In this Issue

Member Bulletin
Foreword - John Pane - Vice President iappANZ
Purposeful and pragmatic patient privacy. Polarising... or possible?

Be There or Be Square
From the Queensland Treasury trenches - Practical perspective on audits, compliance planning & regular PIAs

Privacy After Hours

What's New in Privacy?
Privacy Awareness Week 2010 - 2-8 May
Privacy Awareness Week 2010 - a jurisdictional snapshot
Privacy Professionals - there is help out there!
iappANZ privacy certification exam - April 2010
e-VALUE-ating Privacy - a golden opportunity for ANZ businesses
ANZ DashBoard Digest - going WEEKLY!

Contact us

Member Bulletin

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:

It has been a busy and interesting month in the world of the privacy professional. There has been controversy, government policy and legal developments with important implications for
us both as privacy pros and as citizens. And, serving as an exclamation point, the IAPP just turned 10!

A most interesting debate in the press has been surrounding the proposed introduction of a national health identifier. Privacy advocates have made some compelling arguments not only about the inherent risks, but also the speed at which the proposed Bill is being driven.

In addition to the national health identifier issue, a student identifier is being proposed by the Commonwealth government. Newsworthy? You bet.

There has also been a huge buzz over Google Buzz! Google’s CEO Eric Schmidt was reported as saying:

“I would say that we did not understand how to communicate Google Buzz and its privacy. There was a lot of confusion when it came out on Tuesday, and people thought that somehow we were publishing their email addresses and private information, which was not true. I think it was our fault that we did not communicate that fact very well, but the important thing is that no really bad stuff happens in the sense that nobody’s personal information was disclose”.

(Read more here)

Finally, consider this excerpt of an article written by security expert Bruce Schneier:

Technology is not the problem because technology is neutral. Policies about how technology can and cannot be used determine privacy, and the balance is changing away from privacy. “We can accept the new balance or set the balance”.

(The complete article is here)

This last article really got me thinking. Does it mean we, as a professional group, need to think and act more like privacy advocates? Yes, I think we do sometimes. Does it mean by doing so we are doing our employers a disservice or not acting in their interests? No, I don’t think that is the case. Why? Because privacy has a value and its major currency is TRUST.

Trust is one of the cornerstones of all relationships. If you can influence your organisation to think beyond “what is the minimum I must do to achieve legal compliance?” then you are on the path to becoming trustworthy. Organisations that behave predictably, fairly and with their clients’ and customers’ interests at front of mind are, more often than not, developing enduring trust-based relationships.

John Pane

Vice President
iappANZ Board

Purposeful and pragmatic patient privacy. Polarising… or possible?
Why is it that privacy is so polarising? For a fundamental human right that we treasure and guard instinctively from the moment we get home every evening, privacy is remarkably dispensable in public discourse and policy.

Technologists have an unfortunate tendency to belittle privacy in words and in deeds. Scott McNally’s quip that “you have no privacy, get over it” usually tops the list of gaffs, yet a more insidious viewpoint was actually revealed by the then-chair of IBM, Lou Gerstner, who in 2000 boldly asserted that “privacy is not a technology issue”.

Perhaps Mr Gerstner meant no harm, but his slogan is often read by technologists as a disclaimer that distances them from “business issues” like privacy. Positioning privacy apart like this gives licence to technologists to ignore their own role in privacy, and it exacerbates the difficulty we all face in building privacy into complex systems. I’m often asked by IT project managers “Why should we be doing a PIA now, when the design hasn’t been finalised?”, and my answer is “You should do a PIA early precisely because the design isn’t finalised!”

Make no mistake: anyone who asserts that “privacy is dead” is trying to sell you something, whether it’s a national security ideology, or a new pair of runners (as you leave the gym, walk by a shoe shop for the fifth time in a week, and your mobile phone announces the presence of an assumed exercise junkie!).

But cynicism isn’t confined to technologists and politicians. We’re in the midst of a late, rushed and therefore rather shallow debate over national health identifiers, where the privacy issues are being played down (or underestimated) by many e-health proponents.

I engaged with the recent Senate Community Affairs Committee inquiry into the Health Identifiers Act 2010, and I’ve reviewed the hearing transcripts. Many advocates of the proposed system maintain that the identifier is “just a number” and that no clinical information is associated with it. But I’m afraid that’s just not true. While I am generally in favour of health identifiers (and I’ve devoted years to the cause of e-health), I worry that the identifier proposal before us is indeed privacy invasive, that its implications are not thought through, and that there aren’t any alternative architectures on the table.

