone else’s resources – safe from outsiders who should not have access to it?** Is the virtual IT infrastructure robust enough to prevent users in your own organisation from inadvertently or deliberately accessing restricted data?

In a virtual IT infrastructure, the person or organisation that generates data gives up some measure of control over it. Organisations must rely on the infrastructure provider to support, maintain and reinforce data security at all times. When an organisation manages and maintains its own data and IT infrastructure, data ownership rights and data stewardship responsibilities are clear. When data are created and maintained in a cloud, these seemingly simple questions may not have straightforward answers.

**Can a governmental authority gain access to data through the IT infrastructure provider?** How are security breaches handled? Who is ultimately responsible for the resulting harm when sensitive data are stolen or misappropriated from the cloud? What happens to orphaned data? When ownership of data is disputed, how will the virtual IT infrastructure provider respond? Can the provider deny an organisation access to its own data? If yes, under what circumstances? Should certain types of data be excluded from being created or stored in the cloud? What happens to the data if a virtual IT provider goes out of business or gets acquired by another firm?

Laws regarding information, information security, and information privacy are constantly evolving. Often, meaningful regulations aren’t developed until a major incident exposes weaknesses in current laws and practices. Too often, consumers are left to answer these important questions on their own, without any significant legal protection or precedent. In the absence of meaningful regulation, industry guidelines and best practices sometimes suffice. This approach can be powerful among responsible providers and consumers, but it lacks the enforceability of law.
In the absence of specific legal provisions for the handling of sensitive data in the virtualised environment, the best fallback is a contractual agreement or set of agreements among parties that specifies the rights and responsibilities of the virtual IT provider and data creators, and the penalties that can follow in the event of a breach of contract.

**Chris Mather**

*Chris Mather* is the owner and director of CMather.com. The company offers expert advice and consultation on Domain Names, Web Hosting and Web Design Services. This article was created for the iappANZ readership. This, and similar articles, can be accessed at: www.CMather.com.

**Privacy certification… should you be bothered?**

Short answer: YES!!

Privacy is a growing concern across organisations in the ANZ region and, increasingly, privacy-related roles are being made available only to those who can demonstrate expertise. Similar to certifications achieved by accountants and auditors, privacy certification provides you with internationally recognised evidence of your knowledge, and it may be the edge you need to secure meaningful work in your field.

The International Association of Privacy Professionals (IAPP) says it best on their [certification page](#):

“In the rapidly evolving field of privacy and data protection, certification demonstrates a comprehensive knowledge of privacy principles and practices and is a must for professionals entering and practicing in the field of privacy. Achieving an IAPP credential validates your expertise and distinguishes you from others in the field.”

**What certifications are available? Are they relevant to my work here?**

The IAPP offers four credentials, two of which are relevant to iappANZ members. These are: [Certified Information Privacy Professional (CIPP)](#) and [Certified Information Privacy Professional/Information Technology (CIPP/IT)](#).

To achieve either of these credentials, you must first successfully complete the [Certification Foundation](#). The Certification Foundation covers basic privacy and data protection concepts from a global perspective, provides the basis for a multi-faceted approach to privacy and data protection and is a foundation for distinct IAPP privacy certifications – in our case, CIPP and CIPP/IT.

CIPP debuted in 2004 in the US, and has been made available to iappANZ members by our IAPP affiliates. While the IAPP website focuses on the US-based relevance of the credential, the course content itself is applicable to privacy professionals the world over.

CIPP/IT assesses understanding of privacy and data protection practices in the development, engineering, deployment and auditing of IT products and services.

**What about testing? Will I have to travel to Baltimore?**

Although the IAPP website refers to US-based certification testing only, testing is available to iappANZ members locally, with details of testing dates and times made known via the iappANZ website and the Member Bulletin. If you’re interested, **tell us**! We would be glad to put you in touch
with the resources you need to study for certification, and we are happy to organise testing on a more regular basis as demand increases.

For what it’s worth, I’m working on my privacy certifications as we speak. Even with 12 years of expertise in privacy, I can see the benefit…

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

Privacy and the dead

Perhaps for obvious reasons we don’t hear much about the privacy interests of the dead. Privacy law is a mixed bag when it comes to statutory rules for handling the personal information of a deceased individual. Freedom of information laws also give rise to uncertainties regarding the rights of the living to access information about persons dead for up to 30 years.

When presented with the opportunity to start to address this question on a principled basis and to encourage national uniformity in the law, the Commonwealth Government ducked. Constitutional difficulties were cited for not proceeding with amendments to the Privacy Act to extend relevant principles to the handling of personal information about a dead person.

No one seems to have noticed much. Or lamented the passing.

