President’s letter

Dear Readers,

iappANZ is in its fifth year and 2013 is the year for increased member benefits and iappANZ brand awareness. We are doing this through more events, training, additional alliances and improved communication to you all. As I write, the Privacy Amendment (Privacy Alerts) Bill 2013 has been introduced into parliament and is having the second reading, so the June Bulletin will showcase Board Member Peter Leonard, who will give us a briefing on what that means for our organisations.

Now for our Association update, Privacy Awareness Week was the most successful ever, as Australian privacy Commissioner Timothy Pilgrim says in his contribution this month, which we expect to be the first of many.

iappANZ hosted two tables at the Sydney OAIC Breakfast, where we enjoyed insightful presentations by our members Gary Blair (CBA) and Stephen Wilson (Lockstep Consulting). The Brisbane lunchtime event at Corrs was a sell-out, and by serendipity, member James Kelaher was inspired by the same theme that Gary spoke of, ‘Information as an Asset worth protecting’; and this month I am sure you will find his fascinating piece “Rethinking Information and its Value” a great read.

The Brisbane launch of the ‘State of Privacy Awareness’ in Australian Organisations by the Global Chief Privacy Officer for McAfee, Michelle Dennedy has some astonishing figures reflecting significant opportunities for privacy professionals which you can read about in this edition. The Commissioner also showed that he will not be adopting a softly, softly approach as he responded to one question as to enforcement of the new regulations on the 13th March 2014, asking “What is wrong with the 12th?”
Training on the new legislation and implementation will be provided in respect of the new regime at no cost to members over the coming months. We are aware of the challenges and will be providing general and industry specific courses starting in July. Watch out for our news flashes.

iappANZ Privacy Summit on Monday 25 November 2013 will be our best. Held at the Westin Hotel, George St, Sydney at the Heritage GPO will feature international experts such as former UK ICO Richard Thomas CBE on high profile Data Breaches and Mikko Niva, Nokia’s CPO who will discuss privacy problem solving frameworks and engineering processes. And of course, there will be hands on workshops which you asked for with industry specific expert co-ordinators.

Finally, take a look at some of these first rate articles by this month’s contributors and you will see why our sister organisation iapp in the States is now offering the Bulletin to its global readers. I particularly enjoyed the profile section which features Rio Tinto’s CPO & Counsel Carolyn Lidgerwood – great practical and sartorial advice! I do hope you will all consider entering a piece in our inaugural writing competition with the winner to be announced at our Summit. Enjoy the read.

Warm regards

Emma Hossack  
President, iappANZ

---

**Vice President’s Foreword**

On Monday 29 April 2013, I attended the launch of Privacy Awareness Week 2013 at the Hilton Hotel. The annual event hosted by the Office of the Australian Information Commissioner (OAIC) is visibly getting bigger and bigger each year as well gaining momentum across diverse sectors. Arguably this year’s was the most significant given that privacy law reforms passed last year will commence in less than 12 months time. In fact, Privacy Commissioner Timothy Pilgrim stated: ‘This is one of the most significant Privacy Awareness Weeks we’ve ever had ... During this week, I’m asking private sector organisations and agencies to consider where they are at with preparations for the new laws. Early preparation is definitely going to be key for compliance with the new requirements ...’

Mr Pilgrim also announced that over 150 partners from the private sector, government agencies, and the not-for-profit sector joined the OAIC during Privacy Awareness Week to promote the protection of privacy in Australia. This is very encouraging given the pressure the OAIC is under to communicate and support information on privacy law reforms this year. So, we won’t be seeing a nationwide consumer campaign on privacy awareness and action. What we will be seeing (and have seen) is the OAIC investing its limited resources to educating organisations on compliance requirements and practical resources to expedite communication to relevant stakeholders. iappANZ will be striving to compliment the OAIC’s work in the pivotal lead up to the reforms and as our President Emma Hossack notes, the Board’s energies will be focused on providing practical compliance training for our members with attention to some key sectors affected by the reforms.

The OAIC’s new Guide to information security, ‘reasonable steps’ to protect personal information was launched at the event. A timely launch as news of LivingSocial’s data hacking made breaking news all over the world that week! Mr Pilgrim made some notable comments on privacy by design (i.e. building privacy into processes, systems, products and initiatives at the engineering stage) which is a concept referred to in the Guide. In particular, Pilgrim observed that there has been some recent discussion on obtaining insurances for data breaches by enterprises. Pilgrim’s view is that implementing privacy thinking into the product construction stage may be the best insurance an innovative organisation can invest in! Something like reinforcing cement when building a new house, the message - get it done and get it done early to save your organisation becoming a statistic at next year’s OAIC breakfast! Board Director, Kate Reynolds provides a useful snapshot of the Guide and implementation in this bulletin.

Also in this bulletin you will find thoughtful pieces by Michael Burnett on the regulation of the use of de-identified credit reporting information for the purpose of conducting research in the context of broader privacy law issues. Christine Cowper writes on the evolution of privacy management maturity models for reporting on the status of an entity’s privacy program and initiatives in this region.

Many thanks to our contributors and if you would like to provide any insights into any of the topics covered this month as a letter to the editor, please send them in and continue the conversation.

