President’s Letter
By Anna Kuperman
President
M: 0419 803 263

Dear members,

I am excited to share with you some fabulous news on an iappANZ road-show for Privacy Awareness Week 2015 – Privacy everyday. Our mission is to get across to as many members as we can during this week and we are looking to partner with our privacy friends in Brisbane and Adelaide to see if we can extend our road-show. If you are a member in Brisbane or Adelaide and your organisation would like to get involved with hosting an event during PAW, please let us know.

We will be running events in Sydney, Melbourne and New Zealand featuring Professor Fred Cate as our guest international speaker. Professor Cate has a distinguished profile as a scholar, educator, policy advisor, speaker and author in the world of privacy and cyber-security and has testified before numerous congressional committees and speaks frequently before professional, industry, and government groups. We are fortunate to have Professor Cate share his insights and learnings on privacy in the digital age. There will be more information coming to you around Professor Cate and each of our planned PAW sessions in coming weeks and months.

Our kick-off event in February featuring Richard Thomas on a Risk Based Approach to Privacy together with Privacy Commissioner Timothy Pilgrim, NSW Privacy Commissioner Dr Elizabeth Coombs and Board Director, Olga Ganopolsky was very well attended and we thank you for your continued support. Our Victorian members were invited to attend a Global Knowledge Net meeting (GKN) at Minter Ellison offices with Helen Lewin, Victorian Deputy Privacy Commissioner which from all reports was a great conversation amongst peers and stakeholders.

We encourage members to get in touch with our General Manager, Emma Heath (Emma.Heath@iappanz.org) if you have a particular area of interest that you would like to explore in a GKN meeting in your State. Emma can share all ideas with the relevant GKN Chair to ensure that member interests are captured for upcoming meetings. The Board has an ambitious pipeline of privacy initiatives and collaborative partnerships to engage with our members this year and we hope to see many of you during our events in PAW.

Happy reading, Anna Kuperman
This week, Acxiom hosted its third Privacy & Data Roundtable Discussion, after successful events in the USA and Japan. The event drew together marketers and business leaders as well as policy, legal and compliance professionals and others with an interest in the intersection between data driven marketing and privacy. The iappANZ thanks Acxiom for including us in this event.

This month’s Privacy Unbound kicks off with some insights from Australia’s Privacy Commissioner, Timothy Pilgrim. Join the Privacy Commissioner as he shares his views on big issues, trends and events for 2015 and the proposed metadata retention scheme and gives us insight to what it means to do “Privacy Everyday”.

Kate Monckton celebrates the first anniversary of the reforms to the Commonwealth Privacy Act by looking back on a year in privacy law.

Peter Leonard turns our minds to the challenges of risk management methodologies in privacy and reminds us of the importance of that the concept of the reasonable man and reasonableness in privacy when assessing what is personal information, what is reasonable steps or whether information is truly “de-identified”... and what happens when a risk based interpretation of “disclosure” bumps up against its plain meaning? Who knew that privacy could give rise to 50 shades of grey every day?

Nigel Phair shines the spotlight on insider threats. What practical steps can we take to avoid and mitigate the fallout when a disgruntled employee, ex-contractor or consultant exploits legitimate access to an organisation’s information assets for unauthorised or malicious purposes?

Eugenia Kolivos and Sarah Godden write about the complexity that emerges when data is moved across country boundaries through the adoption of cloud storage and service solutions. Applying insights from other international regulatory regimes, they provide useful tips for managing this risk.

Olga Ganapolsky reports on the Senate recommendation to introduce mandatory data breach reporting.

This month we profile Eric Lowenstein. A member of iappANZ, Eric leads Aon’s national cyber risk strategy, advising clients on how to identify and assess their cyber risk exposures and developing risk transfer solutions to cover identified gaps. Eric also helps out on iappANZ’s Training & Events Sub-Committee.

Will any of these authors be the winner of this year’s writing prize? If you’d like to know (and perhaps critically assess them for yourself), turn to page 19 for the rules!

Jobs: Minter Ellison is advertising for a Senior Lawyer. Want to know more? Better read on.

Events: Upcoming events are profiled at the end of this month’s edition.

Welcome Sub-Committee members

Lastly, I’d like to take this opportunity to welcome those members who responded to my call last month and have joined a Sub-Committee in 2015. We are grateful for your time and the vitality and diversity of views that you bring to iappANZ initiatives. Participating in a Sub-Committee is a great way to get to know the Board and other members as well as directly shaping the offering of this organisation over the coming year.
A message about iappANZ membership benefits

iappANZ has grown into the pre-eminent forum for people with an interest in privacy in Australian and New Zealand, offering our members a wealth of opportunities to expand their privacy knowledge, compliance, interests and networks. We continue to work with public entities across all industry sectors as well as Privacy Commissioners in both countries.

As an iappANZ member you are entitled to receive a range of great member benefits as outlined at: www.iappANZ.org.

Through our affiliation with the International Association of Privacy Professionals (IAPP, USA), you are also entitled to additional member benefits, including the knowledge and resources located within the members’ only area of the IAPP website at: www.privacyassociation.org.

Accessing all the benefits available to you through your IAPP account is easy: simply login to your MyIAPP account using your email address as the username. If you do not yet have a password or have forgotten yours just click on the “Reset your password” link and instructions on how to create a new password will be sent to you.

Should you not wish for iappANZ to confirm your membership details in accordance with iappANZ’s privacy policy, please let me know by emailing me at E: emma.heath@iappanz.org

I hope that access to these additional privacy resources will be of benefit to your work as a privacy professional.

Emma Heath, iappANZ General Manager

Visit our website, join us on LinkedIn or follow us on Twitter

To join the privacy conversation, keep up to date on developments and events and to make connections in your professional community, connect with us today!

Our website is www.iappANZ.org.au. You can log in to our member area from our website homepage with your email and password to access past bulletins. You can also get a new password or be reminded of your username if you have forgotten it. Just click on the links on the log in box. If you still need help email us at admin@iappanz.org.