The case for reform

The Commonwealth Privacy Act defines personal information as information about a living individual, except Part VIA which provides a separate regime for the collection, use and disclosure of personal information in the event of a declared emergency, including information about a dead person.

The Government in announcing the phase one response to the Australian Law Reform Commission report rejected three recommendations proposing extension of the law to personal information of an individual dead for up to 30 years.

ALRC 108, For Your Information, acknowledged that a deceased individual may ‘feel no shame or humiliation’, but argued public policy reasons in proposing a new part of the act to regulate the use and disclosure of the personal information of a deceased person, with principles to apply to access by third parties, data quality, and data security.

The report said protection provided by the Privacy Act was analogous to the protection provided by legal duties of confidentiality. Unlike the right to sue for defamation, such rights should survive death, although the lapse of time and overriding other considerations would apply in certain circumstances.

The Commission argued that the statutory protections recommended would ensure that living individuals would be confident in providing personal information, including sensitive information, in the knowledge that it will not be disclosed in inappropriate circumstances after they die; that living relatives and others would be protected from distress caused by the inappropriate handling of a deceased individual’s personal information; and that family members and others would have clearer rights of access to such information where this was reasonable in the circumstances.
Constitutional issues

The Government response acknowledged there were arguments for and against the proposals but cited “significant constitutional limitations” on Commonwealth power to legislate as the reason for rejecting the recommendations.

The Privacy Act was passed on the basis of the Parliament’s power to make laws with respect to external affairs. The Preamble states the legislation was intended to implement Australia’s obligations relating to privacy under the International Covenant on Civil and Political Rights as well as the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

While these instruments do not expressly apply to deceased individuals, the ALRC said it was arguable that the provisions recommended would fall within the rights protected by Article 17 of the ICCPR, that such rights, as matters of international concern, came within the external affairs power, or that they relate to the rights of living individuals or are incidental to those rights. To avoid uncertainty the Commission however suggested it would be preferable to seek a referral of power from the states.

Patchwork privacy laws

With the Commonwealth deciding to drop the ball straight away, the issue of privacy and the dead seems out of contention as part of planned future attempts to pursue uniform national privacy principles.

Information about the dead will continue to subject to the existing laws, or subject to none at all. Such information is outside the scope of the Privacy Act that applies to Commonwealth agencies and big business; covered by some but not all state privacy laws that in the main apply to state government agencies; and in the hands of agencies at all levels of government, but not the private sector, subject to freedom of information laws.

Although the Privacy Act does not apply, the Privacy Commissioner’s plain English guidance to government agencies is “to respect the sensitivities of family members when using or disclosing information about deceased individuals.”

Despite the gap in the law, agencies for the most part appear to act appropriately. Centrelink and Veterans Affairs are no doubt highly experienced in this area and incidents like leaving a computer disc in the Qantas lounge containing details of how the body of Australia’s first soldier killed in Iraq was misplaced are, fortunately, rare.

The Commissioner does not offer published guidance to private sector bodies. Those not covered by the act or who enjoy exemptions such as media organisations engaged in journalism can in effect write their own rules, although banks, insurance companies and others who deal with these issues routinely seem to have well developed protocols.

At the state level, NSW privacy and Victorian health privacy legislation covers information about individuals who have been dead for not more than 30 years. The Northern Territory Information Act, which combines privacy, freedom of information and archives provisions, covers personal information within the first five years after an individual dies. Tasmanian privacy legislation extends protection to the personal information of individuals who have been dead for not more than 25 years. ACT health privacy legislation covers deceased individuals without imposing any time restrictions. Queensland’s Information Privacy Act and the South Australian Information Privacy Principles only apply to information of a living person. South Australia and Western Australia are yet to enact privacy legislation.
FOI issues

Beyond privacy laws, the Commonwealth FOI Act and the state equivalents provide avenues for third parties to apply for access to information about a deceased individual held by a government agency. A decision on disclosure usually involves consideration of whether release of personal information would be unreasonable, or on balance, in the public interest.

Even a spouse seeking access may still need a convincing case. The Queensland Information Commissioner decided that disclosure to the wife of a deceased husband of some but not all medical records (those that would assist her to brief a specialist to give an opinion about the cancer suffered by him) would, on balance, be in the public interest, as it would assist her to pursue legal proceedings in respect of loss consequent upon her husband's death, or to evaluate whether a legal proceeding was available, or worth pursuing.

FOI laws require an agency to take practicable steps to consult the deceased’s personal legal representative, next of kin or another family member prior to disclosure of personal information, and to give weight to any opinion expressed by the third party in reaching a decision.

The words “closest living relative” mean "nearest of kin" or "nearest in blood relation". See, Antill-Pockley v Perpetual Trustee Co Ltd [1974] HCA 52 per Gibbs J (at [6]).