Without questioning the claim that the identifier is inherently non-clinical, privacy is treated in the legislation and in the debate as simply a governance issue. And those who are still digging deeper into privacy have been characterised as “hijackers” who are “defending privacy to the exclusion of all thought of benefits to the individual brought about by better healthcare” [Dr Mukesh Haikerwal, *Sydney Morning Herald*, 22 March 2010].

But privacy advocates aren’t uncaring about e-health, and they don’t see privacy and healthcare efficacy as competing with each other. So dig deeper we must.

The proposed Individual Health Identifier (IHI) is designed around a central directory which serves up patient identifiers to any provider authorised to request them. Neither the design nor the legislation contemplate any way for patients to carry and present their identifiers for themselves (and thus the draft law is oddly technology-
specific). So here’s the problem: each and every time a provider draws down an IHI (which will be routine the first time a patient presents at any clinic) this will be logged, creating an elaborate track of the individual’s journey through the health system. If the IHI service knows that I have attended an emergency room, then a drug & alcohol clinic and finally been admitted to a mental health facility, then a wealth of clinical information is actually being aggregated, personal information that would otherwise remain totally confidential between the providers and me.

The IHI service will also know when a rural patient visits a doctor in another town, a teenager sees a doctor who is not their family GP, or a patient seeks a second opinion. The sheer visibility of these intensely personal encounters will inhibit some from seeking the healthcare they desire. It doesn’t have to be this way.

All agree that privacy is a cornerstone of healthcare, so let’s not be drawn into the grim myth that efficacy and privacy are at odds, or that privacy is simply a governance issue that can be treated in isolation. Like e-health itself, privacy is complex and subtle, and deserves more collaboration, multiple disciplines, and optimism.

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.

___

Be There or Be Square

Foursquare, for the uninitiated, is one of the latest global social media crazes.

While small (1 million users as compared to Facebook’s over-400 million users), it’s a location-based social networking service that is sweeping across Asia and likely to land with a thud in Australia.

Whereas walking past a billboard and receiving a ‘text promotion’ from a retailer hasn’t caught on, the Foursquare phenomenon is a sure fire way for businesses to reach out to customers.

And it’s not the only location-based service changing the privacy landscape. An upcoming Location Based Service for Latin America Conference in May 2010 puts the number of location-based social networking services at one hundred and eight... and counting.
In the case of Foursquare, it encourages users to “check in” at locations using a mobile application iphone, smartphone and blackberry, or through the internet.

Foursquare has recently been integrated with other social media tools and you can choose to broadcast your location on Twitter and shortly on Facebook. Who knows, possibly, Blippy may join the bandwagon. Blippy lets you monitor (via store and credit cards) what your friends are buying – like we want to know each others’ spending habits and which stores we’re shopping at in real time!

If you don’t want to let your employer know you’ve taken a long lunch break, or tip off a friend that you’re in their neighborhood, you can limit your broadcast. This is an atypical approach in the social media arena. Let it all hang out or, if you want to be discreet, use some privacy tools to keep it all on the down low.

Perhaps, what sets Foursquare apart from other social networking phenomenon is its gaming aspect: Users of Foursquare score points for telling the application where they are at any given time – a process called “checking in” (as in, logging or signing in).

You “check in” from your favorite park, restaurant, bar or shopping centre. There’s even a leader board so you can compete with your friends to see who has scored the most points. If you’ve frequented a place more than anyone else you earn the title of Mayor. This will give you access to even greater discounts, freebies and not to mention a virtual empire to rule.

So what does Foursquare mean for privacy?

First, friends/ acquaintances/ contacts will be able to keep closer tabs on what others are doing at any point in time.

Second, relatively fun and harmless information can be joined up with other public information and reveal patterns of behavior. One site, titled pleaserobme.com, is dedicated to raising awareness about the potential for Foursquare-esque ‘over-sharing’ and the intended and unintended consequences for privacy and personal safety.

Third, it’s redefining traditional loyalty and market research approaches. In the past, your FlyBuys card may have told a retailer how often and how much you paid for a certain product. Foursquare now tells a retailer, and your followers, how you feel about a product. For example, if you think a cafe serves the best latte in town, you can give visitors a heads up by leaving them a tip such as “Billie is the best barista in town”. The next time a user “checks in” at the same location, he or she will get a pop-up of the same tip.

