While iappANZ aims to provide its Members with timely and relevant information about what’s happening in the Australia and New Zealand privacy environments, we are also aware that our membership is part of a unique community of practice – where access to practical strategies for accomplishing the tasks of a privacy professional are as valuable as a resource as the legal, academic and political discourse available through iappANZ and other sources.

The Member Bulletin is a regular publication, exclusive to Members, that highlights the issues affecting today’s privacy professionals as part of their day-to-day business and points Members toward information and strategies that may assist them.

Foreword:

At risk of causing our resident Editor in Chief to haul me off my soap-box and remind me that a foreword is meant to be a snappy “this is what you’re getting this month” pondering of the contents of the Member Bulletin… I trust you’ll enjoy this month’s great compilation AND my commentary on clouds. – JP

Hey! You! Get off of my cloud!

Rewind: 1943. “I think there is a world market for maybe 5 computers”. So (reportedly) said Thomas Watson, then-chairman of IBM.

Fast forward: 1967. In his watershed book Privacy and Freedom, Alan Westin explored privacy and its attributes in an evolving modern world. Westin characterized privacy as a concept that exists everywhere but also differs everywhere according to cultural and personal orientations.

Fast Forward: 2010. No one in 1943 or 1967 would have predicted information technology’s “big bang” or the information economy it set in motion. Revisiting Westin’s premise that “privacy exists everywhere”: Is this actually true, now that our personal data is everywhere – literally!? Enter - The cloud

Cloud computing is already entrenched in our day-to-day lives and is expanding rapidly, but not without problems, some quite complex and novel.

There has been, and will continue to be, a good deal of public discussion of the technical architecture of cloud computing and the business models that support it. However, vigorous debate about the privacy, legal, regulatory and policy issues have not really kept pace.
Government, business and other stakeholders need to do better. What can we do to make the cloud safer and more trustworthy? Here are some issues to think about.

1. **Caveat emptor!**

Users should pay more attention to the cloud provider’s terms of service and the risks of using a cloud provider. But how do we create this awareness? User awareness, I think, is only one half of the problem. At the risk of sounding paternalistic, I say that (as with other types of agreements) users must take personal responsibility when entering into a contract with a cloud service provider, irrespective of whether that service is free or for a fee. If you don’t like the terms, don’t use the service.

2. **Weasel words**

Reading and understanding the terms of service may be the single most important thing for an individual to do before using a cloud provider. This is the other half of the problem mentioned above. Regrettably, the terms of service are often so complex and written in what appears to be a combination of Elvish and legalese, requiring much motivation and persistence to thoroughly review and comprehend them, if indeed one can!

Standardization and simplification of terminology, terms of service and importantly its method of delivery to users would help businesses and especially users to better understand the risks and consequences of using a cloud provider. End User License Agreement, Software Licenses and similar documents should all be written in plain English, in a format which is easily read and understood and important privacy, security and data protection risks highlighted separately... say, in something similar to a dietary nutrition label.

3. **Standardization**

The cloud computing industry or the International Standards Organization could establish standards or common frameworks to help users to analyze the difference between cloud providers and to assess the risks that users face.

One approach may be to group cloud services into types or categories based on how personal data is protected, country risk, etc. For example, there might be two basic (entry level) types of cloud providers. One provider would promise never to use or disclose information unless required by law. It might employ mandatory encryption that prevents the provider from examining the content of user information. Strong governance, auditing and security controls are included in the package of obligations as well. The other class of cloud provider might make no or fewer promises regarding the protection of user information and might retain a broader ability to change the terms of service. This ‘no frills’ provider might operate in a country where there is no privacy legislation.

4. **Glasnost!**

If the cloud computing industry adopted better, clearer and more transparent policies and practices, businesses that outsource data processing and users would be better able to assess the privacy risks they face. For example, some users may be anxious to maintain full ownership of photographs and may not want to grant a cloud provider any rights over their photos. Another example would be where some organizations are happy for their data to be hosted or processed in the UK, but not China or the Philippines where privacy protections are scant.

