Welcome to our autumn edition of Privacy Unbound. A flying start to the year for your privacy organisation, which has just completed its first 10 member training sessions and is thrilled to announce that it is now a part of the Global iapp Knowledge Net. What this means is that in future you will be able to get CPE points to maintain your certifications when you attend our sessions. It also means you are a part of a global network spanning 52 countries and it should create some great new networks for you.

We are also delighted to confirm the date for the annual privacy summit – 17th November 2014 at The Westin Hotel Sydney – save the date. Also on the event front, we have 3 events programmed for May 2014. Save the 6th May in Sydney for either the breakfast debate discussed below or the afternoon session on breaches. And if you are in Brisbane, Commissioner Pilgrim and CPO Michelle Dennedy will be there on the 8th May to give you a run down on breaches and how to assess and improve any vulnerabilities in your organisation. All of these events will be on our website soon and open for registration.

Our aim is not to simply provide you with legal updates (and this month there is a beauty on the data breach notification Bill by our Editor and iappANZ Board Director Veronica Scott), but to give you the broadest and most current information relating to your privacy practice. This month we have offerings which I hope do just that. Mr March, aka Peter Leonard has left his bat cave and come out with some great and very current pieces on the ALRC Inquiry into serious invasions of privacy in the digital era. This sets the stage for our Privacy Awareness Week debate on 6th May in Sydney where the ALRC Commissioner McDonald, OAIC Commissioner John McMillan and a third and stellar guest to be confirmed will provide some lively discussion over breakfast.

Once again, by popular demand we bring you the Q+A session with the Australian Privacy Commissioner Timothy Pilgrim and for our New Zealand readers, I am going to ask your new Privacy President’s Letter

By Emma Hossack
President
emma.hossack@iappanz.org
m:+61411478799
It’s great to hear from previous iappANZ Board Director Helen Lewin who is profiled this month – she gives us some fascinating views on the move from private to public practice and plenty more. If you are interested in being profiled in our Privacy Unbound bulletin, or would like to nominate someone else, let us know.

I have enjoyed all the pieces in this edition, but perhaps my favourite this month is from David Templeton (‘Response and responsibility’). An insightful and practical review of the Target data security breach. Plenty to learn from that, including the fact that no matter what technology you use, without a culture of privacy, organisations are at risk.

Warm regards

Emma Hossack, President

Vice President’s Foreword
By Anna Kuperman
Vice President
M: 0419 803 263

When I think about the month of March, the following words come to mind: ‘Must get it done NOW!’ I’m sure those words ring true for many of our readers whether said loudly in meeting rooms or quietly in a darkened room. Well, the high drama of the 12 March deadline has well and truly passed, I sense that the continuing work on data reviews, flows, risk, assurance and overall sanity will continue. So, in this month’s Privacy Unbound, our editors proudly introduce two of our heavy hitting Board Directors, Peter Leonard and James Kelaher.

We also have an article from iappANZ Board Director and Secretary, David Templeton on the Target data security breach which provides some very insightful observations and questions relevant to any senior person or stakeholder in data management or in a compliance function. Every case study of a data breach that I have ever read lands at the inevitable question – did the organisation have a sufficiently robust structure and culture to respond swiftly and methodically to an information security crisis? Not easy!

Turning from malware to marketing, an article from our friends in the Corrs privacy group highlights the privacy issues with data aggregation to enhance user profiles in the marketing world and the notifications that should be provided.

Our iappANZ Treasurer, Melanie Marks provides another informative and very useful Q&A session with Privacy Commissioner Timothy Pilgrim on the OAIC’s proposed privacy regulatory action policy. Peter Leonard writes a great piece on de-identification, big data analytics and the vicious cycle of data identification and de-identification in the real world as well as a thought provoking piece on the statutory cause of action for invasions of privacy. And yet another phoenix topic rising, our Editor Veronica Scott and colleague Tarryn Ryan from Minter Ellison discuss the state of play with data breach notification. Finally, we are thrilled that one of our former iappANZ Board Directors Helen Lewin has been appointed as the Deputy Victorian Privacy Commissioner and agreed to answers our questions about her new role and background.

Please ‘SAVE THE DATE’ for the Privacy Awareness Week in our schedule ... it’s a big week for privacy and for iappANZ.
Introducing your new iappANZ Board for 2014

Each month we will be introducing some of our iappANZ Board Directors for 2014. We are very pleased to continue this with two more of our Directors, Peter Leonard, who is in his second year on the Board and James Kelaher, who has just joined us this year...

Peter Leonard

Where to start with a profile of Peter Leonard, iappANZ's Renaissance man, who is in his second term on the Board? Let’s start with the boy from Bega who grew up to forge new frontiers in Australian telecommunications law - or as Communications Alliance put it - ‘one of Australia’s foremost and most highly respected telecoms lawyers since the pre-Telstra era, playing key roles in … competitive telco market evolution’. Choice of telecoms and number portability - who could have dreamed of that in 1988? That’s when Peter headed to Gilbert + Tobin (G+T) as a founding partner, and where he currently heads the Content and Data practice in Gilbert +Tobin’s TMT + Projects group.

Peter works on transactions for Asia-Pacific clients in the technology, media, communications and internet business fields. That means immersion in all sorts of data and privacy issues from data analytics to telecommunications interception, from privacy audits to regulatory wrangling. Peter also:

• chairs the Law Council of Australia’s Media and Communications Committee;
• is a member of the Advisory Board of the Centre for Media and Telecommunications Law at the University of Melbourne; and
• is an active member of the International Bar Association and American Bar Association.

Peter writes a lot too. You’ll see his latest articles in this bulletin (and yes we have more than one from him this month). He is our Mr March for sure.

As Peter is always first with the news about privacy law developments, his fellow iappANZ board members are convinced he spends his spare time sitting in a darkened room watching Hansard transcript feeds on multiple TV screens ... privacy law's answer to Elvis Presley at Graceland, minus the peanut butter and jelly sandwiches.

Peter holds a Bachelor of Economics and Masters of Laws from the University of Sydney.
And then we have James, one of the iappANZ’s newest board members. Based in sunny Brisbane, James is a director of the Smart group of companies. This figures as James is one smart cookie!

The Smart group is active in the ‘privacy space’ (among other things, providing technology and consulting services, www.smart-group.com.au), and that’s where James comes in. While having expertise across many different areas, in the land of privacy, James’s focus is on online privacy, identity management and technology, and he knows an awful lot about health privacy.