Fourth, it’s ‘monetizing’ social media. Already hundreds of retailers have jumped on board to offer freebies. The problem, as Daniel Lyons rightly points out in his article Google’s Orwell Moment, “buying things with your privacy means you really don’t know how much you’re paying. With money, five bucks is five bucks”.


So what is the value of your list of friends, your opinions? Is it worth a few freebies? Finally, it provides incentives for over-visiting a location or ‘over-sharing’ information about personal likes or dislikes. It plays on our desire to stand out from the crowd. If you’ve been to a place more than anyone else, you’ll be crowned the Mayor of that location. Many food and beverage outlets dish out privileges and freebies to Mayors. Perhaps it’s the best seat in the house, never having to wait in a queue for a free smoothie. Every one of your friends will know you’re the top dog. So much for going online to ‘get lost in the crowd’.

If social media trends continue as forecasted, Foursquare is likely to stick around for a while.

Given, its privacy implications, privacy professionals should place a call to their organisation’s marketing and communications area to ask if Foursquare is on their list of preferred sites. At the same time, it would be a worthwhile exercise to take stock of how many other social networking sites your organisation is involved with, and what privacy safeguards, if any, are in place.

_Brent Carey_

iappANZ Board

^ Index

---

**From the Queensland Treasury trenches – a practical perspective on audits, compliance planning and regular PIAs**

At the top of my list for lessons learned in the trenches is the importance of conducting a privacy assessment or ‘audit’ in agencies. This cannot be overstated. From a compliance point of view, assessing the actual state of privacy compliance against statutory requirements and best practice helps agencies meet their obligations - under legislation, and also in terms of regulatory and public perception (e.g. engendering trust from the community we serve). Such assessments help agencies avoid potentially high financial risks and the investigation of individual staff that can result from non-compliance.

Next on my list is that agencies, all agencies, need to develop some form of ongoing Privacy Compliance Plan. If this is not done then all the hard work in carrying out the original assessment (or ‘audit’) will be lost over time (e.g. when the responsible officer leaves the privacy compliance role and moves to Aruba to retire) - resulting in increased risks for the agency.

Lastly, I believe that Privacy Impact Assessments (PIAs) are extremely valuable tools and should be conducted as a matter of routine agency business. Past experience has shown that if a PIA is not carried out, and should have
been, the results can and will cause project blow-outs and a great deal of unnecessary work to retrofit privacy for internal or whole of government initiatives involving personal information.

**Gerry Cottle**
iappANZ Board

**Gerry Cottle** is the Manager Administrative Review for Queensland Treasury where he has held this position for 8 years. Prior to this Gerry worked for the Queensland Department of Justice and Attorney-General (JAG). During his period in JAG Gerry was a keen advocate for privacy legislation and was involved in the original Whole of Government policy drive for Privacy as an administrative scheme in the Queensland Public Sector.

Gerry has produced a comprehensive manual for Queensland Treasury, entitled *Information Privacy Assessments - Processes and Procedures Manual*. The manual is an approach to privacy auditing and other processes in the context of Queensland’s Information Privacy Act 2009. Queensland Treasury has generously agreed to make this manual available for iappANZ Members to read. You can access this document in the coming days by visiting the members only section on our website.

---

**Privacy After Hours**

Details about April and May Privacy After Hours and other events - including those coinciding with Privacy Awareness Week (2-8 May 2010) - will be provided via email to members over the coming weeks.

For additional information about events happening in your city (including some great conference opportunities), please see the events page on our website.

---

**What's New in Privacy?**

*Privacy Awareness Week 2010 - 2-8 May*
Privacy Awareness Week (PAW), an annual initiative of the Asia Pacific Privacy Authorities (APPA) since 2007, has been confirmed for 2-8 May, 2010.

Public and private sector organisations across the Asia Pacific region will use the week to promote a variety of awareness raising events and activities relating to privacy rights and responsibilities.

Also, APPA will be launching an on-line ID theft prevention tool, with local launches of the same planned for the involved jurisdictions.

Keen to take part? The Privacy Awareness Week website contains information about PAW activities in your jurisdiction, and posts contact details for the various privacy regulators taking part.

^ Index

Privacy Awareness Week 2010 - a jurisdictional snapshot

Australia

Over PAW, the Federal Privacy Commissioner will encourage awareness under the mantra “Privacy: It’s in Your Hands” and will be releasing a wealth of information and best practice materials, including a corporate module of the Privacy Impact Assessment Guide. Check out the Privacy Awareness Week website and the April edition of the Member Bulletin for further details.