5. **‘I was never ruined but twice, once when I lost a lawsuit and once when I won one” Voltaire**
Probably the greatest challenge facing the cloud is which law applies and when. It is even more difficult when data may be stored and processed in multiple jurisdictions around the globe.

It is beyond the scope of this small piece to provide an answer on how to build a global regulatory framework but I would proffer a small caution in relation to the predicted status quo when settling legal disputes between cloud providers and the businesses and individuals who use them:

“An incompetent lawyer can delay a trial for months or years. A competent lawyer can delay one even longer”! Evelle J Younger

*Apologies to those of our readers who are lawyers!

John Pane
Vice President
iappANZ

**Practical Privacy: What goes around…**

Two of the last projects I initiated as Privacy Commissioner were:

- The first *Privacy Impact Assessment Guide*; and

The first PIA Guide was finalised and launched in August 2006 by my successor, Karen Curtis. The launch and its subsequent promulgation and uptake within Government has been a real success story.

More recently, in May she launched a Revised *Privacy Impact Assessment Guide* during *Privacy Awareness Week*. Importantly, the Revised Guide explicitly offers guidance on privacy impact assessment in the private sector. This supports the adoption by the federal Government of the following Recommendations in the report of the Australian Law Reform Commission, *For Your Information*, that:

**Recommendation 47–4** “The Privacy Act should be amended to empower the Privacy Commissioner to:
(a) direct an agency to provide to the Privacy Commissioner a Privacy Impact Assessment in relation to a new project or development that the Privacy Commissioner considers may have a significant impact on the handling of personal information; ...”

**Recommendation 47–5** “The Office of the Privacy Commissioner should develop and publish Privacy Impact Assessment Guidelines tailored to the needs of organisations. A review should be undertaken in five years from the commencement of the amended Privacy Act to assess whether the power in Recommendation 47–4 should be extended to include organisations.”

*Privacy & Boards: What You Don’t Know Can Hurt You* was an adaptation of the original guide developed by the Information and Privacy Commissioner of Ontario, Ann Cavoukian, and developed in conjunction with the Australian Institute of Company Directors. The guide was launched in April 2006 at the Institute’s annual conference.
Earlier in May this year, I went to Directorship:10, the Institute’s 2010 annual conference. One of the best sessions of the conference was moderated by Oracle’s Roland Slee on The Commercial Benefits of Today’s Social Networking Platforms. Panellists were Laurel Papworth, Online Community Strategist, World Communities; Ross Monaghan, Lecturer, Deakin University and Kate Carruthers, Strategy Consultant with Hyro Limited. Kate’s slides are online at www.slideshare.net/carruthk while Laurel promises hers will be posted eventually at www.slideshare.net/silkcharm.

The panellists gave us a fabulous expose of three kinds of risks being faced by organisations from new media such as Youtube, Facebook and Twitter. These risks are:

- Employees and others associated with the organisation using new media in a way that undermines reputation and brand. We saw a particularly graphic Youtube example of staff making pizzas on work premises with the branding clearly on display.

- Impact of others on the organisation using ‘crowd sourcing’ to undermine reputation or brand and being able to do so with campaigns that are successful within minutes or hours with thousands of followers. The first thing is to have enough ‘presence’ is to able to learn very rapidly that something is afoot and second to be able to respond. The example given related to two women who claimed, again on Youtube, that they had been barred from flying because they were prettier than the flight crew when in fact the women were barred for unacceptable behaviour, followed by the airline response on Youtube that was posted within hours.

- The converse is also possible: imaginative ways of promoting the organisation’s reputation or brand using new media. We have all seen many examples of this, but one that I really like is the one that promotes a car insurance comparison website via a series of videos and a new media presence that has gone viral via many media, including Facebook: see http://comparethemeerkat.com! Given the rate of increase in popularity of new media and the corresponding decline in older media, engagement is essential if the organisation or brand isn’t to slip quietly from view.

