Foreword:

We have delayed publication of the April Member Bulletin to this week, to coincide with 2011 Privacy Awareness Week (PAW), an initiative of the Asia Pacific Privacy Authorities (APPA) which aims to promote privacy awareness across the public and private sectors. This week, from 1 to 7 May 2011, privacy regulators, lead agencies and other privacy professionals across the Asia-Pacific region will be celebrating privacy and promoting best practice in the collection and handling of personal information.

PAW is now well underway (notwithstanding the 2 May public holiday in Australia) and the iappANZ has an exciting line up of events for you in four major cities. In Brisbane, a lunch seminar on Privacy Impact Assessments is being offered and presents great value to those members seeking to understand what they are and how to conduct them. In Sydney and Auckland, we have organised presentations on social media and privacy from the Australian and New Zealand Privacy Commissioners and what privacy means to Google (one of which was held on 29 April as a pre-PAW launch event). In Melbourne, we have a breakfast seminar on credit reporting reforms and what they mean for your organisation. For further information about these events please check out the Events page on our website!

An April highlight well worth mentioning is the release by the Senate’s Environment and Communications Reference Committee of its report, “The adequacy of protections for the privacy of Australians online”. This report looks at the privacy protections and data collection on social networking sites.

As part of the strategic direction being taken by the iappANZ Board, the Board has decided to recruit a part-time General Manager to further grow the iappANZ and respond to the needs of privacy professionals in Australia and New Zealand. Information about the role can be found in the What’s New in Privacy? section of this Bulletin. [You are welcome to contact me by email at annelies@iappanz.org if you are interested in this role].

All the best,

Annelies Moens
Vice President
iappANZ
**Member Survey: what do you want from your association?**

Well, the results are in! Thank you to all members who took part in our 2011 survey of privacy professionals in Australia and New Zealand.

In total 127 people responded to our survey (116 of whom answered all questions), which gives us a terrific amount of useful data from which to draw some conclusions about what privacy professionals want from the iappANZ.

The iappANZ Board is busy analysing the results to see how we should steer our course for the future, but here's a taste of some of the survey results:

- 96% of attendees at our 2010 annual conference rated it successful from a networking and/or educational perspective
- Privacy professionals want more educational and professional development opportunities, preferably in bite-sized form: 1-2 hour briefings were favoured over half-day or full-day workshops
- We like to eat while we learn: preference was shown for breakfast and lunch ‘learning’ events over after hours ‘social’ events
- A strong preference was shown for practical, skills-based topics, such as ‘how to conduct a privacy impact assessment’ and ‘how to deal with a data security breach’
- Our annual conference is also highly valued, with a preference expressed for a mix of single sessions and parallel sessions, allowing for a greater range of topics to be covered on the day
- Highly valued resources for members include this Member Bulletin and the weekly emailed digest of privacy news from the ANZ region
- 77% of our members would recommend iappANZ membership to their colleagues

Thanks again for your participation in our survey!

Anna Johnston  
iappANZ Board

**Let’s talk about IDENTITY**

The Digital Identity movement is in crisis. Recent months have seen Microsoft shelve its Cardspace offering and cede leadership in this space. The leading web Single Sign On solution OpenID is being abandoned by important players. The blogosphere is thick with the cynical resignation that Facebook has “won the identity wars” (use of the battle cry metaphor is itself indicative of cooperation being shaky).

The Whitehouse has released a sophisticated and well intended model for public-private partnership in electronic authentication, in the form of the National Strategy for Trusted Identities in Cyberspace (NSTIC) (http://www.nist.gov/nstic). It has had a mixed reception. Many in the US are instinctively wary of any government involvement in identity management; in the current political climate, few trust such an initiative to be separable from homeland security programs and other intrusions. Others laud NSTIC for its careful attention to privacy and its adoption of leading edge privacy enhancing technologies from the “Identity Metasystem”.

Anna Johnston  
iappANZ Board
I myself find that NSTIC introduces complexities and new personal information flows that may outweigh its technical privacy measures. NSTIC adopts the new orthodoxy of “identity federation” and enshrines the idea that trusted third party “Identity Providers” and “Attribute Providers” will intermediate between customers and service providers, to broker minimum disclosure of PI between the parties. One important paradox in all this is that users may find themselves disclosing more PI than ever when signing up with identity providers, to enjoy such newfangled services as “Verified Anonymity”.

How did we get to this point? Does digital life really need to be so complicated, with multi-lateral arrangements introduced in the name of securing conventionally straightforward transactions like buying liquor? If we are committed to protecting personal information, through Privacy-by-Design, then complexity is our enemy.