Victoria

Victoria’s theme for PAW is “Stop & Think: Don’t leave a privacy risk behind”. The full PAW program will soon be available on the Privacy Victoria website, with planned events for staff of Victorian public sector organisations to include regional presentations in Gippsland and Barwon South Western, a forum on IT Security and a screening of a privacy related film. April’s Member Bulletin will provide privacy professionals in Victoria with more information on PAW-happenings in their state.

NSW

This year, NSW’s focus will be “Keeping Your Identity Safe”. The April edition of the Member Bulletin will provide more details about the planned prgram of events, which to date includes a self-testing online identity “Toolkit” to be released by the NSW Privacy Commissioner.

Queensland
The Queensland Office of the Information Commissioner (OIC) is developing a number of resources in celebration of PAW. These will be profiled in the April issue of the Member Bulletin. If you are a privacy professional working in a Queensland agency covered by the Information Privacy Act 2009 and wish to find out more please contact the OIC on (07) 3005 7155.

**Northern Territory**

The Office of the Information Commissioner NT will soon be making details available about it’s PAW program, which is tipped to include promotional materials and an emailed privacy “tip of the day” for the duration of the week. Look for more information in next month’s Member Bulletin.

**New Zealand**

A Privacy Forum entitled ‘The Future of Privacy’ is planned for New Zealand during PAW, with details available on the NZ Privacy Commissioner’s website and in the April edition of the Member Bulletin. Included in the impressive speaking line-up is a plenary session delivered by Sir Geoffrey Palmer (President of the Law Commission, NZ) and an address by Canadian academic and privacy expert, Colin Bennett.

^ Index

**Privacy Professionals - there is help out there!**

A reminder to privacy professionals that there is a wealth of best practice and statutory compliance information available to you at the click of a mouse.

The Federal Privacy Commissioner has webpages dedicated to assisting privacy professionals find the specialised resources already available on their website.

- Please visit [http://www.privacy.gov.au/professionals](http://www.privacy.gov.au/professionals) to take advantage of these resources.
- If you are an Australian or ACT government privacy contact officer, additional information is available for you at [http://www.privacy.gov.au/government/pco](http://www.privacy.gov.au/government/pco).

The New Zealand Privacy Commissioner also provides helpful information to agency privacy officers, which can be found at: [http://www.privacy.org.nz/privacy-officers/](http://www.privacy.org.nz/privacy-officers/).

A resource that is profiled by the NZ Privacy Commissioner, but which is not directly affiliated with that office, is the Privacy Officers Round Table (PORT). Established in 2005, PORT is an informal, self-managing group of privacy
professionals working across New Zealand’s public and private sectors. Though informal, quarterly gatherings allow members to network, exchange ideas and discuss privacy issues relevant to their professions.

^ Index

iappANZ privacy certification exam - April 2010

It’s cram time! The first IAPP privacy certification event since the iappANZ annual conference in 2009 is now upon us.

Date: 29 April 2010
Time: 9am - 1pm
Location: Offices of Ernst & Young Melbourne CBD

This is a testing-only event, and is open for testing for all IAPP privacy certifications. This event is open to iappANZ members as well as members of the public who are seeking to certify.

Our best wishes to iappANZ members who are sitting this privacy certification exam!

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

^ Index

e-VALUE-ating Privacy - a golden opportunity for ANZ businesses

Are you looking for a way to calculate the ROI or value of privacy, or how to factor privacy in to a business case beyond the minimalist legal compliance approach?

The UK Information Commissioner’s Office (ICO) has released The Privacy Dividend (March 2010), a report that urges businesses to consider the financial benefits of developing strong data protection and privacy controls.

^ Index

ANZ Dashboard Digest - going WEEKLY!

The IAPP has decided to issue the ANZ Dashboard Digest on a weekly basis from Friday 2 April 2010!!
This excellent opportunity is due to plenty of media attention to privacy issues in our region, and continued interest in ANZ privacy news displayed by iappANZ members and privacy professionals worldwide.

If you wish to subscribe to the ANZ Dashboard Digest, you can visit the iappANZ website for more information or simply enter your email address as requested when you visit here.

Do you have interesting articles or information you would like to share with Privacy Professionals? Contact Nicole Stephensen (Contributing Editor-in-Chief, iappANZ Board) by emailing communications@iappANZ.org.
Please mark your email with attention to Nicole Stephensen - Member Bulletin

Email: admin@iappANZ.org
Web: www.iappANZ.org
Phone: +61 3 9895 4475
Fax: +61 3 9898 0249
Mail: PO Box 193, Surrey Hills Victoria Australia 3127