BUT think of the privacy implications! When I identified myself as the previous Privacy Commissioner, there was a roar of interest and the debate was very interesting and very sensible. The first steps for privacy professionals are obvious and simple when this arises in their organisations. For example:

- Make sure you are always first to know about initiatives to use new media and insert a privacy ‘consciousness’;

- Workshop ideas with the staff involved: I was part of a very vigorous workshop recently with a company that wanted to do just that;

- Establish some control procedures in terms of a privacy sign off as well as all the other sign offs before anything goes live;

- Monitor, monitor and monitor after launch;

- Educate staff on the risks they face if they behave inappropriately using new media, while also respecting any whistleblower policy that your organisation might have. Remember: staff will engage in new media whether not they are formally permitted to do so, even if it is only in their private capacity and away from work.
My conclusion: *Privacy & Boards: What You Don’t Know Can Hurt You* may have been ahead of its time, but its time is coming!

_Malcolm Crompton_

iappANZ Board

Malcolm is Managing Director of Information Integrity Solutions Pty Ltd, [www.iispartners.com](http://www.iispartners.com), and is Past President of the iappANZ. He was Privacy Commissioner of Australia until 2004.

**Privacy compliance monitoring – 6 steps to success**

How robust is your privacy framework? I’m sure all of you said “Very”, but how do you know?

Well-developed governance documentation, such as policies and procedures, play an extremely important part in contributing to an effective control environment within an organisation. These documents provide direction and guidance on how an organisation will ensure compliance with relevant legislation, regulation and industry standards and that management goals and corporate strategies are met.

One of the key policies of an organisation is _Privacy_.

**Monitoring compliance with your privacy policy is important because it allows you to:**

1. Determine if your privacy policy, existing procedures and framework are being adhered to
2. Minimise the consequences of policy failure through early detection and remediation
3. Provide feedback that is necessary for policy improvement
4. Demonstrate to key stakeholders (e.g., Board, shareholders, employees, customers) that your organisation is committed to strong policies.

**The monitoring process**

There are many options for monitoring compliance with your privacy policy, such as listing target areas, metrics and methods of measurement. Monitoring must be designed to demonstrate the implementation and achievement of the policy goals. It is also essential that a cost benefit balance is achieved.

Below is an example of a six step process to ensure compliance with your privacy policy.

**Step by step**

<table>
<thead>
<tr>
<th>STEP</th>
<th>ACTION</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Establish goals and objectives</td>
<td>Identify monitoring goals based on privacy policy objectives, risk assessment and feedback from internal incident reporting systems.</td>
</tr>
<tr>
<td></td>
<td>• Determine the baseline (risk assessment)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Identify the desirable outcomes (where do we want to be)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Goal setting (Broad &amp; Specific)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Define target areas to review</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>--------------------------------</td>
<td>---</td>
</tr>
<tr>
<td>2</td>
<td>• Identify high risk areas</td>
<td>If results for target area are always good, measure something else</td>
</tr>
<tr>
<td></td>
<td>• Identify high volume areas</td>
<td>Incident reporting should identify key targets</td>
</tr>
<tr>
<td></td>
<td>• Identify problem-prone areas</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Define minimum standards for routine monitoring in order to reinforce compliance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Determine the ability to readily collect the needed data (may not be feasible or cost-effective to measure)</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Define targets, metrics and methods</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Target</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Compliance with Policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Require workforce training, if applicable</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Metric</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Signed acknowledgment of receipt of policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• % of workforce trained, if applicable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Number of new products which have gone through</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Method</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Procedural audits (required documentation)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Computer system audits (access controls)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Walkthroughs (observations)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Surveys and interviews (workforce awareness)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Drills/mystery shopper?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Establish frequency</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Ongoing (high risk areas)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Quarterly (past problem areas, new policies and procedures)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Annually (departmental reviews)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Informally</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Formally (external)</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Perform Monitoring Reporting</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Document results</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Compare results to objectives</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Identify non-compliance areas</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Highlight areas for root cause analysis</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Document areas for special attention in future monitoring</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Identify trends</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Act on results</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Take corrective action</td>
<td>If there is no analysis and or action, monitoring is a waste of time</td>
</tr>
<tr>
<td></td>
<td>o Revise policies and procedures</td>
<td></td>
</tr>
<tr>
<td></td>
<td>o Refine or focus training</td>
<td>If the results consistently meet expectations, monitor something else!</td>
</tr>
<tr>
<td></td>
<td>o Redesign processes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>o Tighten supervision</td>
<td>Things that can cause</td>
</tr>
<tr>
<td></td>
<td>o Modify monitoring program</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Re-monitor for compliance within 2 – 4 weeks after corrective action is taken</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Continue quarterly monitoring for some period, or flag</td>
<td></td>
</tr>
</tbody>
</table>
Initial and ongoing monitoring and measurement of the privacy policy, its performance and outcomes is essential to ensure that the desired results have been, and continue to be, achieved.