And here’s why - prior to joining the Smart Group, James was a managing director and board member of the Health Insurance Commission and a deputy secretary in the Department of Human Services. James chaired the Australian government’s PKI registration authority charged with introducing information security to the health sector – no small task!

James is also:

- a member of the National Consultative Committee on Security and Risk;
- a member of the National Standing Committee on Cloud Computing;
- a director of QEstel (a regional telco provider) and TrustWorks360 (an online identity solution developer which follows the privacy by design principles).

You might think all that would chew up all of James’s time but no – when he’s not wearing his privacy hat he can be found cycling or doing yoga … or watching cable TV shows like Banshee, Longmire and Justified.

James grew up in Sydney and is long-time supporter of the Roosters NRL team, which he regards as very sensitive information in the Sunshine State.

James holds a Bachelor’s degree in Arts/Commerce from Australian National University and an MBA from Deakin University.

Response and Responsibility
by David Templeton

FireEye is probably a familiar name. It offers state of the art malware protection for corporate networks. Its software is widely recognized as innovative and highly effective, and it was probably not surprising that the retail giant Target purchased FireEye’s malware detection system to protect the enormous volume of personal information (including credit card data) that Target handles and holds.

What was surprising was that having installed FireEye’s state of the art protection, and having established a security team in Bangalore with sufficient expertise to recognize and interpret its malware warnings, Target simply failed to act on those warnings when its Bangalore monitoring team escalated them to the firm’s headquarters in the US, back in early December 2013 while we were recovering from iappANZ’s Privacy Summit. Had it done so, Target could have averted one of the largest malicious data thefts in history. But it didn’t.

(The Target hack, and apparently linked and more or less contemporaneous attacks on other North American retailers including Niemann Marcus has been widely reported in online and print media. Some of the most extensive coverage appeared earlier this month in BloombergBusinessWeek. Factual aspects of the hack are based on this and other related reporting, particularly in the New York Times. Technically oriented accounts are
The result is that around 40 million credit card numbers, 70 million customer names and associated address details have been pilfered by persons unknown somewhere in Eastern Europe. Individual credentials have already appeared on the usual black market sites. Target’s US sales have been severely damaged and it has spent millions on customer response, investigation, regulatory and court filings and so on. The final cost will be staggering.

Exactly why the warnings were not acted upon, and the many questions beginning with “who” and “when” and “how” are painful issues for Target, which is really the victim here as much as any of the affected customers. It’s not my role to speculate about fault. Nevertheless, this terrible incident resonates uncannily with prior organisational failures to recognize and act upon early warnings.

What follows are some observations drawn from history (and to some extent experience) as to cultural issues in organisations that might impair the ability of organisations to deal with early indications of an emerging crisis. In Target’s case, hackers apparently gained access via compromised vendor credentials and once in, loaded malware that hijacked a server where it then stockpiled customer information as retail purchases were processed and eventually uploaded the data back to the hackers. Target’s malware protection identified and reported the unauthorised intrusion while there was still time to prevent data loss.

It is timely, of course, to reflect on the cultural and organizational components of the systems that your organisations, agencies or clients need in order to comply with their privacy obligations, maintain trust in their brands and preserve the value of their information assets.

Remember, some threats need to be acted upon urgently. Information security must be able to close the stable doors before the horse has bolted. Some of the questions to consider in evaluating how quickly you can get to those doors include:

1. Will an urgent warning be recognised? Do all the key people know how to interpret warnings and reports from your information security systems, and how to respond? Can the information security team effectively assimilate all relevant inputs, eg are customer or vendor issues that might have a bearing on your threat environment relayed to your information security team?

2. Is there a plan to deal with an early warning? Has the plan been tested and practiced? As part of the plan, are escalation paths clear to all key people? And, in case the horse does bolt, is there a plan for how to respond to a data breach?

3. Have these plans been rehearsed?
   In today's environment, whether it be malicious hack or just system failure, data breaches are probably more likely than fires or other serious operational interruptions. No one baulks at the idea of a fire drill, and no one properly versed in the risks would baulk at an information security drill.

4. Are there cultural or other barriers to raising or acting on alarms? Is there a healthy common view of the big picture – or are individual personalities likely to be overinvested in being right? Are mistakes tolerated? Will concern or uncertainty be tolerated at an executive level, or will it count against an employee? Will concerns without compelling evidence be treated as unwelcome noise? Are factors such as cost, service levels or expected business performance outcomes likely to desensitise the organization to warnings? Will the urgency of dealing with a security breach be understood?

Look at NASA and its classic failure of risk management, the Challenger space shuttle disaster. Clear warnings within NASA that the launch, taking place in unexpectedly low temperatures, presented risks of critical component failure were ignored because of cultural and organisational imperatives that made a launch delay less tolerable than a risk of catastrophe.

(The issues that contributed to the loss of Challenger and its crew on 28 January 1986 are canvassed at http://en.wikipedia.org/wiki/Space_Shuttle_Challenger_disaster.)

5. Do the big issues have clear owners who can influence the company’s leadership into action when needed?

---

http://bgr.com/2014/02/13/target-data-hack-how-it-happened/. And in McAfee’s latest Quarterly threat report: http://www.mcafee.com/au/resources/reports/rp-quarterly-threat-q4-2013.pdf. The incident is the subject of public enquiry and a number of legal proceedings. It has reignited US payments system reform discussions and has seen stocks in smart card manufacturers leap.)
6. Is the organisation **too thinly spread** to deal with key early indicators?
7. Does the organisation’s **business continuity plan** anticipate and adequately deal with operational issues arising because of information crisis aversion?

Having asked all these questions, be aware that it is quite possible that you are part of the problem. Be courageous if you think so, it’s definitely not the end of the world and unwitting cultural complicity is more common than you might think. Ask yourself:

1. Do I fully understand what my role might be accountable for in planning for, and executing a response to an information security crisis?
2. Do I have the trust and attention of the leaders who would need to be fully engaged in order to deal with an emerging information security crisis?
3. Can I assemble the resources I would need quickly enough to respond to an emerging information security crisis?
4. Do I have line of sight over all the inputs I need to do my job effectively?
5. Is there anything I may have been blind to, for reasons of time, cost or knowledge deficit?
6. Is there any reason my team might find it difficult to tell me anything I need to know?

If you can answer anything but yes to 1, 2, 3, and 4, and anything but no to 5 and 6, then you may need to address them. These are common issues for risk managers and regrettably, in prolonged cost-cutting environments tolerance for thin coverage gradually builds.