Kind regards

Anna Kuperman  
Vice President, iappANZ

---

**OAIC News By Timothy Pilgrim Australian Privacy Commissioner**

On 15 May 2013 I had the honour of delivering the keynote address at the opening of the Personal Data Protection Commission of Singapore. The audience consisted of around 400 representatives...
of businesses based in Singapore. This was a great opportunity to talk about the importance of ‘privacy by design’ and data security, and to share a global perspective on data protection.

With their recent enactment of personal data protection law and the establishment of the PDPC, Singapore joins an important global community of data protection regulators. Having a connected group of data protection regulators across the world is essential given the global nature of information flows and is now something I do on a daily basis.

These laws are important for the people of Singapore and the global community. Given the large number of multinational organisations located in Singapore and the massive amounts of personal information that many of them handle, it is pleasing to know that the protection of personal information will be further protected through law and that there is a regulator ensuring that this is the case.

In other news, the Office of the Australian Privacy Commissioner (OAIC) celebrated Privacy Awareness Week (PAW) 2013 from 28 April to 4 May with a record number of 158 PAW partners in Australia. It was encouraging to see so many agencies and organisations demonstrate their commitment to privacy.

I would like to thank everyone involved for their support this year. Our PAW 2013 partners demonstrated their commitment to privacy by running computer based learning programs, client sessions and staff briefings; as well as attending OAIC events, and promoting PAW materials on their websites and intranets.

The OAIC released a number of privacy guidance materials during the Week that are now available on our website, including the Guide to Information Security: ‘Reasonable steps’ to protect personal information and a single page summary of the guide. These resources provide guidance on the ‘reasonable steps’ entities are required to take under the Privacy Act to protect personal information.

We also produced other materials to assist businesses prepare for the reforms, such as the Australian Privacy Principle (APP) Comparison Guide and an APP compliance checklists. These materials are available via the Privacy reforms page on the OAIC website.

Although PAW 2013 has finished, we are encouraging businesses to keep preparing for the changes to Australian privacy laws that will commence in just nine months. Further information about how your organisation can prepare for the reforms is available on the OAIC website (www.oaic.gov.au). Join us on Twitter or Facebook to receive the latest privacy related updates, or subscribe to OAICnet on the OAIC website.

You may have also seen media coverage about the OAIC’s participation in an ‘internet sweep’. Nineteen privacy enforcement authorities from around the globe, including Germany, United Kingdom and the United States, took part in the first International Internet Privacy Sweep, an initiative of the Global Privacy Enforcement Network (GPEN). The sweep theme was ‘Privacy Practice Transparency’.

The OAIC examined the 50 most visited websites used by Australians to assess the accessibility, readability and content of their privacy policies. The privacy policies were also considered to see how they would rate against new transparency requirements due to commence in March 2014, in particular Australian Privacy Principle (APP) 1 — Open and transparent management of personal information.

The results of the Australian Sweep will be released later this year.

**Timothy Pilgrim**
Australian Privacy Commissioner

---

**iappANZ Profile - Carolyn Lidgerwood, Rio Tinto’s Global Privacy Counsel**

**What did you want to be when you grew up?**
I knew, I wanted to get out of Tungamah but in retrospect I’m not sure why. Tungamah is a terrific place (http://en.wikipedia.org/wiki/Tungamah).

**What advice would you give to the young privacy professional?**

a) Do some regulatory law and learn how to read a statute. Know what’s in section 15AA of the Acts Interpretation Act 1901. I’m serious.

b) Surround yourself with ‘early adopter techie types’ so that you can learn about new technology by osmosis. Even if this means you will also learn much about Dr Who.

c) Work in or with companies so you learn how to provide practical privacy advice that works.

d) Use the IAPP books on European laws, Canadian laws and US laws if you’re presented with a global privacy compliance question. I’m not just saying that to make our Madame President of IAPP ANZ happy. The IAPP books are useful sources.

e) Don’t wear your cardigan all the time. (That last bit is of course a joke. We privacy folk love a nice cardigan. As illustrated at the recent IAPP global privacy summit).

**Footy or Rugby?**
Cricket, always cricket. I just wish the West Indies could get back to where they were in the late 1970s/early 1980s – they were magnificent to watch.
Privacy - should we be over it?
I recently saw an article that responded to that famous quote ("You have zero privacy anyway. Get over it") with this headline - "People still value privacy. Get over it." I liked that. Call me old fashioned, but if your personal data is used in ways you don’t expect or haven’t consented to, it can be a rude shock.

Does Australia need a legislated right to privacy or are we doing ok?
My personal view is that an additional statutory cause of action for invasion of privacy would not result in a net benefit to the Australian community. I’m no fan of legislative intervention in the absence of a clearly demonstrated need, and the issues here are vexed (particularly with respect to freedom of speech). Personally, I think this is an area that should be left to the common law.

Favourite food?
It is hard to beat a sponge cake cooked with farm eggs from a Country Women’s Association recipe, and served with real cream and passionfruit icing. Although if I had to name the food of one country to accompany me to a desert island, it would have to be Singapore.