It is also important to identify any gaps, evaluating successes, in ensuring all legislative and regulatory requirements are met.

The completion of monitoring your privacy policy will assist your organisation in proving the effectiveness and overall success of the privacy policy and framework.

Finally, by closely following your monitoring requirements you can assure your Board, shareholders, employees, customers, the value and efficacy of the privacy policy and framework and prove that it is indeed serving its purpose.

Kate Johnstone  
iappANZ member

Kate is Suncorp’s Chief Privacy Officer and was on the inaugural iappANZ Board.

The digital economy – Smartnet explores the privacy side of things

The ‘digital economy’ is the name given to the global online phenomenon that is changing the way that we work, learn, play and communicate. Many see the digital economy as a tremendous opportunity for Australia to punch well above its weight, opening up new opportunities for trade, skills, innovation, knowledge and growth. The national broadband network, Australia’s largest ever infrastructure investment is expected to be a springboard for an economic and social transformation.

But one of the threshold issues that we face as we jostle to become a frontrunner in the global digital race is: what can we do to make increased online activity ‘safe’? And, if we do take online safety seriously, will that prevent Australia from being at the forefront of the digital gold rush?

In many ways Australia’s greatest challenge is to ensure that our national digital agenda looks well beyond Telstra’s share price and whether fibre will go to every home. The digital economy is expected to transform everything from health care and social services through to entertainment. We need to be making sure that we are investing in social and regulatory infrastructure that will enable us to maximise the investments being made in technology. Is this realistic, or even possible?
If Australia’s privacy regime is fragmented and tricky, how can we hope to constructively sustain a rapid escalation of online activity, while also ensuring that personal information and privacy is not fundamentally changed by events taking place in jurisdictions beyond our control and influence?

Next month we will explore these subjects in greater detail, posing the question: ‘As privacy professionals, what can we do make sure that we contribute to this national and global agenda?’

James Kelaher
iappANZ supporter

James is Director of Smartnet Pty Ltd, which is involved with several major federal government departments regarding digital economy strategy. James has formerly held senior management roles in business and government, including the chief operating officer of the Australian Federal Police and the managing director of Medicare. James chaired the government task force that originally proposed the Access Card in 2005 and then he and his deputy, Suzanne Roche, famously resigned when the then minister and departmental secretary stopped taking his advice.

Privacy – a valuable value

Privacy is a set of protections against a related set of problems. These problems are not all related in the same way, but they resemble each other. There is a social value in protecting against each problem, and that value differs depending upon the nature of each problem.