A helpful way to reassure yourself your organisation can deal effectively with emerging threats is to commission an external review of your compliance arrangements, and follow it up by implementing the key recommendations. Right now is a good time to do so, with business processes being reviewed to reflect the new laws in place since the 12 March.

David Templeton is a Senior Manager in ANZ’s Deposits and Home Loans business, and was formerly ANZ Group’s Privacy Compliance Manager. David is also a Board Director of iappANZ.
Privacy, profiles and targeted online advertising

by Eugenia Kolivos, Isaac Lin Dannica Alston

Collecting and handling personal information for the purposes of creating or enhancing individual profiles (particularly in the context of direct marketing and targeted online advertising) can give rise to distinct privacy issues. In particular, questions as to the nature of the information may arise, and in certain circumstances, it may be unclear whether and how certain APPs apply. For instance, it may at first glance be unclear to an entity whether information being collected is actually “personal information”, or whether that information could later take on the character of personal information. Care also needs to be taken in this area with respect to the drafting of privacy policies and collection notices.

One example of where issues may emerge, is where organisations disclose personal information to a marketing service provider to “wash” the personal information (that is, remove the information that can identify or reasonably identify an individual) for the purpose of providing the “washed” information to a third party. This practice appears to be increasingly common; washed data then is matched and combined with third party data about the same individual for the purposes of developing a more detailed profile of the individual. Some entities may believe that the disclosure to the service provider does not amount to a “disclosure” of personal information, given that after the “washing”, the information in the possession of the service provider is no longer personal information. However, at the time the service provider receives the information, the information still comprises “personal information”; the fact that the information may subsequently cease being personal information in the hands of the service provider should be relevant only to the handling of that information after its conversion. This means that the organisation must ensure that the disclosure to the service provider complies with the APPs. Where organisations engage in this practice for the ultimate purpose of direct marketing, including to build more detailed individual profiles, the disclosure will also need to comply with APP 7.

Similarly, organisations will need to be cautious when collecting information that is not personal information at the time it is collected, but is later combined with information that is personal information. For example, where an organisation offers free public Wi-Fi internet to its customers when they visit its premises (ie hotels, airports, cafes etc), the organisation may collect the IP and MAC addresses of individuals entering the WiFi range, even before the individual has connected to that network. On its own, this information would not be enough to reasonably identify a particular individual. However, if the individual is required to provide personal information (eg name and email address) to log onto or use the Wi-Fi, the IP and MAC addresses associated with the device and the personal information supplied may then take on the character of personal information. The APPs would then apply to the handling of those IP and MAC addresses. Similarly, a database of relevant pseudonyms of internet users (eg forum “handles”) and information about those users (eg comments made on a forum), without any information that could identify the relevant individuals,
would not comprise personal information; however, if the organisation holding the database subsequently collects information that allows it to identify the relevant users, the pseudonyms and other information previously held by the organisation would now be personal information and subject to the APPs.

Organisations engaging in targeted online advertising, especially those relying on enhanced individual profiles using personal information collected by a third party, should also take particular care when preparing their privacy policies and notices. Arguably, a general statement that the organisation will use the individual’s personal information for “marketing purposes” or even “direct marketing purposes” may not be sufficient. APP 7 prohibits use or disclosure of personal information for direct marketing purposes except where (among other things) the individual reasonably expects that the use or disclosure is for direct marketing purposes, or either the individual has consented to such use or disclosure or it is impracticable to obtain consent. Referring merely to broad terms such as “marketing purposes” or “direct marketing purposes” in a notice or consent is potentially problematic because:

- firstly, the practice of targeted online advertising, particularly by using an enhanced user profile, is a fairly novel form of marketing, such that individuals may not understand these broad terms to include such practices, but instead will understand them to refer to more traditional forms of direct marketing; and
- the broad language would suggest that the use and disclosure relates only to personal information collected by the organisation from the individual, not information collected by the organisation from a third party; the individual’s reasonable expectation and consent would not extend to use and disclosure of the third party information. In addition, as enhanced individual profiles include personal information acquired from third parties, APP 5(b) would likely in any event require the collection notice to include the fact that the organisation so collects or has collected this information and the circumstances of that collection.

Best practice is therefore to include in the relevant notice or consent, a specific statement notifying that personal information, including where relevant, information obtained from a third party, will be used and disclosed for the purposes of tailoring online advertising to the individual. Where personal information is provided to a third party to obtain an enhanced individual profile, this also should be called out.

Identifying what information is or could take on the character of personal information for the purposes of the Act will not always be obvious at first glance. There are a number of situations which give rise to particular issues and challenges. These situations highlight the importance of entities closely scrutinising their collection, use and disclosure of information to ensure that they are compliant with the notification and other requirements under the APPs.

Eugenia Kolivos is a Partner, Isaac Lin is a Senior Associate and Dannica Alston is a Graduate Lawyer at Corrs Chambers Westgarth
On 6 March 2014, the OAIC released its (draft) privacy regulatory action policy for consultation. The policy explains the OAIC’s range of powers and its approach to using its privacy regulatory powers and making related public communications.

1. The policy states that in considering whether or not to open a Commissioner-initiated investigation (CII) following a data breach incident, the OAIC will “take into account the fact that an entity voluntarily and proactively notified the OAIC of the incident and can demonstrate that it is responding appropriately to the breach.” What is the OAIC’s view on breach notification and if an APP entity considers that a breach incident may have occurred, what is the best way to bring it to the OAIC’s attention?

Agencies and organisations have obligations under the Privacy Act 1988 (Privacy Act) to take reasonable steps to protect the personal information they hold from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

The OAIC strongly recommends that entities develop and implement a data breach response plan, and this plan should outline the different circumstances where it would be appropriate to notify the affected individuals and the OAIC.

The OAIC has always supported data breach notification — notifying affected individuals to avoid or mitigate serious harm to them and notifying the OAIC of serious data breaches is best privacy practice, and may help your organisation mitigate the effects of the breach.

The OAIC does not investigate every data breach that comes to our attention. Before deciding to do so, the OAIC may consider if the organisation had appropriate data protection procedures in place, and whether immediate steps were taken to respond to the breach, including by notifying the OAIC and affected individuals where it is appropriate to do so. A decision to investigate will also depend on whether the organisation is responding adequately and the nature and severity of the breach.