Should the media be exempt from the Privacy Act?
My personal view is yes, definitely yes. While the drafting of the current journalism exemption is not perfect, an exemption is needed because freedom of speech (particularly in the reporting of news and current affairs) is so important. Declaration of interest: I have worked as a broadcasting lawyer for most of my working life.

Anything private you would like to reveal (within reason of course!)?
Coming from six generations of Australian farmers, a visit to the sheep pavilion at the Show is my idea of a good time. It’s not rocket science, but I do know the difference between a Corriedale, a Border Leicester, a Lincoln, a White Dorper, a Suffolk and a Texel - but Dorsets are my favourites.

Carolyn Lidgerwood is Rio Tinto’s global privacy counsel, and has recently moved from her high rise office in Collins street to the gum tree vistas of Bundoora. Prior to joining Rio Tinto 2 years ago, Carolyn was General Counsel and Company Secretary at Southern Cross Media (long before it acquired 2DAY FM and its prank call). Before then Carolyn worked in broadcasting law and privacy law at Gilbert + Tobin for more than 10 years, after formative years with the Australian Broadcasting Authority, Arthur Robinson & Hedderwicks (now Allen) and Chief Justice Black of the Federal Court. She isn’t really as old as she sounds.

The Credit Reporting Scheme of Regulation of De-Identified Credit Reporting Information: A Case of Regulatory Overreach By Michael Burnett Lawyer At Gilbert + Tobin Lawyers

One of the key reforms implemented by the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Amendment Act) is a comprehensive overhaul of the credit reporting scheme in Part IIIA of the Privacy Act 1988 (Cth) (the Act). Generally, new Part IIIA is a vast improvement on the current scheme, aspects of which the Government has described as ‘overly complicated and confusing’.

Significantly, new Part IIIA implements a ‘more comprehensive’ credit reporting system in Australia. In credit reporting-speak, this means that credit reporting bodies and credit providers will have access to a broader range of personal information for credit reporting purposes. This includes borrower’s ‘repayment history information’, the use and disclosure of which is not currently permitted under the Act.
The policy objective of the new scheme is to balance the privacy interests of the individual against the interest, in this case, of the credit reporting industry in accessing sufficient personal information to make informed assessments as to individuals' consumer credit risk. To this end, the Government has sought to balance the industry's access to a broader range of personal information with relatively prescriptive restrictions as to the use of that information.

Whether the Government has been successful in striking an appropriate balance is yet to be seen and will no doubt continue to be the subject of some debate. One area, however, in which there appears to be some regulatory overreach, is in the regulation of the use and disclosure of de-identified credit reporting information.

Traditionally, privacy law has not regulated de-personalised information, other than to require the permanent de-identification, or destruction, of personal information if it is no longer needed for a lawful purpose. The terms of section 20M of new Part IIIA, however, represent a clear departure from this approach. The case for such a departure is far from clear and warrants closer scrutiny.

Section 20M prohibits a credit reporting body from using or disclosing de-identified credit reporting information. A single exception to this rule applies if the use or disclosure is for the purpose of conducting research and the credit reporting body complies with legislative rules made by the Commissioner.

Significantly, the provision goes on to empower the Commissioner to make prescriptive legislative rules about the kinds of de-identified information that may or may not be used or disclosed for research purposes, whether or not the research relates to credit, the purposes of conducting the research, consultation about the research, and how the research is to be conducted.

According to the Explanatory Memorandum, the purpose of this provision is to address concerns about the effectiveness of methods used to de-identify personal information and the risks of that information being re-linked to individuals (although no information is given as to the nature of these concerns or risks).

If this is indeed the case, then arguably, the measures adopted to address such mischief are somewhat overwrought. Rather than imposing a blanket ban against the use and disclosure of de-identified information, more measured and less intrusive solutions could be adopted to deal with these risks, such as:

- empowering the Commissioner to develop guidelines as to appropriate de-identification methods; and/or
- imposing a general prohibition against the re-identification of credit reporting information.

Further concerns arise as to the appropriateness of empowering the Commissioner to make binding rules regarding credit-related research. The Commissioner's unreasonably broad power to, among other things, determine the purposes for which credit-related research may be conducted threatens to restrict the range of research undertaken into the use and provision of credit in Australia. Arguably, a less-intrusive solution would be to task an industry-led committee to develop and provide guidance as to appropriate research purposes and methods involving de-identified credit reporting information.

One area in which there is possibly a case for the regulation of de-identified information is in health research. Here, the use and disclosure of de-identified health information is an issue of some concern, particularly in relation to research involving small data sets and/or rare or unique conditions, which may, by their nature, lead to the identification of specific individuals. It is difficult, however, to accept that these same concerns would apply equally in the context of credit reporting research, which generally involves the use of large data sets and, arguably, less sensitive information.

Of course, a more fundamental issue arises as to the point at which de-identified information at risk of re-identification becomes information ‘about an individual who is reasonably identifiable’, and therefore falls within the scope of ‘personal information’. Given the associated compliance risks, these very practical issues will need to be further considered by credit reporting bodies prior to the de-identification process.