Where siblings differed concerning access to information about their deceased mother the Western Australian Information Commissioner decided the eldest qualified as the closest living relative.

Where parents are separated and in the absence of court orders relating to parental responsibility or statutory prescription, both parents may qualify as the closest living relative of a deceased child.

On occasion, complex and opposing interests must be considered.

The NSW Administrative Decisions Tribunal decided important public interests justified disclosure to the mother of a deceased child, information (with identifying particulars deleted) held by the Police in statements about the child's death provided for coronial proceedings that never proceeded. The decision to grant access was despite the objections of the three people who made statements, including the father/ex husband who was looking after the child when she died, and arguments from the Police that the statements had been obtained on the basis of confidentiality.

Early FOI legislation stipulates that the interest or motive of the applicant in seeking access is generally an irrelevant consideration and not to be taken into account in reaching a decision to grant access. The Commonwealth act operates on the basis that disclosure to an applicant is disclosure to the world.

Recent reforms in some jurisdictions recognise any special interest in access that an applicant may be able to demonstrate. The NSW Government Information (Public Access) Act 2009 (section 55) allows the applicant’s identity and relationship with any other person, motives for making the access application, or any other factors particular to the applicant, to the extent known to the decision maker, to be taken into account in reaching a decision.

While welcome, such a change is a long way short of what is needed. No set of laws can cover every eventuality in such a complex area but there is a case for uniform and consistent principles regarding the handling of information about a deceased individual, whether held by public or private sector bodies.

And a ghost may be heard...
The ALRC recommendations proposed a step in the right direction. It’s a pity that the opportunity has passed without fanfare or fuss… unless distant voices are heard by the Senate Finance and Public Administration Committee which will be looking at proposed privacy reform legislation well into 2011.

Peter Timmins

Peter Timmins is a Sydney based lawyer and consultant who writes the Open and Shut blog - www.foi-privacy.blogspot.com

Privacy law reform: changes and challenges for marketing

One of the most fundamental changes to the Australian Privacy Principles is the inclusion of a Privacy Principle exclusively dedicated to Direct Marketing. This inclusion acknowledges the vital role personal information plays in business and how it underpins our economy.

More importantly the Direct Marketing principle is technology neutral which is important because Direct Marketing encompasses all information based marketing that occurs at a distance and that invites a measurable and tangible response. It includes marketing conducted by mail, telephone, email, the internet and social media.

As many privacy practitioners would know there has been a significant loophole in the National Privacy Principles since their introduction in 2000. Essentially under the current regime an organisation that collects personal information for the primary purpose of direct marketing has no obligation to provide the option to the consumer to opt-out or respect opt-out requests if received. The Australian Direct Marketing Association’s Code of Practice fills this gap and it is fitting that the review of the current Privacy legislation does likewise.

In its recommendations, the Australian Law Reform Commission (ALRC) suggested that the new direct marketing privacy provisions should be changed such that consumers should always have the ability to opt-out and that the law should oblige organisations to respect such requests. The ALRC recommended that the revised Privacy Act should create two different opt out regimes, one more stringent and one less so, dependant on whether an individual is an existing customer of an organisation or not.

The ALRC’s recommendation was accepted by Government in its October 2009 first stage response to the ALRC’s report; however, the Government included a small proviso that the concept of existing customer be changed to existing relationship.

Unfortunately the exposure draft of the new Australian Privacy Principles reflects neither the ALRC’s recommendations nor the Governments view. The new legislation determines that the opt-out regime organisations have to comply with is based upon whether the information that the organisation is using is obtained from the individual or not.

This new approach will create a number of challenges from a number of different perspectives and fails to take into consideration how the marketing industry works. Unfortunately industry’s processes cannot be neatly divided into two streams on the basis of whether information was obtained from the individual or not. Using such a distinction will lead to an environment where consumers, regulators and industry will be unable to easily determine which obligations or rights apply.
In addition, it disregards the approach taken in more modern Australian privacy laws such as the Spam Act and the Do Not Call Register Act which apply different regimes (albeit for consent) according to the conduct of the individual and whether a business or another type of relationship exists.

If the current draft provisions become law every organisation will need to examine, on a case by case basis, each campaign and potentially each individual record to determine whether any elements of the information that is being used were or were not obtained from the individual. Alternatively the organisation will automatically have to default to the more onerous opt out regime.

As a result, any marketing that is not covered by the Spam Act such as mail, internet advertising (when its based on personal information) and telephone marketing will be affected.

Under the draft legislation, the least onerous opt-out regime simply requires an organisation to provide a simple means by which the individual may easily request not to receive direct communications from the organisation.