The OAIC’s Data breach notification guide is a valuable resource for entities in establishing processes for dealing with a potential or actual data breach. I also strongly recommend that entities familiarise themselves with APP guideline 11.

2. The policy outlines a range of sources that the OAIC will consider in determining its regulatory priorities and where it will take privacy regulatory action. By way of example, how will data breach notification trends, surveys, media reports and annual reports from recognised external dispute resolution (EDR) schemes impact the OAIC’s decision making?

When deciding whether to take regulatory action the OAIC will take into account a variety of factors, which are outlined in full in paragraph 33 of the policy and include the objects of the Privacy Act, the seriousness of the conduct or incident, whether the conduct is likely to continue if no intervention is taken, whether the entity has been investigated for similar issues in the past, and whether they have taken active steps to mitigate the situation, including contacting or cooperating with the OAIC.

3. Please outline the role played by the Information Advisory Committee and Privacy Advisory Committee in OAIC’s regulatory approach.

The Information Advisory Committee (IAC) and the Privacy Advisory Committee (PAC) are statutory committees established to provide assistance and advice to the Australian Information Commissioner. These committees provide advice on privacy and information policy issues, but they do not play a role in taking regulatory action or in setting the OAIC’s regulatory approach.

4. The Policy details the OAIC’s role in international enforcement, and specifically the efficiencies that can be gained by working in partnership with privacy regulators in foreign jurisdictions with aligned privacy interests. Have there been any previous opportunities for international cooperation that you would like to highlight?
Privacy regulation is increasingly required to take place in an international context - the international nature of everything from business to data storage means that many privacy issues, particularly as relates to technology, have an impact in more than the jurisdiction.

Over the last three years, the OAIC has been working cooperatively with the Asia Pacific Privacy Authorities (APPA) technology working group to engage with global organisations about their information handling practices. The OAIC has also recently worked with an international group of data protection commissioners to examine the privacy implications of cutting edge technologies. This is a good example of the importance of working closely with regulators around the world, as well as with businesses, to ensure privacy protections are built into technology and business processes at the outset, hopefully negating the necessity for regulatory action in the future.

The OAIC has published guidance on when de-identification may be appropriate, how to choose appropriate de-identification techniques and how to assess the risk of re-identification.

5. What risk assessment approach does the OAIC recommend when it comes to ‘confidentialisation’?

The OAIC’s Privacy business resource 4: De-identification of data and information outlines when de-identification may be appropriate, how to choose appropriate de-identification techniques and how to assess the risk of re-identification.

When de-identifying data for the purposes of section 6 of the Privacy Act, entities should conduct a robust risk assessment. The risk of re-identification will depend on a number of factors, including the type of data and how difficult or impractical it would be to re-identify. The OAIC recommends applying the ‘motivated intruder’ test, which considers whether a reasonably competent and motivated person may be able to re-identify the data using publically available tools. The OAIC also recommends looking at data ‘in the round’, to assess whether a member of the public may be able to re-identify the information either in isolation or in conjunction with other publically available data.

6. What material changes been made to the OAIC’s guidance, since the release of the current PIA guide?

The OAIC’s Privacy Impact Assessment Guide is being been updated to take into account the changes to the Privacy Act from 12 March. The guide will be much shorter and has been re-ordered. In updating this guide we have also taken into account research on best privacy practice and privacy impact assessment guides from other similar jurisdictions. The draft guide has been out for public consultation and will be formally released during Privacy Awareness Week 2014.

The updated Guide to conducting privacy impact assessments will help all APP entities undertake a privacy impact assessment, and sets out a ten step process to follow, as well as guidance about how to complete these steps.

7. One of the Information Commissioner’s new powers is to issue ‘PIA directions’ - in essence, directing an agency to give the Commissioner a privacy impact assessment (PIA) about a proposed activity or function. The Commissioner may issue a PIA direction where the proposed activity involves the handling of personal information, and the Commissioner considers that the activity or function might have a significant impact on the privacy of individuals. Whilst this power extends only to the public sector, what advice does the OAIC have for business regarding the conduct of PIAs?

Conducting a PIA for projects that involve personal information ensures privacy can be built into the design. Undertaking a threshold assessment can assist organisations and agencies to determine whether a PIA is necessary for a project, and should be routinely conducted for every project involving the handling of personal information. The greater the project’s complexity and privacy scope, the more likely it is that a comprehensive PIA will be required to determine and manage its privacy impacts.

The changes to privacy processes that are needed to make them compliant with the new laws are the biggest we have seen in two decades. That means that the importance of conducting privacy impact assessments should remain at the forefront of our awareness. With such substantial changes to the law, if you have not already done so, I would recommend approaching all your ‘business-as-usual processes’ as ‘new’. Projects and processes that you have used for years have never been used under the new laws, and the last thing you want is an embedded practice that you have overlooked to let you down when it comes to compliance.

Under the new laws, the OAIC will be able to require Australian Government Agencies to undertake PIAs. Although this does not currently apply to private sector entities, there will be a review of these provisions within the next 5 years, and part of this review will be to determine whether the power to require a PIA should be extended to cover all APP entities.
De-identification of personal information and privacy regulation: are we moving forward or backwards?

By Peter Leonard

One open issue in privacy regulation is appropriate regulation of ‘big data’ analysis of customer transactional data.

The issue can be simply stated. Good privacy practice requires minimisation of use of personal information. Often the most effective way to minimise use of personal information is to remove identifiers and then use only anonymised but still disaggregated, transaction level data (for example, stripping the customer identifier and using a random number instead). Many valuable business data analytics tasks can be effectively performed using anonymised transaction level data. The use of effectively de-identified information should be facilitated by privacy regulation. Effective de-identification obviates privacy and security risks that are attendant upon use of personally identifying information for data analytical applications. But at the same time as conducting such anonymised transaction level analytics, most organisations continue to collect and maintain customer records, including personal information, to facilitate the organisation’s dealings with individual customers. Can an organisation effectively separate the two streams of activity? Should the fact that an organisation maintains any database of personal information infect the organisation’s handling of de-identified information, such that this de-identified information must be treated as personal information and managed in accordance with the APPs?