The case for new Part IIIA's incursion into the use of the de-identified personal information, including for the purposes of research and analysis, is not strong. The terms of section 20M are unnecessarily broad and go further than needed to deal with concerns around the re-identification of credit reporting information. In this age of 'Big Data' and anticipated privacy reform, the regulation of the use of de-identified information under privacy law will no doubt continue to be an issue of concern and debate.

Michael Burnett is a lawyer at Gilbert + Tobin Lawyers and regularly advises on domestic and foreign privacy law, including credit reporting regulation.

Footnotes:


Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 90-91.

This issue was the focus of considerable discussion during the course of the Senate Legal and Constitutional Affairs Committee’s Inquiry into the Privacy Amendment (Enhancing Privacy Protection) Bill 2012. See, for example, Commonwealth, Official Committee Hansard, Senate Legal and Constitutional Affairs Legislation Committee, 10 August 2012, 24-26.

Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth), ss 20M(3) and (4).

Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 144.
Privacy management maturity models (PMMMs) are not yet widely used in Australia or New Zealand but they potentially offer privacy practitioners an effective new tool. PMMMs provide a framework for the assessment and development of an organisation’s privacy capabilities; as such they complement compliance audits and Privacy Impact Assessments. Organisations’ privacy capability is becoming more important as government and business reputations are increasingly affected by data breaches and other loss of trust issues. Additionally, from March 2014, Australian organisations and agencies could be asked to demonstrate that they have taken reasonable steps to comply with the APPs by implementing relevant practices, procedures and systems.

Maturity models have been in use for over 15 years in other fields. Their origins are in software development and were triggered by the need to assess the capability of software providers. The concept has since been adapted and generalised and is now in wide use to assess the process capability maturity of organisations in a diverse range of areas including project management, risk management and information technology. Typically a maturity model will involve:

- **Maturity Levels**: A 5-level process maturity continuum - where the uppermost (5th) level is a notional ideal state where processes would be systematically managed by a combination of process optimisation and continuous process improvement.

- **Key Process Areas**: A Key Process Area identifies a cluster of related activities that, when performed together, achieve a set of key goals.

- **Goals**: The goals of a key process area summarize the states that must exist for that key process area to have been implemented in an effective and lasting way. The extent to which the goals have been accomplished is an indicator of how much capability the organisation has established at that maturity level. The goals signify the scope, boundaries, and intent of each key process area.

- **Common Features**: Common features include practices that implement and institutionalise a key process area. There are five types of common features: commitment to perform, ability to perform, activities performed, measurement and analysis, and verifying implementation.

- **Key Practices**: The key practices describe the elements of infrastructure and practice that contribute most effectively to the implementation and institutionalisation of the area.

Maturity models assist with, benchmarking across and within organisations, assessing processes and activities and process improvement. Benchmarking and process enforcement are critical to privacy management and demand for exploration of such tools is increasing. Work on specific privacy maturity models is limited so far in Australia and New Zealand. The American Institute of Certified Public Accountants, Inc. and Canadian Institute of Chartered Accountants (AICPA/CICA) have produced a detailed privacy maturity model. While privacy regulators have not produced maturity models as such, there is a range of relevant material including:

- A range of guidelines and case notes about the application of privacy principles from the Office of the Australian Information Commissioner and from the New Zealand Office of the Privacy Commissioner.

- Office of the Privacy Commissioner of Canada PIPEDA Self Assessment Tool.

- Office of the Privacy Commissioner of Canada Getting Accountability Right with a Privacy Management Program.

PMMMs differ from maturity models in other spheres in that the key process areas and goals will in part be defined by sets of privacy principles, often backed by law. Privacy principles are high-level, minimum standards and so compliance with the law as well as the appropriate maturity levels are affected by an organisation’s context, its approaches to risk assessment, governance and accountability and factors such as privacy culture. Privacy practitioners will also recognise that best privacy practice calls for more than simple compliance with the law, as compliance does not necessarily on its own ensure that customers trust the organisation.

The AICPA/CICA model reflects some of these points. It is based on a set of privacy principles – the voluntary ‘generally’ accepted privacy principles – and also addresses enabling factors such as governance and staff training. The model tends to focus on compliance but does include good practice elements including reference to Privacy by Design.

For practitioners who might now be saying ‘aha’ and reaching for a PMMM, there are a few more things to think about. Obviously, the model needs to reflect the law of the jurisdiction in which the organisation is operating. In Australia and New Zealand the privacy principles in the relevant privacy law would apply rather than the ‘generally accepted’ privacy principles. Also, as noted in the AICPA/CICA Privacy Maturity Model booklet ‘becoming privacy compliant is a journey’ and the right maturity target for an organisation depends on its circumstances and risk appetite. Organisations...
will also need to consider how the assessments will be undertaken. Issues include:

- The level of detail in the PMMM process areas, goals and the criteria for maturity levels, that will yield useful insights without being unwieldy to measure and interpret
- How to set benchmarks that are relevant to the organisation, and which would also be credible to a regulator if needed
- How to obtain a reasonably objective sense of current best practice within an industry or sector – privacy regulators, industry bodies and survey report will provide some insights and then it comes down to what organisations are willing to share
- The evidence that would be available to make an assessment and to decide on a move from one maturity level to the next
- Whether to undertake the assessment internally or to have an independent assessment.