Many theories of privacy describe it as an individual right. But is it more than that? For example, Thomas I Emerson, a legal theorist and modern day architect of American civil liberties laws once said that privacy “is based upon premises of individualism, that the society exists to promote the worth and dignity of the individual. . . . The right of privacy . . . is essentially the right not to participate in the collective life—the right to shut out the community.”[1]

In the words of one American court:: “Privacy is inherently personal. The right to privacy recognizes the sovereignty of the individual.”[2]

Traditionally, rights have often been understood as protecting the individual against the incursion of the community, based on respect for the individual’s personhood or autonomy. Many theories of privacy’s value understand privacy in this manner.

For example, Charles Fried argues that privacy is one of the “basic rights in persons, rights to which all are entitled equally, by virtue of their status as persons. . . . In this sense, the view is Kantian; it requires recognition of persons as ends, and forbids the overriding of their most fundamental interests for the purpose of maximizing the happiness or welfare of all.”[3]

Privacy issues involve balancing societal interests on both sides of the scale. But many of the interests that compete with privacy, however, also involve people’s autonomy and dignity. And therein lies the rub. Free speech, for example, is also an individual right which is essential to autonomy. Yet in can clash with privacy by being in direct conflict with one person’s desire to speak about another person’s life. Security, too, is not merely an important societal interest; it is fundamental to individual autonomy as well. Autonomy and dignity are often on both sides of the balance, so it becomes difficult to know which side is the one that protects the “sovereignty of the individual.”
I think that the value of protecting the individual is a social one. Society involves a great deal of friction, it requires certain information to flow somewhat freely and other types of information to flow selectively, or not at all. Part of what makes a society a good place in which to live is the extent to which it allows people freedom from the intrusiveness of others. A society without privacy protection would be truly Orwellian – always under the constant unblinking gaze of government, business or others.

Privacy is not simply a way to remove individuals from social control, as it is itself a form of social control that emerges from the norms and values of society itself. It is not an external restraint on society but is in fact an essential internal function of society. Therefore, privacy has a social value. When privacy protects the individual, it does so also for the sake of society. As such it should not be weighed as an individual right against the greater social good. It is the greater social good.

Notes:

John Pane
Vice President
iappANZ

Lockstep’s chief discusses Google, wifi and the gulf between IT and privacy

Privacy awareness has been growing strongly for some years. Everyone knows by now that privacy and security are not the same thing; control is the name of the game.

Yet I look at many of the responses to Google’s most recent misadventure over wireless network data and I fear that we still have a long way to go. Too many people are naively downplaying the incident as if privacy and secrecy are somehow equivalent.

It’s understandable for people to have a range of views about privacy. Not only is it personally felt, it is also a soft and multi-disciplined field, involving philosophy, human rights, civil liberties and politics. Yet information privacy turns out to be rather clinical. It’s generally written in such a way that neatly sidesteps the philosophical and moral mine fields. This should make privacy law clearer and more accessible to a wider audience, and yet its implications for IT remain misunderstood by many technicians.

A few weeks ago it came to attention that Google Street View cars were collecting information from wireless networks as they drive past homes and offices. The extent of this collection wasn’t clear at first, and speculation was confined to the seriousness of having Google record the network names and device addresses that are transmitted publicly by any “wifi” installation. In and of itself, basic network data is not identifying, but a nice privacy question arises if it can be linked to named individuals through Google’s other vast data sets. Perhaps that’s a technicality.

Yet the plot thickened after the German Data Protection Authority began probing, with Google then revealing that their cars were also sampling regular data traversing unencrypted networks within range. Google explained in a blog that software written by an engineer for some experimental wifi project was inadvertently included in the main Street View system.
Google has moved quickly and with evident transparency once it learned of the mistake in the software configuration. Meanwhile the Australian Privacy Commissioner has launched an investigation.

On blogs and discussion groups, many have downplayed Google’s collection of what they say is “public” data. Some blame the victims, insisting that if network operators haven’t taken care to lock down their wireless networks and turn on encryption, then their “broadcasts” are basically up for grabs. Yet carelessness with security does not equate to granting blanket consent for personal information to be collected and used for anything a technology company can think of.