There is deep irony in digital identity formulations. In normal life, we are totally at ease with the concept of identity, with all its nuance and separate dimensions. We understand the different flavours of personal identity, national identity and corporate identity. We talk naturally, nay instinctively, about “identifying with” friends, communities, sporting teams, suburbs, cities, countries, causes, and companies. In multiculturalism, there is the idea that more than one cultural identity may co-exist in the one person.

It seems clear to me that we switch identities unconsciously in daily life, when for example we wear a uniform to work, or our team’s colours to a footy game. And there is the “High School Reunion” effect when we are confronted with friends we haven’t seen for decades, and experience the jolt of reliving our own identities as they once were.

So human identity is malleable stuff. But when it comes to digital identity—that is, simply knowing and showing who we are online—we make a total mess of it. We have inherited from computer science a conceptual framework with arbitrary identity constructs, reasonable to technicians but at odds with the human condition. For example, technologists insist that “authentication” (knowing who someone is) has primacy over and must always precede “authorization” (telling what they are entitled to do). Yet in real life we often deal with people based on their authority alone; we rarely need to know who a pharmacist, a bank manager, an auditor or even our own boss “really” are. Many other standard security ideas are really foreign. Think about Single Sign On. It makes sense to use one password at work to access all corporate computer systems, but some have tried to extend SSO to the entire web, so that one general purpose identity might grant us access to social networks, merchants, banks and health services. Yet SSO is unprecedented in the real world; after all, it would be like asking your employer to re-key the front door of the office to match your house key.

Meanwhile, in spite of all the earnest theoretical work on identity and “trust”, cyber crime and privacy breaches only get worse, and none of the “Identity 2.0” initiatives have succeeded in serious business settings like e-government, banking and e-health.

It seems vital that we take stock and review the premises of federated identity if better progress is to be made. We would do well to use plain language for describing identity online, for it might breed plain thinking. I don’t propose any new definitions—heaven forbid! Instead, we could use simpler forms of words in their everyday sense.

So what is identity? Simply, my identity is how I am known in a circle I move in. I am a member of many different circles: of colleagues, customers, users, members, professionals, friends and relatives. When we look at identity this way, it illuminates complexities like “interoperability”. There is a common intuition that digital identities can be made to interoperate, but this is shown to be misplaced by the fact that belonging to one circle doesn’t automatically mean you belong to any others.

Age-old societal conventions and behaviours around identity serve to protect our privacy. To preserve privacy online, we should work to retain as many of our identity concepts as possible, when we move from real world to digital.
Stephen Wilson
Lockstep Group

Stephen runs the Lockstep Group, which provides independent advice and analysis in privacy and cyber security, and researches and develops novel privacy enhancing technologies. He blogs at http://www.lockstep.com.au/blog and tweets as @steve_lockstep.

Privacy Impact Assessments: the who, what, why, how and when of PIAs

What is a PIA – and why should we do one?

Privacy Impact Assessments (PIAs) are a way of measuring the privacy impacts posed by legislative, policy or technological initiatives.

PIAs are usually undertaken as part of a sound project management strategy, to assess whether it is safe to proceed to the implementation phase of a significant legislative, policy or technological initiative. A failure to properly embed appropriate privacy protection measures may result in a breach of privacy laws, or prohibitive costs in ‘retro-fitting’ a system to ensure legal compliance or address community concerns about privacy.

‘Privacy’ in this sense can encompass personal information privacy, communications privacy, behavioural privacy and territorial privacy. Privacy impacts arising from an initiative may be negative (privacy-invasive) and/or positive (privacy-enhancing).

A PIA report should do more than just assess an initiative’s likely compliance with statutory privacy principles. It should also assess the privacy control environment – the policies, procedures and structures which affect accountability for privacy compliance - and wider community concerns and perceptions about the initiative.

A PIA report should describe and de-mystify the initiative, identify and analyse the privacy implications, and make recommendations for minimising privacy intrusion, and maximising privacy protection – while ensuring the initiative’s objectives are met.

How is a PIA of benefit?

A PIA report should provide:

- greater clarity as to the privacy obligations applying to organisations involved in or affected by the initiative
- identification of risk areas for the proposal in relation to both privacy compliance and community expectations
- suggested strategies to address those risks – by minimising privacy intrusions, and maximising privacy protections, and
- recommendations for further action to ensure privacy protection is incorporated as necessary into legislation, policies and procedures, and governance arrangements.