While still a work in progress, PMMMs do seem to have the potential to assist privacy practitioners to diagnose areas for improvement in privacy capability and practice within their organisations. There are clearly some challenges in getting a tool that is fit for the particular industry or organisation but it seems likely to be a fruitful endeavour.

Christine Cowper is a member of iappANZ and Principal Consultant with Information Integrity Solutions Pty Ltd (IIS). IIS is a global privacy consultancy whose services include privacy strategy development, privacy reviews and health checks and privacy impact assessments. IIS’ recent engagements include high-level privacy health checks, the development of 'how to manuals' and privacy capability assessments.

Christine can be contacted at: ccowper@iispartners.com

Footnotes:


This description is from http://en.wikipedia.org/wiki/Capability_Maturity_Model

Available at http://www.cica.ca/resources-and-member-benefits/privacy-resources-for-firms-and-organizations/docs/item48094.pdf

Available at http://www.oaic.gov.au


Available at https://www.priv.gc.ca/information/pub/ar-vr/pipeda_sa_tool_200807_e.asp

Available at http://www.priv.gc.ca/index_e.asp
Back in February this year, Stephen Wilson of Lockstep Consulting wrote an article for this bulletin about Privacy by Design. I wholeheartedly agree with his view of how engineers view privacy; ‘It’s not that they’re uninterested in privacy; rather, it’s rare for privacy objectives to be expressed in ways they can relate to. The only thing the IPPs, NPPs or APPs have to say about security is that it must be “reasonable” given the sensitivity of the Personal Information concerned.’

A few weeks ago, to coincide with Privacy Awareness week, the Office of the Australian Information Commissioner (OAIC) launched the Guide to Information Security, which helps organisations and agencies understand what may constitute ‘reasonable steps’ for protecting personal information. This gives us privacy professionals a fantastic opportunity to work with our security teams to help change these views by providing a tangible, practical approach.

The Guide essentially contains a security checklist which an organisation can work through. The vast majority of suggested controls should not be new concepts to your security teams and quite frankly, I would be concerned if they were. The OAIC’s recommendations cover pretty much the whole gambit of the security lifecycle; policy and planning, risk, operational, assurance and data breach management. I would recommend setting up a series of workshops with the relevant people in your organisation to map the current state of your security operations and associated controls with the OAIC’s Guide to identify any gaps before working with the business to mitigate any residual risk.

Even an organisation which feels pretty confident in their security posture cannot afford to become complacent. Increasingly sophisticated attack vectors, which have emerged over the last few years, mean that if a skilled, well resourced attacker really wants to penetrate an organisation, they can and will. The 2013 Verizon Data Breach Investigations Report even acknowledges that; ‘...a growing segment of the security community adopted an “assume you’re breached” mentality’. If you think your own organisation or agency hasn’t already fallen prey to some kind of malicious attack, I recommend you go and speak to someone in your security team immediately who should put you straight pretty quickly!

Organisations rarely make the news because of their great security and lack of breaches. Rather they are increasingly judged by the manner in which they respond to security incidents regardless of whether or not they took ‘reasonable steps’ to prevent such an occurrence.

High profile security breaches over the past few years have further demonstrated that even organisations which make security their business are not immune. In 2011 RSA Security publicly admitted that their two factor authentication product, SecureID, used by a huge amount of companies had been compromised resulting in them having to re-issue approximately 40 million tokens. The compromise was the result of a spear phishing attack which exploited an un-patched vulnerability in Abode Flash (full write up here). Even though RSA publicly and voluntarily admitted the breach at the time of the attack, they faced strong criticism from customers, the public and the media for not releasing what they perceived to be sufficient detail quickly enough.

Mandatory data breach notification laws, which exist in other parts of the world and are currently being considered in Australia have also helped to raise the profile and public expectation of an organisation’s response to such an event.

The OAIC refers to an organisation’s need to have a robust data breach response plan in its Guide to Information Security and has previously published Data Breach Notification: a Guide to Handling Personal Information Security Breaches. If you haven’t read this guide, do so. Socialise it with whomever in your organisation (whether internal or outsourced) is responsible for breach management. I would recommend setting up a series of workshops with the relevant people in your organisation to map the current state of your security operations and associated controls with the OAIC’s Guide to identify any gaps before working with the business to mitigate any residual risk.

Be as ready as you possibly can be. Your security team, whether in-house or outsourced needs to be one of your most valued assets in the organisation as they will likely be the ones who are notified or detect an incident initially and will be there throughout the lifecycle of handling a breach. Being proactive and engaging with them before you need to and providing them with a clear understanding of privacy requirements will only help you and your organisation in the long run.

**Suggested Action Points**

- Read the OAIC’s Guide to Information Security
- Meet with your security teams (whether in-house or outsourced) and map the suggested controls to your organisation’s current security framework to identify gaps that will require review
- Read the OAIC’s Data Breach Notification: a Guide to Handling Personal Information Security Breaches
- Review your incident response plans. Ensure that whoever in your organisation deals with security incidents and response is familiar with the guide and integrates it into existing plans where appropriately
- Test your response plans before they are required

**Kate Reynolds**

iappANZ Board Director

Kate has held a number of privacy and security related positions for large companies including Microsoft and Symantec both in Australia and the UK.