The critical legal point to me is crystal clear: Information privacy law basically prohibits businesses from collecting personal information without an express need to do so, or without consent, whether the source data is in the public domain or not. It’s almost a tenet of Web 2.0 that “information wants to be free” but privacy law, like the Trade Practices Act, serves to protect the ‘little guy’ against exploitation by big business.

When they learn about how the Privacy Act treats collection, many IT practitioners are incredulous, pointing out that vast volumes of information is generated and shared as a by-product of how networks work. And this fact of digital life really does need to be understood by all concerned: lawyers, legislators, policy makers, technologists and auditors.

On close inspection it turns out there are technical breaches of the Privacy Act occurring all the time, by virtue of how computer systems operate, and in particular, how they tend to generate and hang on to log data.

A classic instance is the personal data logged by e-commerce servers. Peoples’ shopping habits represent personal information and e-merchants may fall foul of privacy law if they are logging all transaction details without an express need. Worse, if the purchasing history includes medicines or even herbal remedies, then e-merchants are likely holding Sensitive Information. Naturally customers’ buying patterns can be an important marketing resource, but as such it can only be legally exploited if collected with consent and the primary purpose (marketing in this case) has been made clear to all concerned.

Many organisations may find themselves in trouble because their technicians have enabled rich logging just because they can, or they guess the information might be useful one day, without being specific and open about it. The engineer at Google appears not to have understood the Collection Principle, and I’m guessing that the culture at Google has not internalised the privacy principles in general.

Technologists especially should heed several lessons from the wifi misadventure:

— Some might find it counter-intuitive but nevertheless, publicly available information is still subject to information privacy law if it relates to identifiable individuals.

— Terminology matters (as technicians know all too well in their own fields). The words “public” and “private” are not precise, so privacy law avoids them and instead is very specific about “Personal Information”

— Engineers need to resist the temptation to collect personal information just because they can.

— And software quality processes should include pre-release checks to see if excessive information collection is going on for whatever reason.

Stephen Wilson
iappANZ Member
Stephen Wilson runs the Lockstep Group, which provides independent advice and analysis in privacy and cyber security, and researches and develops innovative PETs. See www.lockstep.com.au/about/privacy.

Privacy After Hours

The iappANZ continues to hold Privacy After Hours and other events for its members.

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 24 June 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.

Sydney

SAVE THE DATE
Thursday 10 June 2010

Splitting hairs? iappANZ members and their guests are invited to join Colin Bennett, visiting professor and world-renown privacy expert from the University of British Columbia, Canada, to discuss the very real juxtaposition between the privacy ‘advocate’ and the privacy ‘professional’.

Date: Thursday 10 June 2010

Time: 4:00 to 6:00pm

Venue: To be confirmed

Cost: Nil

More Info: Details of this event will be sent to iappANZ members via email over the coming days.

Brisbane
iappANZ members and their guests

are invited by

Professor Terry Caelli, Director, NICTA Queensland Research Laboratory ~and~
Dr Stefan Lehmann, Convenor of the QRL Big Picture Seminar Series

to this privacy seminar
as part of the
Big Picture Seminar Series!

Privacy by Design:
An Oxymoron, An Impossibility or The Way To Go?

In this seminar, Malcolm Crompton (Managing Director Information Integrity Solutions P/L and past president of the iappANZ), discusses 'privacy by design' as a strategic element of privacy protection and provides contextual commentary in the areas of identity management, social networking and health identifiers.

Please stay following the seminar for refreshments and an opportunity to network with your privacy and security colleagues!