The PIA report should therefore be a valuable resource for the project team, to assist in finalising the design of the initiative.
The PIA can also be used to further inform and educate those involved in, or affected by, the initiative as it is implemented – for example, in the design of guidelines, education materials, staff training, system design and program evaluation. PIAs can also perform an important role in any community or stakeholder consultation.

**How does a PIA work?**

Identifying privacy impacts and risks involves an examination of how the proposal will “affect the choices individuals have regarding how information about them is handled, the potential degree of intrusiveness into the private lives of individuals, compliance with privacy law, and how the project fits into community expectations”.

An initiative is therefore assessed at each point in the life cycle of the personal information likely to be handled by the organisation/s involved. The assessment is made with respect to both compliance with privacy laws, and in terms of community expectations.

The Australian Privacy Commissioner has set out a number of considerations when assessing privacy risks:

- **Balancing interests:** provide an appropriate balance between the goals of the project, the interests of the agency and those of individuals who may be affected.
- **Minimum standards:** ensure a minimum standard of privacy protection for individuals affected by the project. The IPPs may not apply in all circumstances or situations, e.g. where the project involves the transfer of personal information across public or private sectors, or across jurisdictions.
- **Proportionality:** ensure that any privacy infringement is proportional to, or appropriately balanced with, any benefits gained from the infringement.
- **Transparency and accountability:** ensure that measures affecting privacy are transparent, through adequate notice and privacy policies, and that agencies are accountable for how they handle personal information, including through effective complaint-handling, audit and oversight.
- **Flexibility:** be sufficiently flexible to take account of the diversity of individuals affected by the project.
- **Deliverable promises:** ensure that privacy protections are included in law or other binding obligations, and build them in to new technology.
- **Privacy Enhancing Technology:** consider using privacy enhancing technologies.
- **Review after implementation:** Consider how the project’s privacy impacts will be assessed or audited.

**What should the PIA achieve?**

The resulting PIA report should identify avoidable risks, and suggest measures to eliminate or lessen those risks to an appropriate level.

Recommendations should however seek to achieve a balance - between the interests of the organisation proposing the initiative, and the people affected by it. Those recommendations which are most strongly urged should therefore be those which can significantly improve privacy protection for the people affected, without significantly impacting on the achievements of the proposal’s objectives.

---

Who can conduct a PIA?

PIAs can be conducted by external consultants, or in-house. External consultants bring expertise, independence and a ‘fresh eye’ to the project, and may be able to work faster than an in-house team with competing priorities. In-house PIAs may nonetheless be suitable, especially where the budget is tight.

When and how should we start?

As soon as possible. The earlier privacy risks are identified, the easier it will be to build solutions into the design of the initiative.

Where else can we find information?

The Victorian and Australian Privacy Commissioners have each published guides to assist agencies wanting to conduct an in-house PIA, which can be adapted to suit other jurisdictions’ laws as well.

Anna Johnston
iappANZ Board

Anna is the Director of Salinger Privacy. She has conducted numerous PIAs for government clients, and in 2009 wrote the Privacy Impact Assessments Guide on behalf of the Victorian Privacy Commissioner. See: www.salingerprivacy.com.au.

Along with Queensland’s Privacy Commissioner, Anna is presenting on the topic of PIAs at a Privacy Awareness Week Event being held in Brisbane on 3 May 2011.

Privacy After Hours & other events

The iappANZ Board continues to work alongside members to ensure the regular delivery of timely, relevant and engaging Privacy After Hours and other events across the ANZ region. These events help our association to grow and, perhaps more importantly, allow the great privacy professionals in our region to connect with each other, share knowledge and explore opportunities for professional growth.

Our hub cities (that is, cities with the greatest concentration of iappANZ members) are Sydney, Melbourne and Brisbane… however we are keen to promote Privacy After Hours and other events in all our member locations, and would be thrilled to work with you to this end.

If you are keen to host an event in your city (whether you have a fully formed plan, or are simply at the brainstorming stage) please let us know by emailing admin@iappANZ.org.
2011 PRIVACY AWARENESS WEEK (PAW)

29 April 2011 – SYDNEY - Lunch Seminar

Last Friday saw the pre-PAW kick-off event with Google and the Federal Privacy Commissioner at a lunch seminar attended by more than 60 people. Alma Whitten, the Privacy Lead at Google gave an in depth presentation on search result and cookie privacy, as well as general privacy initiatives at Google, including its government transparency report. This enables users to find the number of requests that it receives from government agencies around the world, requesting disclosure of personal information and take down content notices. More information is available at: http://www.google.com/transparencyreport/governmentrequests/

A similar event will be run in Auckland with the New Zealand Privacy Commissioner and Google this week, in conjunction with NZ-based PAW events.