Our LinkedIn group is: http://www.linkedin.com/groups?gid=1128247&trk=anetsrch_name&qoback=.gdr_1281574752237_3

Follow us on Twitter at: https://twitter.com/iappANZ
Five Questions for Timothy Pilgrim, the Australian Privacy Commissioner

by Melanie Marks

“Questions for the Privacy Commissioner” returns again this year to Privacy Unbound. This month we start with Australian Privacy Commissioner Timothy Pilgrim answering questions about current developments in 2015 for his Office and for the privacy profession.

1. What are the big issues, trends and events on the Commissioner’s radar for 2015?

We are currently working on our new Privacy Management Framework. This will be a useful tool for organisations when they’re developing or reviewing their privacy program. The framework will emphasise governance, leadership and accountability as forming the basis of a robust privacy management plan. I encourage organisations to refer to this framework when it’s launched during Privacy Awareness Week in May.

Over the last two years we have participated in the annual Global Privacy Enforcement Network sweep. In 2013 we looked at the privacy policies of the 50 most visited websites in Australian and in 2014 we examined the types of permissions that popular iOS mobile apps were seeking, including how the apps explained to consumers why they wanted the personal information and what they planned to do with it.

We will again be participating in the GPEN sweep this year, with a focus on children’s online privacy. It will be held in the week after Privacy Awareness Week.

We are also rolling out our 2015 assessment program. We are currently assessing the online privacy policies of 21 APP entities against the requirements of Australian Privacy Principle 1. These assessments will look at whether the policies are clearly expressed and up-to-date, cover the content and contact requirements and are available in an appropriate form. We have identified these entities for inclusion in this assessment if they met one or more of the following criteria: the entity was identified for follow up action during the OAIC’s 2013 GPEN sweep; the OAIC has received a large volume of complaints about the entity in 2013-14; or the entity had one of the most visited websites in Australia.

We have already conducted assessments of the online privacy policies of seven agencies in the Australian Capital Territory and have sent feedback to those agencies. We have also commenced a series of assessments of the access controls applied by health care provider organisations relating to access by their staff to the eHealth system.

Other assessments will be occurring throughout 2015.

2. Last month you attended the public hearing on Australia’s proposed data retention legislation. What can we expect to happen next with respect to the proposed regime?

I had the opportunity to outline my views on the Government’s proposed data retention scheme through our submission and then again when I gave evidence to the Parliamentary Joint Committee on Intelligence and Security in late January. A data retention scheme would impact on the privacy of individuals. There are cases where the right to privacy must be balanced with other rights, and in this case, the prevailing consideration is the safety and security of individuals. Given the proposed Bill would limit the right to privacy I emphasised the need to consider whether a scheme is a necessary and proportionate response to meeting the needs of Australian law enforcement and security. If the Committee were to recommend the scheme, then I proposed a number of additional privacy safeguards for the Committee’s consideration. We will now have to wait and see what the Committee decides when it shortly hands down its report.
3. **Privacy Authorities Australia, comprising all of the state and territory privacy regulators met this month. Could you give us some insight into the issues discussed at that forum and what sorts of outcomes we can expect to see?**

The Privacy Authorities Australia meetings, are valuable opportunity for the Commissioners from New South Wales, the Northern Territory, Queensland, Victoria and the Commonwealth to discuss privacy issues and concerns specific to their jurisdiction, as well as common issues. The meeting considered topics such as national consistency in the development of privacy health guidance, cloud computing, education apps for schools, and facial biometrics. And of course, we also discussed planning for Privacy Awareness Week. The meeting will convene again in the second half of 2015 and will focus on future opportunities for issues-based collaboration.

4. **The Office has just announced the topic of Privacy Awareness Week (PAW) this year, being “Privacy everyday”. What are the top 3 things that privacy professionals can do to engender “privacy everyday” in their organisations or the organisations they advise?**

We have selected this theme with the aim of educating organisations about the importance of embedding privacy-by-design principles into business as usual processes. Over the last 12 months I know that organisations have been working hard to comply with the new requirements but we would like to now shift the conversation from basic compliance to ongoing privacy governance. Leadership commitment to a culture of privacy and accountability is the most effective way of rising past basic compliance to good standards of privacy practice.

The top 3 things that can be done to embed ‘privacy everyday’ in organisations are:

- **Buy-in from the top –** leadership commitment is key for successful privacy governance
- **Establish robust and effective privacy practices, procedures and systems** that are well integrated with broader business processes
- **Regularly review your processes and conduct privacy impact assessments for business decisions or projects that involve new or changes to information handling practices.**

I would like to encourage all iappANZ members to join with us in participating in Privacy Awareness Week by signing up as a partner. So far we have 100 partners registered but we’d like to see many more. It’s a great way to demonstrate to your customers and staff that your organisation takes privacy seriously.

We look forward to some insights next month from Commissioner Pilgrim on privacy reform, one year past implementation.

*If you’d like to suggest a topic for an upcoming edition, please email it to melanie.marks@cba.com.au*

Timothy Pilgrim is the Australian Privacy Commissioner and Melanie Marks is Executive Manager - Digital Trust and Privacy at Commonwealth Bank (Acting) and the Vice President of iappANZ
ONE YEAR ON ... PRIVACY LAWS

One year ago, the new Australian Privacy Principles came into effect uniting the way public and private sector handle personal information. Below we take a look back over the last year at some of the top privacy stories and look ahead to what’s coming.

March 2014

News of the privacy law changes was widely covered by national media, much of it along the lines of ‘are you ready’ and what the changes meant to individuals and businesses. Along with the introduction of the Australian Privacy Principles, March saw an overhaul of the consumer credit reporting laws. One section of these proved particularly controversial. The radio personality Alan Jones loudly and repeatedly criticised the time period (5 days) after which a late payment would be noted on an individual’s credit history, which resulted in the Attorney-General, George Brandis, stepping in and changing it (14 days). More information here.

One day before the laws changes, Telstra were found to have breached the existing privacy laws by exposing the personal information of over 15,000 of its customers and were ordered to pay a fine. The full story is here.

April 2014

In April, the collective eyes of privacy professionals around the world, turned toward the USA as President Obama announced a ninety day review of consumer privacy laws and big data.