The privacy analysis is relatively straightforward in the context of de-identified information being exposed to third parties or even put into the public domain. Personal information that has been de-identified is no longer personal information. Personal information is de-identified ‘if the information is no longer about an identifiable individual or an individual who is reasonably identifiable’. Privacy regulators in jurisdictions that have considered this issue in any depth conclude that the analysis of whether personal information has become effectively de-identified must be considered looking at the particular facts and circumstances, or as it is sometimes put, ‘contextually’ or ‘in the round’. The Australian Privacy Commissioner’s recent Australian Privacy Principles Guidelines cite by way of example a variant of the frequently cited Governor William Weld example: information that an unnamed person with a certain medical condition lives in a specific postcode area may not enable the individual to be identified and would not therefore be personal information. By contrast, it may be personal information if held by an entity or individual with specific knowledge that could link an individual to the medical condition and the postcode. The Guidelines sensibly suggest (at paragraph B.86) that whether an individual is ‘reasonably identifiable’ from particular information will depend on considerations that include:

- the nature and amount of information;
- the circumstances of its receipt;
- who will have access to the information and other information either held by or available to the APP entity that holds the information; and
- whether it is possible for the individual or entity that holds the information to identify the individual, using available resources (including other information available to that individual or entity). Where it may be possible to identify an individual using available resources, the practicability, including the time and cost involved, will be relevant to deciding whether an individual is ‘reasonably identifiable’;
- if the information is publically released, whether a reasonable member of the public who accesses that information would be able to identify the individual.

But the privacy analysis ceases to be straightforward when the consideration shifts to the effectiveness of separation of two streams of activity within an organisation, one being management of a customer relationship management database and the other data analytics activities using de-identified transactional data. Consider the Commissioner’s statement in the Guidelines (at paragraph B.87), as follows: “Even though it may be technically possible to identify an individual from information, if doing so is so impractical that there is
almost no likelihood of it occurring, the information would not generally be regarded as ‘personal information’. An individual may not be reasonably identifiable if the steps required to do so are excessively time-consuming or costly in all the circumstances.”

This statement appears to look only at infeasibility or impracticality of re-identification. It does not appear to consider whether technical, operational or contractual safeguards are likely to be effective to ensure that re-identification will not be attempted (or inadvertently facilitated) within an organisation in the course of, or in any way following, that analysis of deidentified data. In other words, the statement does not appear to focus upon unlikelihood through an organisation taking steps to ensure re-identification will not occur, even while it remains feasible. The statement also proposes what appears to be intended to be a very high hurdle - “almost no likelihood of it occurring” - that does not have any accepted legal meaning and is therefore not readily translatable into operational recommendations.

If the Commissioner’s statement in the Guidelines is taken on its face, many data analytics activities within Australian corporations today that use de-identified transactional data are regulated as uses of personal information because re-identification remains a theoretical possibility, albeit remote. This would be the case notwithstanding the extent of safeguards that are deployed within the corporation to ensure that re-identification will not happen and notwithstanding any contractual commitments given by a corporation to its customers about how their personal information will (only) be used. In short, this approach would create a problem today for the many Australian corporations that conduct transactional data analysis for everyday business activities as diverse as logistics, stocking and stock placement, let alone new data analytics applications such as one-to-one marketing or other targeting of individual customers based upon knowledge of the individuals’ identity.

There is a significant risk here of regulatory over-reach. Any overreach would retard beneficial applications of customer data analytics and increase the disadvantage of offline retailers seeking to compete with online retailers. How? Most offline businesses know very little about their current and prospective customers. Offline businesses cannot reliably measure their customers pre-buying activity and therefore don’t know whether customers are responding to particular advertising or marketing initiatives. Offline businesses don’t know anything at all about prospective customers browsing and comparison of products before they make their in store purchase. Insights derived from data analytics of offline transactions address this competitive disadvantage. Use of these insights can facilitate business optimisation, substantially reduce costs of doing business and product wastage. For example, insights based upon store traffic data by time of day, local demographic data, weather predictions and scheduled local events can help retailers and their major suppliers better anticipate customer requirements and by so doing so get the right products in the right quantities just in time to the right stores. Retailers may target promotions and one-to-one offers to customers based upon their anticipated needs, in the same way as major online retailers.

So what is the appropriate regulatory response?

Of course, ‘big data’ retail analytics rightly gives rise to concerns about consumer privacy and excessive surveillance of individuals. These concerns are magnified when big data analytics is not understood by consumers and the processes are not transparent. But customer data is the most valuable commercial asset for most retailers. Any breach of trust between a retailer and its individual customers about uses of personal information can irreparably damage a business brand. Regulation does not need to deem personal information where it does not need to be regulated: it is the effectiveness of the barriers between handling of personal information and uses of deidentified data that should be examined, not uses of deidentified data. Data scientists conducting customer data analytics needs to be encouraged to engineer in, through ‘privacy by design’, effective technical, operational and legal safeguards that embed a high level of privacy protection for individuals. The way to do this is not to extend the net of regulation by expanding what is personal information to cover all uses of de-identified but still disaggregated transaction level information within an organisation. Instead, regulation needs to create the right requirements and incentives for organisations to effectively, sustainably and demonstrably quarantine or segregate analytics activities using de-identified transaction level information within and outside the organisation from all possible uses and disclosures of personal information.

The Commissioner’s revised Privacy business resource 4: De-identification of data and information suggests a more nuanced understanding of this need and an appropriate regulatory response. The Commissioner states “The risk of re-identification will depend
on the nature of the information asset, the de-identification techniques used and the context of the disclosure. Relevant factors to consider when determining whether an information asset has been effectively de-identified could include the cost, difficulty, practicality and likelihood of re-identification. Depending on the outcome of the risk analysis and the de-identification process, information and data custodians may need to engage an expert to undertake a statistical or scientific assessment of the information asset to ensure the risk of re-identification is low.” The difference between this formulation and that in the Commissioner’s Guidelines may appear subtle, but it is important: ‘likelihood’ of re-identification is referenced as an additional factor, together with ‘cost’, ‘difficulty’ and ‘practicality’. The relevant hurdle is also expressed as an objectively based assessment - the risk of re-identification must be reduced to be reliably assessed as “low” – as distinct from “almost no likelihood of it occurring”.

Is this sophistry or too sophisticated word-smithing? No. Uses of personal information can be effectively quarantined or segregated such that any risk of re-identification from advertent or inadvertent matching back of outcomes of analytics activities using de-identified transaction level can be objectively assessed as low. Technical infeasibility of re-identification within an organisation is probably unattainable in most situations. The Privacy Commissioner can regulate uses of personal information by requiring demonstrably reliable, repeatable and verifiable technical, operational and contractual safeguards that quarantine or segregate analytics activities using de-identified transaction level information from all possible uses of personal information. We are at the early stages of thinking about what the full range of those safeguards might be and how to objectively assess their effectiveness to guard against both advertent and inadvertent re-identification risk. But that challenge is manageable. An extension of regulation or personal information to all transactional level analysis within organisations is not manageable and would not be good privacy policy.