---

**Footnotes:**

---
As an accountant who has developed an interest in privacy as a result of my work in government and business, I am continually surprised by the different perspectives that I encounter as I commute between these four worlds.

**Information as an Asset**

Increasingly many businesses are founded on the way that they collect, compile and use data; in fact one will often see businesses claim that ‘information is the key to our business’. The same is true of government, where information about program registrants and recipients of services, collected from the public over many years, is fundamental to the fulfilling of their service delivery charter. In both these cases, information could be correctly – and often is – called an ‘asset’.

Certainly, if a business or government agency lost access to, or confidence in, its information holdings, it would struggle to function. In both cases, the cost and inefficiency of operating would be prohibitive. In the case of government there would be a huge tax-payer backlash if an agency was required to start from fresh and had to re-collect all the data that people have previously provided. In fact we often see this playing out when an agency is unable to access existing client data for privacy or data accuracy reasons and needs to initiate some kind of stand-alone registration process; new registration levels are low and clients and staff are frustrated by the processes involved. In other words the creation of ‘information’ can be costly for all parties concerned and there can be good reasons for getting as much (re)use out of it as possible.

**Information as a Liability**

However, from a legal and privacy perspective, many categories of information holdings should be kept to just the minimum necessary for functions to be performed and legislation to be complied with. Certainly any personal information held needs to be carefully secured, kept up to date and accounted for. (By the way, the same can often be said of commercial information.) In many respects, this kind of information is not so much an asset, but a potential liability; because of the potential risks and costs that are entailed for both the organisation holding the data and the other parties to whom the information relates, if a breach occurs.

So, it appears that information can be an asset for some and a liability for others, depending on the circumstances.

**Accounting for Information**

According to the accountants, whose standards are now part of the global fabric of government and business accountability, information – especially personal information – is generally neither an asset nor a liability. This is because, according to international accounting standards, an asset basically represents ‘future economic benefits, controlled by the entity as a result of past transactions or other events’. In other words something that has a calculable financial value and can be converted to cash now or in the future, such as raw materials, a licence, a machine, a building and so forth; something tangible.

That is why you don’t see in the annual financial statements of Medicare, Telstra, NAB, Wesfarmers, BHP-Billiton, Centrelink, Australia Post or the ATO the billions of dollars spent on collecting and compiling all of the data about customers, patients, families, employees, suppliers, hospitals, income, and so forth. This information is not tangible.

Interestingly, in the 1970’s about 80% of an organisation’s value was determined by the tangible assets it held. Nowadays, according to a study of the top 500 listed companies in the US, only 20% of those companies’ value is represented by tangible assets, the rest is made up of brand, knowledge and information – these are the assets that generally determine the value of a modern organisation. But, for the most part they are not on the ‘balance sheet’, even if the computers, whose only function is to collect, store and use the information, are.

Over many decades we have all been inculcated with the need to preserve assets: to guard against stock leakage or inventory theft, to sign for the custody of goods delivered and to participate in stocktakes. We implicitly understand these practices to be part of the organisational custodianship process. In more recent times, we have come to recognise the importance of ‘human capital’ and the associated processes of caring for and investing in people. I am sure you can see where this is heading.

But what about the other side of accounting: liabilities, where accountants record the value of ‘future sacrifices of economic benefits that an entity is required to make as a consequence of past transactions or events’. If an actual event has occurred (such as the delivery of goods which must be paid for by a certain date) or it is known that it will very probably occur (such as an obligation to pay a settlement in a commercial dispute), then a firm must record a liability for the amount concerned on its balance sheet.

But an organisation cannot create a liability on its balance sheet ‘just in case’ a possible adverse event might happen in the future. That would be equivalent to reaching into the pocket of the owner
or the tax payer to say, ‘look, I am a bit anxious that there is going to be a stuff up – so give me some money now, so that if it happens, I can use your money to buy my way out of trouble’. That is what good management practices, and sometimes insurance, are for – to mitigate risks.

So, while the potential for a privacy breach cannot be recorded as a liability on a firm’s balance sheet, if one does actually occur and compensation or fines must be paid, then it can be. Ah, the logic of accounting!

**Should we Change the Rules?**

Yes, I say! Because if people thought about information differently, they would do a better job of collecting, using, protecting, disclosing, and governing it.

Just imagine the attention that would be focussed on government information custodianship if the information held by agencies was valued and treated as an asset – imagine the size of the balance sheet numbers.

Imagine the impact on company management practices of information holdings that had to be classed as a potential liability, or which had to be written down due to impairment.

Just imagine if the market required that a data breach notification be accompanied by a financial statement, which set out the value of – and impacts on – an organisation’s information asset holdings. I think you would see some new management practices and priorities emerge very quickly.