3 May 2011 – BRISBANE - Seminar

On 3 May, as part of PAW events in Queensland, a number of our members and other interested privacy professionals will be attending An Introduction to “the what, why, when, who and how of Privacy Impact Assessments”. Those attending will learn about how to use Privacy Impact Assessments as an important risk management tool to avert privacy disasters in programs, projects and initiatives.

Speaking at this event are two highly regarded privacy professionals: Linda Matthews - Queensland’s Privacy Commissioner, and Anna Johnston - Director of Salinger Privacy.

A wrap up of this and other PAW events will feature in next month’s Member Bulletin.
What’s new in privacy?

iappANZ opens new role: GENERAL MANAGER

The Board of Directors is seeking to recruit a General Manager (p/t) to grow the iappANZ. Significant opportunities exist to expand the role as the association thrives. This is an excellent leadership & entrepreneurial opportunity with flexible working conditions and location. The role reports to the Board of Directors, through the President.

The key responsibilities of this role include:

- manage a profitable annual conference and sponsors
- grow membership base and raise sponsorship dollars
- manage member facing benefits, such as seminars and other events that may be run (expect approximately 9 per year in major capital cities)
- liaise with professional association management service (PAMS) in relation to member renewals and other functions managed by PAMS
- communicate and develop marketing materials to promote the association
- update association’s website as directed
- manage training/certification

Essential experience required for this role includes:

- Ability to professionally represent the iappANZ and match its needs to member interests
- Event & relationship management skills and experience
- Excellent written and verbal communication skills
- Ability to work autonomously and report to a Board of Directors
- Self-motivated, enthusiastic, reliable and highly organised
- Some knowledge of privacy or the privacy industry desirable

The ideal person for this role will be entrepreneurial and be a champion for customer service. You need to be comfortable reporting to a Board of Directors, be an approachable individual and have a commitment to continuous improvement and the ability to build and maintain rapport with members and stakeholders.

Please send your resume to the Vice-President of the Association at annelies@iappanz.org or call 02 9514 4930.

Don’t be shy… certify!

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 most 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 focusses 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.

FIND OUT MORE at www.iappANZ.org

Editor’s Note

In March, the Member Bulletin included a snapshot in this section entitled “Online Behavioural Advertising: big push for best practice”. In focus was the Australian Digital Advertising Alliance (ADAA)’s 21 March 2011 release of the Australian Best Practice Guideline for Online Behavioural Advertising and an accompanying consumer education website, www.youronlinechoices.com.au.

Without doubt, the matter of online behavioural advertising (OBA) is controversial. Skilled privacy professionals inform both sides of the debate (whether in an ‘enabling OBA’ or ‘critiquing OBA’ context), caught in the privacy version of a Mexican Standoff which is often played out (depending on the context) in the media, privacy and consumer advocacy circles and academia. On the one side there are committed, and certainly pioneering for the ANZ region, efforts to establish best privacy practice in OBA (such as the ADAA’s Guideline). On the other side, there are concerns about the extent to which marketing should delve into the realm of online behaviours at all and whether guidelines or codes of practice alone offer sufficient privacy protections. For example, in a recent article, entitled “Unauthorised online tracking a growing concern”. The Australian (DOUBLECLICK: David Frith) questioned whether the ADAA’s Guideline is truly adequate from a privacy perspective.

Indeed, depending on where one sits (e.g. online user vs. company with online presence), there is a fairly blurry line between the perceived anonymity of a person’s activities while online (and the right to privacy in that context) and the growing perception and use of personal information as a commodity for companies that offer services, information and products online.
In my Polyanna naiveté, I often wonder if an alternative (or perhaps the logical “next step”) to the ADAA’s Guideline is the establishment of an industry-wide “do not track” mechanism...? By establishing such a mechanism in a manner analogous to the national Do Not Call Register established by the Australian Communications and Media Authority, I wonder if the needs of the community, companies and various privacy professionals weighing in on the debate could be met?

That said, I don’t actually have a particular camp preference when it comes to OBA (Is it good? Is it bad?) – largely because I am not yet informed enough about either position to have a view worth presenting. I do, however, have a strong view about how diligently the privacy professionals in both camps have worked (and must continue to work) to find a practical, reasonable and privacy savvy solution to the Standoff. I also have the view that becoming bogged down in discussions about whether to support (yay!) or decry (boo!) OBA is not helpful to privacy professionals on either side of the debate. After all, both sides would agree that failing to provide strong online privacy protection (and a degree of user choice in the process) is not an option.

~ NS