Peter Leonard is a Partner at Gilbert + Tobin Lawyers and is also an iappANZ Director

---

**Mandatory data breach notification legislation on the table, again**

by Tarryn Ryan and Veronica Scott

There is still confusion about whether entities subject to the *Privacy Act 1988* (Cth) (*Privacy Act*) are required to report data security breaches to the OAIC and affected individuals. They are not. However, on 20 March, with little fanfare, Labor Senator Lisa Singh reintroduced mandatory data breach notification legislation to the Senate in the form of a private member's Bill - the *Privacy Amendment (Privacy Alerts) Bill 2014* (Cth).

The Bill proposes the same amendments to the *Privacy Act 1988* (Cth) (*Privacy Act*) as those that were before Parliament last year, but which lapsed when Parliament was prorogued before the federal election. These amendments would require federal government agencies and private sector entities who are subject to the Privacy Act to notify 'significantly affected individuals' and the Office of the Australian Information Commissioner (OAIC) of a 'serious data breach'. What this means is that the OAIC and 'significantly affected individuals' would have to be notified when:

- personal, credit and/or tax file information 'held' by an entity has been subject to unauthorised access or disclosure, including when the loss of such information could compromise its security, in breach of the data security obligations in Australian Privacy Principle 11.1; and
- the entity believes on reasonable grounds that the breach is 'serious', because it will result in a 'real risk of serious harm' to the individual. A 'real risk' is defined as a risk that is not a remote risk and 'harm' includes psychological, physical, reputational, economic or financial harm.

In 2008, the Australian Law Reform Commission (ALRC) recommended introducing mandatory data breach notification as part of its report into reforming the Privacy Act. However the then Labor Government did not include the proposal as part of its initial tranche of
reforms introduced to Parliament in May 2012 in response to the ALRC report. However a year later, and following the release of a discussion paper by the then Federal Attorney-General, the same Government introduced the 2013 Bill.

The 2013 Bill was passed by the House of Representatives but stalled in the Senate after it was referred to a Senate Committee for consideration. The Senate Committee ultimately recommended the passing of the Bill, but with less than three sitting days left before the election it failed to make it through in time.

For the new incarnation of the Bill to be passed by Parliament it will need to get through the Senate (again) and the House of Representatives.

While, during the second reading debate Liberal Senators generally expressed their agreement with the notion of introducing mandatory notification, Liberal Senator Sue Boyce made it clear that the current Federal Government does not support this Bill. In particular Senator Boyce pointed to a lack of clarity around the definitions of ‘serious breach’ and ‘serious harm’ in the legislation, and the added burden on organisations so soon after the commencement of the reforms to the Privacy Act on 12 March. She said that: ‘The government would support the development of principles that would ensure that we were aware when serious breaches that caused real harm had occurred’.

Concerns about the provisions in the legislation echo those that the Coalition (and others) expressed while in opposition in relation to the 2013 Bill, and added to that are concerns about the lack of consultation and insufficient consideration.

It may be no coincidence that this Bill follows the data breach by the Department of Immigration and Boarder Protection as a result of which the personal details of thousands of asylum seekers were inadvertently made public on the Department’s website.

While some might say a new law is better than none, it seems that mandatory data breach notification in the form of this Bill will not become a reality. This is not necessarily a bad thing given the problems with key provisions in proposed legislation. But an opportunity has been missed for a proper debate and public consultation, particularly as privacy is at the forefront of everyone’s minds at the moment and the ALRC has just released its Discussion Paper on Serious Invasions of Privacy in the Digital Era.

The recent OAIC survey of community of attitudes towards privacy found that 96% of Australians believe that they should be notified if government agencies or businesses lose their personal information. Privacy Commissioner Timothy Pilgrim, a supporter of the proposed reforms, remarked at the time that this response was “a strong vote in favour of mandatory data breach notification”.

Back to the drawing board again...

Veronica Scott is Special Counsel in Minter Ellison Lawyers and a Board Director of iappANZ. Tarryn Ryan is a Lawyer at Minter Ellison Lawyers.
Helen Lewin was previously one of the founding Directors of the iappANZ Board and Chief Privacy Officer of Telstra. She has recently been appointed Deputy Victorian Privacy Commissioner. We ask Helen about her new role and her journey through privacy so far.

1. **What are the steps that have lead you to the role of Deputy Victorian Privacy Commissioner?**

My educational background is Bachelor of Jurisprudence and a Bachelor of Laws from Monash University (Melbourne, Australia) but I began my privacy journey in 1991 when I met Australia’s first Federal Privacy Commissioner Frank O’Conner while I was in-house counsel for a private investment firm.

Since then I’ve held the position of Chief Privacy Officer (CPO) and Head of Corporate Compliance at Telstra. Prior to becoming the CPO in 2006, I was the Group Privacy Advisor for Telstra based in Telstra’s Legal Directorate.

As Telstra’s CPO, I was the champion for privacy at Telstra and responsible for setting Telstra’s Privacy Policy and Telstra’s privacy framework. I headed a virtual team of business unit privacy managers, that were each responsible for managing privacy in their respective business units at Telstra including our overseas operations.

It was in 2008, that Telstra was awarded the Large Business Award at the inaugural Australian Privacy Awards. This Privacy Award was the first of its kind in the world. It recognised and rewarded organisations who exhibited a strong commitment to respecting the privacy of Australians.

As Telstra is an industry leader and given the importance it places on customer privacy, Telstra was involved in the development of privacy laws and policy in Australia. As Telstra’s CPO, I represented Telstra before legislators and regulators and also in many industry forums concerning privacy, in particular in the Telecommunications industry as well as other business privacy groups. Most importantly, I was a member of the advisory committee to the Australian Law Reform Commission during the review of Australian privacy law.