Knowing the speed with which accounting standards change, it could be quite an ambitious undertaking to get the value of an organisation’s information recorded on its balance sheet – as either an asset or a liability. But I think it is high time that we started to debate this, because even the debate and awareness will produce a positive change in attitudes and greater awareness of good information and privacy practice.

Surely in this new information economy, we should be recognising that, implicitly we are already attaching value to information. At present those values are somewhat subjective, and in some cases only used when it is advantageous to do so. I guess if the traditional accounting profession does not take up this challenge, we may see a new discipline of ‘information accountants’ emerge and as experts in this field, maybe they will go after 80% of the fees!

**James Kelaher**  
**Director Smartnet**

James Kelaher is a director of the Smart Group, comprising Smartnet an advisory firm, which provides advice to government and private sector organisations, in Australia and overseas; Smart Ecosystems a company that specialises in the application of technology to the management and conservation of scarce resources, and a range of technology companies in which his group has interests, including high speed broadband communications, online payment and transaction security, and privacy protection solutions.

*He has previously held senior management roles in government, including as the deputy and managing director of the Health insurance Commission and the chief operating officer of the Australian Federal Police.*

*James holds a Bachelor’s degree in Arts/Commerce, an MBA, and is a Fellow of the Australian Society of Certified Public Accountants. He is also a member of the Australian Institute of Company Directors, the Risk Management Institute of Australia and the Institute of Privacy Professionals.*

---

**Win A Cash Prize : iappANZ's Writing Prize 2013**

iappANZ is very excited to announce the launch of a new [250 cash] writing prize for an article that is published in our monthly Bulletin between February and October 2013. Anyone can enter (you don’t have to be an iappANZ member), simply by writing and submitting an article between 500-1500 words that tells us something interesting, new and relevant about privacy. Opinions are most welcome but nothing too extreme.

All articles must be submitted by email, preferably in Word, to [kate.johnstone@suncorp.com.au](mailto:kate.johnstone@suncorp.com.au) or an iappANZ email by 20 October 2013. We will need the author's email address and contact number. You can submit as many articles as you like. Click here for more details.

The winner will be announced at our Privacy Summit on 25 November 2013 and their name and details will be published on our website. [We also hope to publish profile of the winner in our Bulletin].

So alert your network and get writing!

More details about the writing prize if you are interested:

• Our Editorial team, Kate Johnstone, Veronica Scott plus President Emma Hossack and Past President Malcolm Crompton, will decide on the winner whose article they judge to be the most interesting, original and relevant to our members.
Articles submitted and published in the February, March and April Bulletins will also be eligible for the prize – we don’t want anyone who has already made a valuable contribution to miss out.

Some people won’t be eligible for the prize (sorry!). They are: iappANZ board members, contractors and employees and their family members.

After the winner is announced we will notify them and arrange for the prize to be delivered to them if they are unlucky not to be at our Summit.

There will (sadly) be one prize only. Its value is AUS$250, so that’s pretty good really.

We may need to verify the winner’s identity so we don’t give the prize to the wrong person.

If the prize is not claimed for any reason (and we hope this won’t happen) the author of the runner-up article as judged by the Editorial team will receive the prize.

To make sure things go smoothly and fairly (and we are sure they will) we just have to say that our decision in relation to any aspect of the award of the prize, including the content and publication of submitted articles, is final and binding and not up for discussion.

---

**State of Privacy Awareness in Australian Organizations - April 2013 Research**

Please [click here](#) to download the Research Data Sheet.

### Australian Organisations at Risk

- Over one third (34 per cent) of respondents responsible for managing customers’ personal information in organisations of over 25 employees don’t believe Personally Identifiable Information is well handled.

- 36 per cent of respondents save data to fileshare services in the cloud (i.e. Dropbox or YouSendIt). 38 per cent either don’t encrypt, or know if they encrypt the data when doing this.

- 38 per cent haven’t ever received training in the management and storage of sensitive data.

- One-fifth (20 per cent) will use a webmail client, such as Gmail or Hotmail, to share information with colleagues and third party suppliers. Of those who have experienced a data breach, the number of webmail users climbs to 36 per cent.

- The main ways of sharing information with colleagues and third party suppliers are by work email (60 per cent), company portal (46 per cent) and a shared server (43 per cent). There is lower but widespread use of secure file transfer (29 per cent), shared passwords (22 per cent), cloud fileshare services, e.g. Dropbox and YouSendIt (21 per cent), portable storage devices (20 per cent) and webmail (20 per cent).

- Of the sixty-two per cent (62 per cent) who have received sensitive data management training, over half (52 per cent) have received training in the last year while nineteen per cent (19 per cent) receive ‘regular frequent updates’.

- The two largest repercussions feared by companies with a data breach were reputation damage and loss of customer trust (both at 68 per cent). Smaller but still noteworthy issues were financial penalties (50 per cent) and the cost of remediation or repair (37 per cent).

- Government organisations were less likely to know whether they have suffered a data breach than corporate businesses. Almost twice as many government respondents interviewed (31 per cent) stated that they were unable to determine if they had suffered a data breach, compared to the average of all respondents (14 per cent).

### Who Curates Data?

- IT and IT Security is responsible for managing customer data in eighty-one percent (81 per cent) of organisations, though other departments can play a role.