Date: Tuesday 1st June 2010
Time: 3:30pm Registration for 4:00pm start
Cost: Free of Charge
Venue: Customs House
399 Queen Street, Brisbane
RSVP: 24 May 2010 to bigpicture-rsvp@lists.nicta.com.au
More Info: Email the Event Secretariat at: admin@portmann-events.com

Event De-Brief – Patrick Sefton talks off-shoring in Queensland

The after hours mini-seminar and networking event held at the Deloitte offices in Brisbane on Thursday 6 May was a success, and well timed to coincide with Privacy Awareness Week (2-8 May). Participant numbers were lower than the number of RSVPs received (tsk!), however this was offset by the great discussion and lively buzz in the room both during and following the speaker components.

Lemm Ex, from Queensland’s Office of the Information Commissioner, welcomed those attending from various public sector agencies, local governments, legal and professional services firms, banks, industry and academic institutions. His message resonated: privacy protection depends on the involvement of each one of us.
Patrick Sefton of Brightline Lawyers spoke candidly to the group about the privacy and security implications of ‘off-shoring’ personal information, and generated a number of questions about ensuring robust privacy clauses in contracts and the vagaries of implied consent. Those attending had the opportunity to stay and mingle with other privacy professionals, and to pick Patrick’s brain further in relation to some of his key messages.

The iappANZ sincerely thanks Deloitte, Brightline Lawyers and the Queensland Office of the Information Commissioner for supporting this Privacy After Hours event!

Dave Kelly  
Partner – Security and Privacy Risk Services  
www.deloitte.com.au

Patrick Sefton  
Principal  
www.brightline.com.au

Lemm Ex  
Principal Privacy Officer  
www.oic.qld.gov.au

What’s new in privacy?

Privacy (w)Rap

Privacy Victoria’s *Watch this space: Children, young people and privacy* conference on Friday 21 May 2010 was attended by nearly 300 delegates who heard from a diverse range of speakers about privacy issues relating to children and young people.

Opened by Victoria's Deputy Premier the Hon Rob Hulls MP and MC’d by noted Australian actor Noni Hazlehurst, the conference featured the performance of a specially commissioned “Privacy Rap” by Tjimba and the Yung Warriors, plenary speakers and concurrent sessions.

While cybersafety issues were high on the agenda, other aspects of privacy as it affects children and youth were explored including the representation of children in the media, young people and the law, and challenges facing social researchers.

A large number of Victorian secondary school students attended the conference, including five Sponsored Delegates who will be developing a privacy awareness project for their schools during 2010. Members of Privacy Victoria’s Youth Advisory Group also made presentations or chaired concurrent sessions. The Australian Communications and Media Authority and Australian Federal Police had information displays.

Papers from the conference will be published on Privacy Victoria’s website soon.

Queensland announces appointment of first Privacy Commissioner

Ms Linda Matthews will take up her position as Queensland’s first Privacy Commissioner in June 2010. Prior to her appointment as Privacy Commissioner, Ms Matthews was South Australia’s Commissioner for Equal Opportunity.

This appointment represents the privacy cornerstone of Queensland’s information reforms, and provides an important avenue of oversight regarding the right of individuals to access and amend their own personal information and the fair handling
of personal information by Queensland agencies bound by the Information Privacy Act 2009.

According to a media release issued by the Office of the Information Commissioner:
“Ms Matthews, as a deputy to the Information Commissioner, will establish and drive a range of initiatives to support the protection of individuals’ private information held by government agencies, while improving its accuracy and access by its owners. Where there are issues about the release of government held private information, Ms Matthews will oversee the team responsible for conciliating complaints about these matters.”

Privacy Awareness Week 2010 – 2-8 May

Privacy authorities in Australia and across the Asia Pacific marked Privacy Awareness Week (PAW) on 2-8 May 2010. This was an annual event to increase awareness of privacy and privacy protection in the public sector and the broader community. For details of this year’s PAW activities and materials, see: www.privacyawarenessweek.org.

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 – WEEKLY is a winner!

Members and other privacy professionals are now receiving 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!