The more onerous opt out regime will require the organisation to include a prominent statement that the individual may make a request not to receive direct marketing communications from the organisation or otherwise let the individual know that they can opt out of future communications.

Put simply: in a world where organisations frequently apply their own learnings to individual customer data, it is likely that many organisations will technically be required to use the more onerous opt out regime.

**Melina Rohan**
iappANZ Member

*Melina is the Director of Corporate and Regulatory Affairs for the Australian Direct Marketing Association (ADMA). ADMA represents some of Australia’s biggest and most trusted brands on marketing related privacy issues.*

---

**Privacy After Hours**

**Sydney**

<table>
<thead>
<tr>
<th>Save the Date!!</th>
</tr>
</thead>
<tbody>
<tr>
<td>iappANZ members and their guests are invited to a presentation by Australia’s Privacy Commissioner, Timothy Pilgrim, followed by an opportunity to network with others in the privacy field.</td>
</tr>
<tr>
<td><strong>Date:</strong> 16 November 2010</td>
</tr>
<tr>
<td><strong>Time:</strong> 4:00pm</td>
</tr>
<tr>
<td><strong>Venue:</strong> SAI Global – Sydney Office</td>
</tr>
<tr>
<td><strong>More info:</strong> Additional details about this event will be made available shortly</td>
</tr>
</tbody>
</table>
Encore! Encore!

iappANZ members and their guests are invited to an encore presentation of Malcolm Crompton’s ‘Privacy by Design: An Oxymoron, An Impossibility or The Way To Go?’

Hosted by the New South Wales branch of National ICT Australia (NICTA), this promises to be an exciting and eye opening discussion of how Australian government and businesses can ‘do privacy better’. Malcolm’s seminar will be followed by an opportunity to network with others in the privacy field.

Date: 17 November 2010
Time: 4:00 to 5:30pm
Venue: Seminar Room, NICTA
Level 4, 13 Garden Street
EVERLEIGH NSW 2015

More info: Additional details about this event can be found on the NICTA website or by reading the attached brochure.

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 30 September 2010 and Thursday 28 October 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?

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 is 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 network with and learn from other privacy professionals, 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.

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

Brendan O’Connor to champion FOI and Privacy for the Commonwealth

Brendan O’Connor has been reappointed as the federal Minister for Home Affairs, and has added the responsibilities for Justice, Privacy and Freedom of Information to his portfolio.

In a recent web post, O’Connor stated that he will “be continuing the valuable work” of Senator Joe Ludwig and John Faulkner in the privacy arena, which will include an ongoing commitment to implement the Australian Law Reform Commission’s many recommendations for simplifying privacy regulation in Australia.

iappANZ Vice President, John Pane, has written to O’Connor and extended a warm welcome to the role. A copy of that letter is attached.
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

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!

Queensland celebrates Right to Information in style!

On 28 September 2010, the Queensland Office of the Information Commissioner, in partnership with the Queensland Government, celebrated Right to Information Day.

The Day was heralded on the evening of 27 September by the second annual Solomon Lecture, which was held at Brisbane’s Gallery of Modern Art (GoMA). Guest speaker, Don Watson, spoke about the
increasing inaccessibility of today’s public sector language and the hum of many of his points could be heard in snippets of conversation during the opportunity to mingle afterward.

On 28 September, the Right To Information Forum was held at the Sofitel Hotel in Brisbane with a packed program. An iappANZ Board Member who attended both events said that the total program was “relevant, engaging and encouraging for participants”.

World Computer Congress 2010 wraps up

iappANZ Board Member and former Australian Privacy Commissioner, Malcolm Crompton, was a panelist along with other noteworthy privacy professionals at the 2010 World Computer Congress held in Brisbane. A recent news piece reflected on the panel’s discussion of social networking sites, user trust and expectations of privacy.

Editor’s note

In my role as a privacy practitioner, I have discovered that social networking sites such as Facebook represent more than just a personal-social phenomenon… they are very much a professional-social phenomenon too.

It is not unheard of for staff in organisations involved with community services and case management to use online forums, blogs and chat strings with “friends” (such as status notifications and corresponding comments enabled by Facebook) to discuss particular challenges or outcomes in their work with empathetic colleagues. On the face of it, this may be a non-issue (and may even be considered beneficial “debriefing”), but what if such discussions refer to the personal information of people to whom they are delivering a service? Privacy minefield, anyone?!

I was recently scouring the web for information about this very issue. While I did not find what I was looking for in sufficient detail (and I will continue looking, I assure you!), I did note the blog page at CMather.com which held a succinct article on some of the basics of protecting personal privacy (particularly your own!) on Facebook. In lieu of reprinting the bulk of that article here, I encourage you to check out 8 Simple Steps to Protect Your Facebook Profile.

- NS