- Other departments that manage customer data are:
  - Operations (30 per cent)
  - Finance (20 per cent)
  - Marketing (16 per cent)
  - Legal (14 per cent)
  - Sales (4 per cent)
- Other (7 per cent)

Those who have experienced a data breach are less likely to have their customer data managed by IT and IT Security (70 per cent) and are more likely to have customer data managed by marketing (33 per cent).

Changes to the Australian Privacy Act

59 per cent of survey respondents are either unaware or unsure that there have been any recent changes to the Australian Privacy Act which will see organisations liable to fines of up to $1.7 Million and individuals up to $370K for not taking reasonable steps to protect this data from March 2014.

Of those organisations aware of the November 2012 changes to Australian Privacy Act, 49 per cent have conducted a Privacy Impact Assessment (PIA). Of this subgroup, 46 per cent of respondents had also conducted reviews of existing technology controls, and 33 per cent have sought legal advice.

Respondents who are aware of the changes are more likely to encrypt data (81 per cent) versus those who are not aware (49 per cent).

Fifty-nine percent (59 per cent) of organisations have visibility to adherence of their organisations Privacy Policy, twenty-six per cent (26 per cent) do not have visibility and fifteen percent (15 per cent) are unsure whether they have visibility to adherence.

Instances of Data Breach

- One in five (21 per cent) Australian organisations have experienced a data breach and fourteen per cent (14 per cent) are unsure if they have.
- Over one third of organisations interviewed, 35 per cent admitted they have either had, or think they may have experienced a data breach.
- In instances of a breach, 18 per cent told no one outside the business.
- In those organisations who had admitted to a data breach, 67 per cent of the time a member of senior management or privacy officer was not informed.
- Meanwhile, of those who experienced a data breach, many incidents were more likely to involve an insecure technology such as a smart device (50 per cent), personal laptop (36 per cent) and free online storage (23 per cent).
- A wide range of types of data were lost. The average number of types lost was 2.34 showing that multiple forms of data were compromised in data breaches. The types of data lost are:
  - Customer information such as names/address/birthday/passwords/contact/detail (48 per cent)
  - Financial data including budgets, purchase orders, supplier information, customer credit cards/invoices (36 per cent)
  - Network/online application passwords (35 per cent)
  - Proprietary information (product launches, sales presentations, customer case studies, etc 36 per cent)
  - Competitive data including information on competitive position, differentiators and competitor intelligence (32 per cent)
  - TFNs (13 per cent)
  - Medical Records (7 per cent)
  - Other (2 per cent)

Organisation Size

- There are marked differences between organisations with 2,000-plus employees compared to those with less than 2,000 employees. For example:
  - Almost a quarter (24 per cent) of employees have no visibility of Information Classification Policy (ICP) adherence, versus 9 per cent of employees in smaller organisations.
  - One third (33 per cent) of employees aren’t aware of changes to Privacy Act, versus nearly half (44 per cent) of employees in smaller organisations.
  - Only 50 per cent of employees will encrypt information, versus 66 per cent of employees in smaller organisations.
  - Organisations with 2,000-plus employees have less visibility of breaches of privacy policies (44 per cent), versus 63 per cent spotted in smaller organisations.
  - Despite the above, employees in the larger organisations believe they manage personal data well (74 per cent) versus smaller organisations (64 per cent).
The “State of Privacy Awareness in Australian Organisations” research included 500 interviews completed online using a permission based panel in April 2013 with those that were responsible for managing an organisation’s customers’ personal information. Quotas were set for company size and industry vertical. This sample size gives a confidence level of ± 4.4 per cent at the 95 per cent confidence interval.

**Upcoming Privacy Events**

Australian Cyber Security Forum – Melbourne 26&27 August 2013. The Australian Cyber Security Forum is the only dedicated independent cyber security conference in Melbourne, targeting senior IT and security managers with the latest tools, strategies and best practices needed to stay ahead of the rising cyber threat landscape.

As a member of iappANZ you will receive 10% discount on verification of your membership. Please click here to find out more details

**Recruitment**

Publish your positions here free of charge if you are a member. In our network there are many opportunities for linking the right people with the right job.

**IAPP Certification**

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: “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, one of which is particularly relevant to iappANZ members, namely the Certified Information Privacy Professional/ Information Technology (CIPP/IT). To achieve this credential, 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/ IT.

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?*

Although the IAPP website refers to US-based certification testing only, testing is available to iappANZ members locally.

The IAPP will continue to manage certification registrations and materials, but you will now be able to set an appointment to sit your exam online at a testing centre in Australia or New Zealand.

FIND OUT MORE HERE

---

Articles featured within this bulletin are not legal advice and are provided as general information and comment only, the authors do not accept responsibility, and opinions are of the authors not that of iappANZ.
iappANZ Contact Details
If you have any comments or suggestions about this communication or any other aspect of iappANZ, please contact us.

E: admin@iappANZ.org  W: www.iappANZ.org  Ph: +61 3 9895 4475  Fax: +61 3 9898 0249  Mail: PO Box 193 Surrey Hills VIC 3127 Australia