2. **What are the key responsibilities of the Deputy Victorian Privacy Commissioner?**

- To assist Victorian government agencies and organisations in understanding the need to protect the privacy of personal information in the public sector, adopting the philosophy of privacy by design and balancing public interest in the free flow of information with the public interest and protection of the privacy of personal information.
- To promote awareness so that privacy is considered responsibly in all information handling activities in the public sector.
- To create, implement and manage advice, investigations, conciliations and audit activities undertaken by the Office of the Victorian Privacy Commissioner;

3. **Having worked in the private sector for so long, are there any striking differences between private and public sector roles?**

Not really, the Information Privacy Principles that govern the State of Victoria are based on the same principles that underpin the Australian Privacy Principles. Just like the customer is the focus in all information activities undertaken by Telstra and correct handling and protection of their personal information was paramount, the same can be said to apply in the Victorian public sector. In the public sector, the “customer” is often the client, patient, student, teacher or an individual in receipt of services from the public sector, and as an individual they are entitled to be assured that their personal information is being handled appropriately and always protected. In all cases there is always a balance to be considered whether privacy is protected for the individual, or whether national security or other public interests need to take precedence.

4. **What are the three most important qualities a privacy professional should have?**

- To be a champion
To have the courage of conviction
To possess good business acumen

5. Where do you think privacy will be in the next ten years?

We have experienced an exponential increase in the intrinsic value of personal information, whether it is in the hands of an individual or a valued asset in the balance sheets of organisations or public sector agencies; with the creation of new attributes of personal information like algorithms, meta data and biometric data with a range of new uses. We have also seen an increasing number of countries around the globe implementing privacy laws and a rich desire by many people in the world for a right to be forgotten and retrieve their personal information from Facebook, Google and others, together with the fight for privacy rights in light of increasing Government surveillance and data retention for national security and law enforcement. This will continue. The right to privacy and privacy of personal information will continue to be a dominant consideration and remain an important human right.

Sound and fury meets privacy: the ALRC and a statutory cause of action for invasion of privacy

by Peter Leonard

Few areas of law incite great passions and media controversy. Information privacy and the activities of the Australian Privacy Commissioner generally fly under the public radar. Not so discussions as to a prospective cause of action for serious invasions of privacy.

The current Rebekah Brooks trial in the United Kingdom reminds us of the phone hacking controversy centred upon the now defunct British tabloid News of the World. It was this controversy that became the catalyst for renewed discussion in Australia about whether we need a new private right of action for invasion of privacy protection and ultimately led to the Federal Government’s reference to the Australian Law Reform Commission to report on that topic - again.

We then encounter the great privacy divides.

In one corner, the privacy and consumer advocates and tort law barristers point to intrusive and sometimes prurient media reporting of what might be considered private activities, including ‘outing’ of gender preferences and social and sexual peccadillos of allegedly public figures.

In another corner, providers of social networking sites point to the impossibility of patrolling user content and working out what is an invasion of an individual’s privacy and what is not. Social networking increasingly conflates public and private space: users of social networking sites have complex and nuanced views about acceptable limits upon reuse or repurposing of images or information that they elect to make available in semi-public places such as their Facebook pages.

In yet another corner, the professional print and electronic media point to a relatively low level of privacy related complaints under existing media codes of practice and the availability of low cost remedies for affected individuals through the Australian Press Council and the Australian Media and Communications Authority. More colourfully, the professional media decry a ‘chilling effect upon freedom of speech’ that is said to arise from any addition of a right of privacy to existing restrictions upon media reporting such as laws of defamation, contempt, closed courts, suppression orders and non-publication orders.

And finally, the de-regulation corner. Creation of any new cause of action might be said to run directly counter to the professed ‘anti red tape’ agenda of the Federal Government and Attorney General George Brandis.
It is worth pausing for a second to note where Australian privacy law is today. There is at present no common law right of action in Australia for intrusion upon an individual’s seclusion or private affairs or for misuse or disclosure of private information. The Federal Privacy Act 1988 and some State and Territory Acts regulate the use by government agencies and many businesses of personal information as embodied in particular records. This is really a sub-category of private information that is personal information collected into a material form, such as a record, for use by regulated businesses and government. There is however a general carve out in the Federal Privacy Act for journalism by media organisations that self-regulate privacy compliance in their reporting, such as through the Statement of Privacy Principles administered by the Australian Press Council. There is a ragbag of Federal, State and Territory laws addressing various aspects of surveillance, tracking and recording technologies. These laws are inconsistent and not well understood. They do not provide nationally coherent coverage or comprehensive rights of individual seclusion.

Any national ‘privacy solution’ is constitutionally complex once the Federal Government strays outside exercise of its communications and corporations powers. And any ‘privacy solution’ must balance freedom of speech, fair but vigorous media reporting, robustness of private speech, and accommodate the semi-public world of social networking, the rapidly developing fields of geo-location based services, data analytics and predictive technologies based upon anonymised information, as well as the industrial internet (or as it is sometimes called ‘the internet of things’) such as sensors talking to other things such as monitoring software.

As soon as we move beyond the regulation of ‘personal information’ as used in its technical sense in the Federal Privacy Act and many similar privacy laws overseas, the proper scope of privacy protection becomes highly contentious, with limited overseas examples.

Into this morass bravely ventures Professor Barbara McDonald and her team at the Australian Law Reform Commission. The ALRC’s Discussion Paper on Serious Invasions of Privacy in the Digital Era was released on Monday 31 March. The Discussion Paper sets out a series of draft proposals, coupled with questions. The questions solicit submissions and make further comments that might inform final proposals. The closing date for submissions to the Discussion Paper is 12 May 2014.

The ALRC proposes draft principles to guide development of a new cause of action that seeks to balance on the one hand, an individual’s right to seclusion and maintain the privacy of private information (such as information about intimate and family matters, health or medical matters, or financial matters) and on the other, freedom of expression and a broader public interest.

The Discussion Paper is divided into the following parts.

Part 1

Part 1 deals with the background to the Inquiry and includes an overview of the current law and what the ALRC has identified as gaps and deficiencies in coverage of current law. Chapter 2 sets out the ALRC’s suggested principles guiding its proposals. These Guiding Principles have been expanded from earlier draft principles detailed in the previous Issues Paper and now include the interesting concept of shared responsibility: specifically, that capable adults with the power and means to do so should exercise control over private information, using tools made available to them by service providers to protect that information. The ALRC also refers to the important role of education in helping people to protect their privacy.

Part 2

Part 2 sets out the detailed legal design of the statutory cause of action. This is the heart of the ALRC’s new work. It includes the elements for actionability:

- what conduct could amount to an invasion of privacy - intrusion upon the plaintiff’s seclusion or private affairs (including by unlawful surveillance) or misuse or disclosure of private information about the plaintiff;
- the fault requirement (being intent or recklessness);
- the requirement of a reasonable expectation of privacy in all the circumstances;
- the ‘seriousness’ threshold (likely to be highly offensive, distressing or harmful to a person of ordinary sensibilities in the position of the plaintiff); and
• the balancing of the defendant’s interests and matters of public interest including freedom of the media to investigate, and inform and comment on matters of public concern and importance.