May 2014

Privacy news in May was more domestic in focus following the announcement that the new Government were to close down the Office of the Australian Information Commissioner (OAIC) leaving the Australian Information Commissioner, John McMillan redundant and moving privacy functions in to the Australian Human Rights Commission.

In May to June 2014, the OAIC was busy with dealing with and reporting on data breach notifications - we had an eBay data breach, then news hit on Catch of the Day notifying the Commissioner about a data breach that occurred in 2011. A spotlight again cast on the strength of the voluntary data breach notification process. Privacy Commissioner, Timothy Pilgrim announces that in 2013-2014 there were 71 data breach notifications to his office, but a number of incidents may still go unreported. Also in the eHealth Annual Report 2013–14, the OAIC reported it received two mandatory data breach notifications under s 75 of Australia’s Personally Controlled Electronic Health Record during the year.

June 2014

In June, the Coalition government refused to back the re-introduction of the lapsed Privacy Alerts Bill, which was not heard by the Senate before the upper house closed ahead of the 2013 federal election. The bill would have mandated data breach notification.

July 2014

A data breach at JP Morgan Chase & Co, due to a ‘basic’ security flaw resulted in the exposure of personal information about 83million account holders.

August 2014

In August, the Australian Privacy Commissioner released an updated guide to securing personal information. This guide helped to explain what his office regard as the ‘reasonable steps’ organisations should consider taking when securing personal information.

1 August 2014 - the ISO/IEC 27018, a Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.

September 2014

The Privacy Commissioner fined Department of Defence $5000 for passing on an employee’s medical records when they had been asked not to by the employee. More details on the story here.

Prospect of a tort of privacy rises again in September 2014 with the Australian Law Reform Commission’s report, Serious Invasions of Privacy in the Digital Era, tabled in Parliament on 3 September 2014, in which it recommends the creation of a tort for the invasion of privacy.

October 2014

The OAIC’s annual report noted a 183 percent growth in privacy related complaints in its annual report. Most of the complaints were made against companies in the financial sector.
Privacy and national security shakedown with the Australian government rushing mandatory data-retention legislation into the parliament with just over two sitting weeks left in the year in October 2014.

**November 2014**

The Privacy Commissioner found that the Department of Immigration breached the Privacy Act when it made the personal information of nearly 10,000 asylum seekers available on its website for 16 days due to a 'copy and paste error'. More on the story [here](#).

Privacy breach complaints almost tripled year-on-year between 2013 and 2014 in Australia according to a report from the OAIC rising from 1,496 in 2013 to 4,239 in 2014. The increase in complaints - 183 per cent - was also attributed to two large unnamed data breaches, which OAIC said resulted in a significant number of individual complaints being lodged with the commissioner about each matter.

**December 2014**

News of the Sony hack and their poor information security management dominated global newspapers. Not only were the affairs of celebrities and Hollywood studios made public, sensitive personal information about Sony’s employees were leaked also.

**January 2015**

In January the OAIC released another updated version of its *Guide to Securing Personal Information*. This time, it looked insider threat risks for the first time.

**February 2015**

The Privacy Commissioner announced that he would be reviewing 21 privacy policies of Australian organisations against the requirements of the Australian Privacy Principles. The report is due in June.

**March 2015**

The hot topic of the moment is the likely imminent passing of the proposed Data Retention Bill, including the recommendations that have been accepted by the Parliamentary Joint Committee on Intelligence and Security. These include mandatory data breach reporting.

Just last week, Telstra announced that it would provide customers access to their metadata for a fee of $25.

Kate Monckton is Privacy Officer at NBN Co and a Director of iappAANZ
Going grey, reasonably privately

by Peter Leonard

Lawyers each day grapple with shades of grey. English law is rightly sceptical of absolutes, moral or otherwise, or allegedly self-evident truths. Good judges seek to find standards for acceptable behaviour that accommodate the complexities of human sensibilities and the practicalities of everyday and business life. And so was born our ‘reasonable man’, more recently transgendered as a ‘reasonable person’.

If you work in privacy, then you are probably better friends with this person than you realise.

Getting to know the ‘reasonable man’

The ‘reasonable man’ had dubious antecedents in French enlightenment philosophy. After he crossed the English Channel, he rode the Clapham Omnibus before graduating to the Bondi Tram and the Shaukiwan Tram. Yes, the ‘reasonable man’ is indeed that person you were sitting next to on the tram or bus this morning – even if he was occupying an unreasonable amount of space.

His first English outing was back in 1837, in the case of Vaughan v. Menlove. Mr Menlove built a hay rick (or what we’d call a hay stack in this part of the world) near the boundary of his property, not far from Mr Vaughan’s cottages. Menlove was warned by Vaughan on several occasions that the rick could spontaneously ignite and therefore was a fire hazard. Menlove said that he had insurance and he would chance it. You guessed it, the hay ignited and burned down Menlove’s barns and stable and then Vaughan’s two cottages on the adjacent property. Mr Menlove’s attorney noted his client’s “misfortune of not possessing the highest order of intelligence” – never a problem nowadays - and argued that negligence should only be found if the jury decided Menlove had not acted with “bona fide [and] to the best of his judgment.” The Court disagreed, stating that such a standard would be too subjective, and: “Instead, therefore, of saying that the liability for negligence should be co-extensive with the judgment of each individual, which would be as variable as the length of the foot of each individual, we ought rather to adhere to the rule which requires in all cases a regard to caution such as a man of ordinary prudence would observe.” A man of ordinary prudence – that’s our reasonable man.

Ordinary prudence was, of course, an articulation of a principle of sensible risk management long before international standards, operating manuals, OH&S and the Big 4 consultants’ methodologies. And so English law jumped headlong into assessment of risk and finding the right (objectively ascertained) shade of grey for the particular circumstances of each case – or judging things ‘in the round’, as modern privacy practitioners like to say.

Is it personal information? What would the reasonable man say?

We start ‘in the round’ grappling with whether a person is ‘reasonably identifiable’. Most Aussie privacy professionals can recite by rote that personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not. Whether a person is ‘reasonably identifiable’ clearly requires an exercise of objective judgment about how unlikely it is that an individual’s identity could be ascertained from the information or opinion.

Privacy law does not give us guidance as to the appropriate, objective standard to apply, so it is impossible to definitely state where on the continuum between completely unidentifiable and readily identifiable that we find the point where an individual is ‘reasonably identifiable’. There is no stated standard, such as balance of probabilities, to help us find that point. Sometimes words such as ‘low’ or ‘remote’ are used, but these words don’t help much. This is largely because the practical problem is actually not defining a point on a continuum at which a possibility can be conveniently found to sit on one side or the other, but assessing a risk. Assessing risk requires a fact-specific enquiry as to what information sources might be available to the person that is dealing with the information in question that might be used to match against or otherwise analyse information about a nominally unidentified individual in order to work out the identity of that person.
In assessing risk ‘in the round’, it seems sensible to follow the lead of the UK Information Commissioner’s Office and the Australian Privacy Commissioner and to have regard to all relevant circumstances surrounding the handing of the relevant information. These circumstances include who has access to it and what safeguards – technical, operational or contractual – are deployed to ensure that purportedly de-identified information is properly protected from re-identification risk. And this is why the discussions that you sometimes see around whether particular types of information are personal information can be sterile debates. Take IP addresses. It depends upon who has the IP address and what capability or inclination they have to match it back to an individual associated with an internet access service to which that IP address was allocated at a particular time. All that can be said as a universal statement is – it depends who has the information and access to other relevant information.

Are our systems good enough? Back to the reasonable man

In recent times, a new brand of risk management consultants has sprung up, selling implementation of standards and proprietary frameworks and methodologies for privacy risk management. For all their strengths in cataloguing sources of risk and mechanisms for risk management and mitigation, these standards, frameworks and methodologies tend to go a bit flabby and vacuous at the point at which we seek to apply the risk assessment generated through their application to everyday processes in dynamic business environments. Having systematically catalogued data flows and information handling processes, how are the risks that we identify to be quantified and weighted? How does a business satisfy itself, its clients and prudential and privacy regulators that the business has effectively quarantined and managed uses of de-identified information at an appropriate level of assurance that this information is properly protected from re-identification risk? What would the reasonable man say?

Any qualification from absolute assurance of persistent de-identification in all hands leads to easy point scoring by some privacy advocates. These advocates point to any possibility of re-identification in some hands – for example, even if proper risk mitigation processes within a corporation handling anonymised information are verifiably implemented and followed but then are breached, for example, through employee oversight – as grounds a conclusion that the purportedly de-identified information should be treated as personal information. Of course, risk mitigation measures must take account of frailties and errors of humans, the devious ingenuity of malicious hackers, the recalcitrant contractors, and so on. But how do you apply a word like ‘low’ or remote’ to work out whether and when you are jumping at shadows?

Heads in the round or in the clouds?

Occasionally the law itself strays into loose use of binary concepts. For example, the Privacy Commissioner’s Guidelines as to ‘disclosure’ reasonably (that word again) inform us that “an APP entity discloses personal information when it makes it accessible to others outside the entity and releases the subsequent handling of the personal information from its effective control” (B.58). Examples provided include where an APP entity “publishes personal information whether intentionally or not and it is accessible to another entity or individual” or “displays a computer screen so that the personal information can be read by another entity or individual” (B.60). When discussing offshore disclosures, the Privacy Commissioner’s Guidelines state that in “limited circumstances providing personal information to an overseas contractor to perform services on behalf of the APP entity may be a use, rather than a disclosure. This occurs where the entity does not release the subsequent handling of personal information from its effective control. In these circumstances, the entity would not need to comply with APP 8. For example, where an APP entity provides personal information to a cloud service provider located overseas for the limited purpose of performing the services of storing and ensuring the entity may access the personal information, this may be a ‘use’ by the entity”(B.13).

So what are these “limited circumstances”? The Commissioner states three requirements. First, a binding contract between the entity and the provider requires the provider only to handle the personal information for these limited purposes. Second, the contract requires subcontractors to agree to the same obligations. Third, the contract gives the entity effective control of how the personal information is handled by the overseas recipient. “Issues to consider include whether the entity retains the right or power to access, change or retrieve the personal information, who else will be able to access the personal information and for what purposes, what type of security measures will be used for the storage and management of the personal information and whether the personal information can be retrieved or permanently deleted by the entity when no longer required or at the end of the contract.”(B.14).
The Privacy Commissioner, in my view rightly, doesn’t express a definitive view as to whether any form of controlled view-only access by the contractor would constitute a disclosure by the customer to the contractor rather than a use by the customer.

The example given in the different context of disclosure when a person “displays a computer screen so that the personal information can be read by another entity or individual” is not directly in point, because it is not clear in that case whether the disclosure arose through the viewing being facilitated without effective control – in effect, the information becoming accessible to all passers-by - or because the viewing was possible at all. Some privacy lawyers point to Europe and say the answers here would be much simpler if the Privacy Act incorporated the EU concept of ‘processing’, which covers just about anything you can do with personal information. Viewing personal information amounts to processing and hence is regulated, so whether something is a use or a disclosure doesn’t need to be asked or answered.

Back here in this part of the world, a sensible, risk management interpretation of the law would be that effective controls may mitigate risk to the point where there is no ‘disclosure’ because the risk of an act or practice contrary to the Act is too low or remote. But this practical view does bump up against the binary nature of the word ‘disclosure’ as in common usage. It is reasonable to say that if you disclose something to me, I know it and I could potentially use it or tell someone else regardless of whether I said I wouldn’t tell anyone else. This absolute or binary interpretation of the word ‘disclosure’ is easy to support both by reference to dictionaries and our memories of adolescent playgrounds. However, it does not readily facilitate a sensible risk management interpretation. So to give the word ‘disclosure’ an appropriately nuanced, sensible risk management interpretation, the Privacy Commissioner is forced to narrowly squeeze the natural meaning of disclosure. This is not tricky or wrong, but it is a case of using fencing wire to fashion a workable tool out of an inherently binary concept that the Parliament and the Parliamentary Drafters should not have left for the Privacy Commissioner and the hapless privacy professional to work out or around.

Sensible application of risk management principles to evaluate the effectiveness of technical, operational or contractual safeguards will often lead to controversial and sometimes uncertain conclusions. But this doesn’t mean that privacy law is loose or unpredictable. It just means that we continue to adapt concepts of reasonableness now nearly two hundred year old, but now applying new methodologies for systematic thinking about risk and its mitigation. It’s enough to turn you grey.

Peter Leonard heads Gilbert + Tobin Lawyers Data and Content Practice and is a Board Director of iappANZ
Meta Data Bill puts mandatory data breach notification proposal back on the agenda

by Olga Ganopolsky

On 27 February, the Parliamentary Joint Committee on Intelligence and Security published its advisory report on Australia’s Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Metadata Retention Bill). The committee’s 362 page report contains a thorough review of the 39 recommendations. These recommendations have now been accepted on a bipartisan basis.

Most of the recommendations are specific to the operation of the frameworks and related protections, should the Metadata Retention Bill be passed. However, recommendation 38, dealing with mandatory data breach reporting is generic. It recommends that:

« a mandatory data breach regime be introduced; and
« the regime should apply by the end of 2015.

As many of you will recall, mandatory data breach reporting was the subject of the Privacy Amendment (Privacy Alerts) Bill 2014 (Privacy Alerts Bill) which replicated the 2013 Bill that nearly made it onto the law books. The Privacy Alerts Bill was introduced into the Senate on 20 March 2014 and was read and debated for the second time on 19 June 2014, but has since lapsed. A data breach scheme was also recommended in The Financial System Inquiry's interim report last year citing concerns about cyber security threats to online business.

Mandatory data breach legislation if passed, would represent significant change in the law. Currently notification to an individual and the OAIC (if any) is driven by obligations in APP11 of the Privacy Act 1988 dealing with security or in the case of consumer credit reporting information, by Part IIIA of the Act. Notification is a voluntary and is largely based on OAIC guidance. The top 5 components of the current OAIC guidance are:

« Agencies and organisations have obligations under the Privacy Act 1988 (Cth) to put in place reasonable security safeguards and to take reasonable steps to protect the personal information that they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure. Those reasonable steps may include the preparation and implementation of a data breach policy and response plan (that includes notifying affected individuals and the OAIC).
« Notification of a data breach supports good privacy practice. Steps and actions in the guide are highly recommended by the OAIC.
« Data breaches are not limited to malicious actions, such as theft or ‘hacking’, but may arise from internal errors or failure to follow information handling policies that cause accidental loss or disclosure.
« In general, if there is a real risk of serious harm as a result of a data breach, the affected individuals and the OAIC should be notified.
« Notification can be an important mitigation strategy for individuals, and can promote transparency and trust in the organisation or agency (according to key messages as provided by the OAIC).

In 2013-2014, according to the OAIC’s annual report, it handled 71 data breach notifications. This was an increase of 16.4% from 2012 - 2013. These notifications deal with a variety of issues; ranging from malicious external hackings, lost data storage devices, technical gaps in testing procedures of a newly installed website and incorrectly addressed emails.

Olga Ganopolsky is General Counsel - Privacy and Data at Macquarie Group and a Director of iappANZ
The Insider Threat

by Nigel Phair

We all know about the Target breach with the theft of 40 million credit and debit card details, and 70 million customer records. We now read weekly about cyber security incidents resulting in a loss of data and other customer identifying information. Fingers are pointed at various groups and jurisdictions, but attribution in cyber space is one of the most difficult aspects to get right.

This all makes great headlines, but we rarely hear about the disgruntled employee, ex-contractor or consultant. Insider threats come from people who exploit legitimate access to an organisation’s information assets for unauthorised or malicious purposes. Many organisations don’t have adequate safeguards to detect or prevent attacks involving insiders. One reason is that many are still in denial about the magnitude of the threat. The 2012 Cyber Crime and Security Survey stated 44% of respondent organisations had been subject to between 1 and 5 internal attacks. In the 2013 Cyber Crime and Security Survey, 52% of respondents listed trusted insiders as the cyber actor which concerns them the most.

Many companies spend the majority of their IT security budget on protection from external attacks. But the figures above serve as a reminder that internal controls and measures are also important, to ensure that internal risks are properly managed. The OAIC have also, for the first time, included a section on insider threat in their most recent release of their Guide to Securing Personal Information, which demonstrates the increased awareness of the risk.

The U.S. Department of Homeland Security lists the following indicators as flags for individuals who may carry out malicious activity against their employer:

- Remotely accesses the network while on vacation, sick or at odd times
- Works odd hours without authorisation
- Notable enthusiasm for overtime, weekend or unusual work schedules
- Unnecessarily copies material, especially if it is proprietary or classified
- Interest in matters outside of the scope of their duties

Should they have sufficient motivation – financial, personal or cause-related – employees, whether they are permanent or casual staff or contractors, often have access to personal information and the opportunity to understand and exploit potential weaknesses in security. A loss of data by a trusted insider may result in the entity contravening its security obligations under APP 11 if it did not take reasonable steps to protect the personal information.

Know your staff

The best security technology in the world can’t help organisations unless employees understand their roles and responsibilities in safeguarding personal information. Training employees is a critical element of security. Employees need to understand the value of protecting customer and Fund information and their role in keeping it safe. Effectively trained staff creates a strong security culture.

Know your information

Identify what personal information an organisation holds and who has access to it is the fundamentals of good information security. Policies, procedures and guidelines that are current and well executed give an organisation a better security posture and when managed in tandem with physical controls and testing, minimise cyber risks from internal attackers.

Practise incident response

A desktop simulation of a loss of personal information can test how an organisation’s cyber incident response capability operates. The exercise should examine organisational capability to prepare for, protect from and respond to the potential effects of an insider attack. It should test strategic decision-making and coordination of incident response; and validate information-sharing relationships and communication pathways.

By assessing the risk and allocating adequate resources to protect personal information, an organisation can build a stronger security foundation and improve resilience. Such examination and communication by key executives will better prepare an organisational response should a data breach occur.

Controls

Security and monitoring controls help organisations protect against internal risks by ensuring personal information is only accessed by authorised persons.

- Inform staff of their roles and responsibilities in protecting personal information
- Deploy security tools to protect personal information
- Use software to reduce the likelihood of system-induced human error
- Enhance staff awareness of the unintentional insider threat
- Provide effective security software, for example two factor authentication for access
- Create staff values and attitudes that align with the organisations mission and societal norms

Nigel Phair is an influential analyst on the intersection of technology, crime and society. Adjunct Professor Phair has published two acclaimed books on the international impact of cybercrime, is a regular media commentator and provides executive advice on cyber security issues. In a 21 year career with the Australian Federal Police he achieved the rank of Detective Superintendent and headed up investigations at the Australian High Tech Crime Centre for four years. Follow Nigel on Twitter @nphair
Cloud Services, Data Security & Cross Jurisdictional Risk
by Eugenia Kolivos and Sarah Godden

Cloud storage and service solutions have many benefits but moving data across country boundaries adds complexity including in the event of actual or suspected breach. Applying insights from other international regulatory regimes, we provide practical tips for managing this risk.

The evolution of cloud computing¹ has provided significant economic benefits by lowering costs to access and use information technology infrastructure (often located offshore and controlled by a third party) to remotely store, transfer, and process data. The benefits of lower overheads comes with the potential for increased risk due to lack of primary custody and possibly weaker control of data in the cloud. An often overlooked risk is the multiple cross-jurisdictional legal issues that arise due to data being transferred through and stored in multiple locations worldwide. This geographical diversity presents significant challenges; complying with multiple legal obligations regarding privacy, data security and breach notifications requirements can be daunting.

In addition to the laws of the jurisdiction in which the data is stored, organisations may also be subject to local data protection and privacy laws in their ‘home’ jurisdictions (where they have operations). The Privacy Act 1988 (Cth) (the Act) provides for the extra-territorial operation of the Act in circumstances where the data has an “Australian link”.² Therefore conduct outside Australia with an Australian link may amount to a breach of the Act despite the data being stored elsewhere,³ unless that conduct is required by the law of that jurisdiction.⁴

Managing cross-jurisdictional risk

Managing cross-jurisdictional data security and regulatory compliance risks demands a disciplined approach and prior planning. Lessons can be drawn from the experience of managing similar international regulatory co-ordination in cartel matters.⁵ The goal is to develop an efficient and effective action plan that can be activated in the event of an actual or suspected breach. The procedure must enable compliance with the requirements of multiple countries.

Ensuring that your response is properly co-ordinated has the following benefits:

- Enabling you to choose a pro-active response strategy where relevant regulators and affected parties are informed by your organisation rather than becoming aware of a breach via media reports or investigations in other jurisdictions. Pro-active response strategies typically result in better relationships with the regulator and may lead to improved regulatory outcomes;
- Co-ordination reduces the risk that a regulatory strategy in one jurisdiction will negatively impact outcomes in a second jurisdiction by giving oversight of overall strategy (including managing admissions and evidence) and primary responsibility for protecting the organisation’s rights – including preservation of legal professional privilege and managing discovery obligations;
- Minimising the time to address an actual or potential breach – dealing reactively with each jurisdiction in a piecemeal manner can be drawn out and risks amplifying negative publicity, brand damage and may even impact insurance arrangements; and

¹ Cloud computing typically enables organisations to access services they could not afford to self supply by sharing between multiple users the costs of construction and operation of extremely large-scale commodity computer data centres which can unlock economies of scale in electricity, internet provision, software and hardware costs.
² Section 5B, Privacy Act 1988 (Cth)
³ Office of the Australian Information Commissioner, Data breach notification guide: a guide to handling personal information security breaches, August 2014.
⁴ Sections 6A and 6B, Privacy Act 1988 (Cth)
⁵ International co-ordination and co-operation is the norm in cartel matters with multiple bilateral arrangements between regulators in all major jurisdictions to allow information sharing, co-ordination of dawn raids (surprise investigations by regulators to search for and seize evidence relating to cartel conduct) and investigations. As a result, corporations co-ordinate and manage their response, preparation of evidence and regulatory notifications across jurisdictions.
Enabling continual improvement through holistic analysis of the actual or potential breach.

Developing an action plan

Set out below are some of the issues that should be considered when developing an action plan.

Appoint a primary response co-ordinator

Determine which jurisdiction will take the lead in co-ordinating the response to a breach in data security. The lead jurisdiction takes responsibility for identifying the affected jurisdictions and obtaining advice in each to determine:

- What has occurred;
- Whether a security breach has occurred in that jurisdiction;
- Whether there are notification requirements, e.g. to affected individuals or regulatory bodies, and whether these are mandatory or voluntary;
- Co-ordinating the response to ensure that all jurisdictions notify together, manage any admissions and evidence consistently and coherently; and
- Determining the relevant time frames for any required notifications.

The lead jurisdiction will also co-ordinate the response strategy to inform staff and if required, respond to media requests or reports.

Fail to plan, plan to fail

This is not news to privacy professionals. You know your organisation and know your data. Where is it? Where is it stored? Where are the relevant servers? How will this affect any claims for legal professional privilege in different jurisdictions? Are data transfer arrangements fit for purpose?

Armed with knowledge of your business, you can determine or seek advice regarding the most likely countries where you will have legal obligations. Do you have legal counsel able to advise in relation to these jurisdictions or are you able to quickly appoint legal advisors as needed? Do you know the likely extent of your obligations in these jurisdictions? Are there data breach reporting requirements? Does transferring data to that jurisdiction (including via email in foreign countries if your server is hosted in that jurisdiction) make those documents potentially discoverable in the event the matter is brought to Court?

The next step is to review your agreements with service providers to determine whether:

- your provider is obliged to notify you of an actual or suspected breach in time for you to meet notification requirements in these jurisdictions (taking into account a reasonable time period to investigate the circumstances and co-ordinate the response); and
- you have contractual processes in place to obtain necessary co-operation from your service provider.

Critical to this is ensuring necessary contact details for your organisation, service providers, legal advisors and regulators are kept up to date and accessible.
Communication

Privacy related matters are inherently personal and therefore are significant to customer and supplier relationships, as well as staff engagement and morale. Particularly where the circumstances of the actual or potential breach become public, it is important for organisations to proactively communicate with affected customers and suppliers, as well as employees.

Continual improvement

Once an actual or suspected breach has been addressed the lead co-ordinator should identify any improvements to business processes, systems or arrangements that can prevent or minimise future occurrences. For example, staff education and compliance training may be enhanced, or improvements made to contractual arrangements or supplier selection criteria, or system improvements could be made to allow earlier detection of potential issues.

Conclusion

Cloud storage and service solutions often result in data crossing national boundaries. In the event of an actual or suspected data security breach, multiple legal jurisdictions may therefore be involved, complicating response management. Prior preparation enables your response to a cross-jurisdictional data breach to be more effective and efficient. Applying insights from other regulatory regimes which require cross-jurisdictional response management puts you on the front foot in preparing an action plan to respond to an actual or suspected data breach.

Eugenia Kolivosis is a Partner at Corrs Chambers Westgarth. She specialises in data security, IT and technology procurement, intellectual property, advertising and marketing.
Sarah Godden is a senior associate at Corrs Chambers Westgarth. She specialises in competition, telecommunications and media regulation and privacy.
Snapshot of a Privacy Professional

iappANZ enjoys introducing its members to each other

This month we introduce Eric Lowenstein

During a career spanning insurance and legal services, Eric has developed a comprehensive mix of financial, strategic, operational and risk management skills. He has over ten years’ insurance experience in a variety of sectors, including legal, underwriting and broking which covers policy drafting, contract reviews and insurance litigation, as well as expertise in public liability, cyber risks, professional indemnity and directors’ & officers’ liability insurance.

Eric tells us his story of his privacy journey - privacy - from a different perspective.

The concept of being a ‘privacy professional’ is new to me. Coming from an insurance perspective, I don’t quite fit the traditional definition, but I still regard myself as a privacy professional. Here is my story.

A “business man doing law” or a “lawyer doing business”?

My professional background has been predominantly working in the insurance industry having had experience in a variety of sectors including legal, underwriting and broking. Most people talk about ‘falling into’ the insurance industry, and I suspect this is the same for some privacy professionals. My story is not that dissimilar – In 2004 I completed my Bachelor of Business Administration with Bachelor of Laws at Macquarie University. During University and the years that followed I was trying to decide whether I was a “business man doing law” or a “lawyer doing business”.

I spent the first few years of my professional career in private practice at Deacons (now Norton Rose) in the insurance litigation team. During that time I completed a Masters of Law and Management at UNSW. It was around this time that I was approached by an Insurer to set up a product development team for their Asia Pacific financial lines operations.

The Emergence of cyber insurance

As part of this experience, I had my first brush with the world of privacy.

In considering the privacy implications around some of the product development aspects, I was involved in the development and design of an emerging product known as ‘Network Security & Privacy’ or ‘Cyber Insurance’. Back then, Cyber Insurance was still getting recognised, but today it’s a large focus of my role. I am currently working at Aon Risk Solutions leading our national cyber risk strategy.

Cyber Insurance is a product designed to protect organisations against a wide range of first party and third party exposures that arise when their customer information is breached or stolen. The impact of cyber risks can be significant – practically, legally and financially. Beyond the immediate costs to resolve cyber issues affecting systems and data, there can be profound impacts on reputation and potentially liability to third parties.

Increasingly complex threat landscape

The issue of cyber security and privacy no longer solely sits within an organisation’s IT or privacy function. With global cyber-crime on the rise and heightened media exposure, the increasing awareness of this risk has opened interaction across a wide range of stakeholders including awareness at board level. This is where I began engaging with privacy professionals and understanding the bridge between their roles and mine.
Like privacy professionals, I keep a very close watch on legislative change both in Australia and overseas and pay particular attention to publicised breaches and privacy commissioner investigations. Any change in legislation or decision can have an impact on insurer sentiment which could ultimately affect premiums and policy coverage.

My involvement with IAPP has been a great opportunity to learn more about this incredibly important topic and network with likeminded professionals who are passionate about the impact of privacy in today’s constantly changing environment.

Eric Lowenstein is Client Manager, Financial Services Group at Aon Risk Solutions. He leads Aon’s national cyber risk strategy and advises clients across diverse industry sectors, helping them identify and assess their cyber risk exposures and developing risk transfer solutions to cover identified gaps. Eric has a Masters of Business Administration (Executive) from the Australian Graduate School of Management, a Masters of Law and Management from the University of New South Wales and a Bachelor of Business Administration with Bachelor of Laws from, Macquarie University. He is also admitted to practice as a Solicitor and is Tier 1 ASIC G 146 Accredited.
iappANZ’s writing prize 2015: entries open

Entries have now opened for this year’s writing prize for an article that is published in our monthly Journal editions from February to October 2015. 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 2015. We will need the author’s email address and contact number. You can submit as many articles as you like.

The winner will be announced at our Privacy Summit in November 2015 and their name and details will be published on our website. We also hope to profile the winner in our Journal. So alert your network and get writing!

More details about the writing prize if you are interested:

- Our Editorial team, Veronica Scott and Carolyn Lidgerwood, plus President Anna Kuperman 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.
- 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.
Employment opportunities for privacy professionals

News about employment opportunities is provided as a service to iappANZ members. If you would like a notice about employment opportunities at your organisation published in Privacy Unbound, please contact our editors (see details on last page).

MinterEllison

Senior Lawyer/Senior Associate, Privacy and Administrative law

About Us

As a top tier law firm, Minter Ellison runs an international practice, working on headline assignments for leading domestic and international clients. We have 15 offices around the world and over 900 lawyers and 800 administrative and support staff.

At Minter Ellison, our people are our brand. Every day, every person in our firm plays a vital role in helping clients to close deals, find solutions, resolve disputes, grasp opportunities and create value. We are a friendly and supportive firm that takes pride in our work, our individual and collective achievements, our clients’ success and our strong reputation in the market.

Your role

Minter Ellison Canberra is currently offering a rare opportunity for an experienced Senior Lawyer or Senior Associate to work with our administrative and public law and litigation team of lawyers under the supervision of partner Alice McCormick. We are looking for an administrative lawyer with experience in information law particularly privacy, data protection and secrecy.

You will be part of our market leading government practice which delivers practical, innovative and solutions focussed advice to our government clients including the Department of Foreign Affairs and Trade, the Department of Immigration and Border Protection, the Department of Health, the Department of Human Services and the Department of Social Services.

What you need

We welcome applications from qualified lawyers with:

- experience in administrative and public law for Commonwealth government agencies
- experience in relation to information law particularly privacy compliance, data protection and secrecy
- the ability to provide clear advice including in relation to statutory interpretation issues
- experience running matters or undertaking advice work with minimal supervision and the ability to drive a matter forward autonomously where appropriate
- strong analytical and project management skills
- attention to detail and excellent drafting and presentation skills
- a strong client focus and demonstrated ability to form enduring relationships with peers, clients and industry experts
- a team player with the ability to effectively delegate to and mentor graduate and junior lawyers and paralegals in the group
- the desire to develop your practice and participate in business development initiatives with a view to being a leader in the firm.

What we offer

You will be part of a bright and energetic team that delivers high quality results for clients. Career progression and development is recognised as vitally important to this role. We offer competitive top tier employment packages including an achievable bonus scheme. We also offer a wide range of employment benefits including:

- additional week of annual leave for Senior Associates and Special Counsel
- salary continuance insurance
- extensive health & wellbeing programs including a free gym membership
- mobile device plan

You will enjoy working in an environment where people care about ensuring that you balance your professional goals with your interests outside of work. Our internal support teams are second to none, and our learning and professional development programs are designed to maximise your legal technical expertise, client and solution focus, business acumen and leadership skills to help you take the next step in your career.

**How to apply**

Please submit your CV for consideration by clicking on the 'Apply' button below. If you would like further information, please contact Eric Norris on +61 6225 3739 for a highly confidential discussion.

*Please note that applications from agencies will not be considered at this time. To be eligible to apply for this role you must be legally permitted to work in Australia.*
## Privacy Events

<table>
<thead>
<tr>
<th>Time, Date &amp; Location</th>
<th>Information</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Wednesday 29 April</strong>&lt;br&gt;4pm-7pm&lt;br&gt;Baker McKenzie Lawyers&lt;br&gt;L27, AMP Centre&lt;br&gt;50 Bridge Street, Sydney</td>
<td>Pharmaceutical Industry and Privacy&lt;br&gt;Speakers include:&lt;br&gt;<strong>Anne-Marie Allgrove</strong> – Partner, Baker McKenzie&lt;br&gt;<strong>Malcolm Crompton</strong> – Director, IIS&lt;br&gt;<strong>Jessica Kanevsky</strong> – Legal Counsel, Abbvie&lt;br&gt;<strong>Greer Harris</strong> - Regional Privacy Officer, Asia Pacific, AstraZeneca</td>
<td>Free for iappANZ members&lt;br&gt;$99 plus GST for non-members&lt;br&gt;Registrations – <a href="mailto:admin@iappANZ.org">admin@iappANZ.org</a></td>
</tr>
<tr>
<td><strong>Events will take place throughout the week of 4-8 May 2015</strong>&lt;br&gt;Monday 4 May – Sydney&lt;br&gt;Tuesday 5 May - Melbourne&lt;br&gt;Wednesday 6 May – Wellington&lt;br&gt;Thursday 7 May, Auckland&lt;br&gt;Friday 8 May, Sydney</td>
<td>Privacy Awareness Week (PAW)&lt;br&gt;iappANZ is arranging a number of events in Sydney, Melbourne and New Zealand to mark PAW which will feature our special guest for the week, Professor Frank Cate.&lt;br&gt;Times, venues and topics for each event will be confirmed</td>
<td>Prices for iappANZ and non-members TBC</td>
</tr>
<tr>
<td><strong>Monday 18 &amp; Tuesday 19 May</strong>&lt;br&gt;Museum of New Zealand&lt;br&gt;Te Papa Tongarewa&lt;br&gt;Cable Street&lt;br&gt;Wellington</td>
<td><strong>Identity Conference 2015, New Zealand</strong>&lt;br&gt;<em>Enabling digital identity and privacy in a connected world</em>&lt;br&gt;&lt;br&gt;Workstream topics and speakers:&lt;br&gt;• Service transformation (1)&lt;br&gt;• Cybersecurity&lt;br&gt;• Data analytics&lt;br&gt;• Privacy-by-design&lt;br&gt;• Service transformation (2)&lt;br&gt;• Cybercrime</td>
<td>The Early Bird rate is available until <strong>Monday 23 March 2015</strong>&lt;br&gt;For full registration details and to register online, visit the <a href="http://www.oaic.gov.au/news-and-events/privacy-awareness-week/what's-on-in-2015">conference website</a></td>
</tr>
</tbody>
</table>
- Transparency and digital citizenship
- The world of sensors and the Internet of Things

Confirmed workstream speakers are:
- Richard Foy, Department of Internal Affairs
- Vikram Kumar, Swerl IO Ltd
- Bianca Mueller, LawDownUnder
- Roger Dennis, Sensing City
- Dave Lacy, ID Care
- Evan Stubbs, SAS
- Ross Hughson, My Info Safe
- Kathryn Dalziel, Taylor Shaw
- Laura Bell, SafeStack

The full conference programme will be published soon.
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.

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 center in Australia or New Zealand.

Our contact details

*Privacy Unbound* is the journal of the International Association of Privacy Professionals, Australia-New Zealand (iappANZ), PO Box 193, Surrey Hills, Victoria 3127, Australia (http://www.iappanz.org/)

If you have content that you would like to submit for publication, please contact the Editors:

**Veronica Scott** (veronica.scott@minterellison.com)
**Carolyn Lidgerwood** (carolyn.lidgerwood@riotinto.com)

*Please note that none of the content published in the Journal should be taken as legal or any other professional advice.*