The ALRC proposes defences, including a possible safe harbour scheme to protect internet intermediaries from liability for serious invasions of privacy committed by third party users of their services.

Proposed remedies include compensatory damages for a plaintiff’s emotional distress as determined by the Court.

Part 3

Part 3 deals with other existing and proposed remedies and legislative regimes. Some of the proposals in this Part are possible alternatives to the statutory cause of action, if the ALRC’s proposed recommendations are not accepted by the Federal Government. They include:

• possible expansion of the right to bring breach of confidence actions to include a right to recover damages for emotional distress arising from disclosure of private information;
• new, uniform harassment legislation;
• badly needed reform of surveillance devices legislation across Australia with the ALRC suggesting that this reform occur regardless of whether the statutory cause of action is enacted.

Finally, the Discussion Paper concludes with proposals for new regulatory mechanisms to counter serious invasions of privacy, including:

• a power for the ACMA similar to that of the OIAC in respect of complaints;
• a power for the OAIC to act as ‘amicus curiae’ (friend of the court) or intervener in court proceedings between an individual and a defendant;
• a new Australian Privacy Principle (APP) in the Federal Privacy Act: this would require an APP entity to (i) provide a simple mechanism for an individual to request destruction or de-identification of personal information that was provided to the entity by the individual and (ii) take reasonable steps in a reasonable time, to comply with such a request, subject to suitable exceptions, or provide the individual with reasons for its non-compliance; and a question as to whether a regulator should have a power to order takedown of online content.

Conclusion

The Discussion Paper continues the ALRC’s recent practice of limited length, clear Guiding Principles and settling recommendations by reference to those principles. The ALRC engages with the mechanics of designing a new cause of action and endeavours to ensure that there are practical, cost effective remedies for individuals. Like the draft recommendations or not, the Discussion Paper will no doubt incite sound and fury on all sides of the great privacy divide over the next few months.

Peter Leonard is a Partner at Gilbert + Tobin Lawyers and is also an iappANZ Board Director
Win a Cash Prize: iappANZ’s writing prize 2014

iappANZ is very excited to announce the launch of its [$250 cash] writing prize for a second year running for an article that is published in our monthly Bulletin between December 2013 and October 2014. 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.

All articles must be submitted by email, preferably in Word, to [veronica.scott@minterellison.com or an iappANZ email] by 20 October 2014. 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 profile 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, Veronica Scott, Carolyn Lidgerwood 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 enough 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.
Recruitment

Watch this space for new positions with the OAIC

The OAIC brings together in one agency the functions of information policy advice and independent oversight of privacy protection and freedom of information. Its vision is a community in which government information is managed as a national resource and personal information is respected and protected. If you would like to work with the OAIC or to find out what positions are currently available, how to apply for jobs and conditions of employment at the OAIC keep an eye on our recruitment section here. The OAIC welcomes applications from the diverse Australian community including Aboriginal and Torres Strait Islander people and people with disability, people of all ages and those from culturally and linguistically diverse backgrounds.

For more information go to the OAIC website.

Up coming Privacy Events

<table>
<thead>
<tr>
<th>Time, Date &amp; Location</th>
<th>Information</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tuesday 6 May</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 7am start             | iappANZ and Gilbert + Tobin Lawyers are hosting a Privacy Awareness Week Debate:  
  *Australian Law Reform Commission inquiry into security invasions of privacy in the digital era.*  
  Speakers include:  
  *Prof John McMillan AO*, inaugural Australian Information Commissioner, OAIC  
  *Prof. Barbara McDonald* – Commissioner, ALRC | Free for iappANZ Members |
| Gilbert + Tobin offices |             |       |
| Level 37, 2 Park Street, Sydney |             | $25 plus GST for Non-members - deductible from membership joining fee. |
| **Tuesday 6 May**      |             |       |
| 5.00pm for 5.30pm start | iappANZ and Commonwealth Bank are hosting a Privacy Awareness Week Privacy Presentation:  
  *Data Breach – where are your vulnerabilities and are you ready? Perspectives on the threat landscape, regulation and how to harden your organisation against breaches.*  
  Guest speakers include:  
  *Tim Rains* - Security, Microsoft Trustworthy Computing  
  *Timothy Pilgrim* - Australian Privacy Commissioner  
  *Michelle Dennedy* - VP and Chief Privacy Officer, McAfee and Author of *The Privacy Engineer’s Manifesto: Getting Policy to Code to QA Value.* | Free for iappANZ Members |
| 7.00pm finish          |             | $25 plus GST for Non-members - deductible from membership joining fee. |
| Commonwealth Bank      |             |       |
| Colonial Theatre       |             |       |
| 201 Sussex Street, Sydney |             |       |
| **Price**              |             |       |
| Free for iappANZ Members |             |       |
| $25 plus GST for Non-members - deductible from membership joining fee. |       |
| More information and how to register email – Emma Heath, GM iappANZ, emma.heath@iappanz.org |       |
| More information and how to register email – Emma Heath, GM iappANZ, emma.heath@iappanz.org |       |
### Thursday 8 May
12.15pm for a 12.30pm start  
1.45pm finish  
Gadens Lawyers, Level 11,  
111 Eagle Street Brisbane

iappANZ and McAfee are hosting a Privacy Awareness Week Lunch Presentation:

*Data breach - where are your vulnerabilities and are you ready? Perspectives on the threat landscape, regulation and how to harden your organisation against breaches.*

Guest speakers include industry leaders and privacy professionals:

- Timothy Pilgrim - Australian Privacy Commissioner  
- Michelle Dennedy - VP and Chief Privacy Officer, McAfee and Author of *The Privacy Engineer's Manifesto: Getting Policy to Code to QA Value*

Free for iappANZ members  
$25 plus GST for Non-members - deductible from membership joining fee  
To register a place contact Emma Heath, GM, iappANZ emma.heath@iappanz.org

### Monday 17 November 2014
All day event  
The Westin Hotel, Sydney

iappANZ Privacy Summit  
Join us for another great set of privacy sessions and international key-note speakers  
Watch this space for further details...

TBC
IAPP Certification

Privacy is a growing concern across organizations 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 recognized 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.

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 center in Australia or New Zealand.

FIND OUT MORE at: