President’s Letter

By Anna Kuperman
President
M: 0419 803 263

Dear Members

Happy mid-year to all our readers! I would like to acknowledge and promote NAIDOC Week being celebrated in the first full week of July in Australia. It is a time to celebrate Aboriginal and Torres Strait Islander cultures and an opportunity to recognise the contributions that Indigenous Australians make to our country and our society. The theme this year is about Aboriginal and Torres Strait Islander peoples’ strong spiritual and cultural connection to land and sea. It is an opportunity to pay respects to country; honour those who work tirelessly on preserving land, sea and culture and to share the stories of many sites of significance or sacred places with the nation. I have enjoyed some great experiences around Sydney during the July school holidays, especially at The Rocks & Australian National Maritime Museum. I encourage you to find out what’s happening locally this week and next.

Turning to another exciting event on the horizon, the date for PRIVACY@WORK 2015 has been announced and apologies for filling your mailboxes so early but we want to get this early into your diaries and ensure that you can benefit from the Early Bird Rate which is an incredible deal. Our keynote speakers have been confirmed and they are an impressive lot – as always! I have great pleasure in introducing you to our keynotes below.

- **Bojana Bellamy (UK)** – President, Centre for Information Policy Leadership, Hunton & Williams LLP, UK. Bojana has over 20 years data protection and privacy executive experience and a deep knowledge of global data privacy and cybersecurity law, compliance and policy. The Centre is a global information policy think tank and leader in global information policy, privacy and cybersecurity.
- **Marie Shroff (NZ)** - pre-eminent privacy thought leader, former New Zealand Privacy Commissioner providing independent comment on significant personal information policies and issues and iappANZ Privacy Hall of Fame inductee.
- **Hilary Wandall (USA)** – Assoc. Vice President, Compliance + Chief Privacy Officer, Merck global health care company
operating in 140 countries. She has broad multi-disciplinary experience in HIV research, genetic and cellular toxicology, internet marketing, corporate law, ethics and compliance, and privacy and data protection.

For our New Zealand members, your New Zealand sub-committee has been working exceptionally hard to pull together great events later in July on Risk Management with an equally impressive line-up of local experts. Spaces filled for these events before our GM had time to advise the Board of the event promotion going live. Truly impressed with the growing level of engagement we are experiencing and anticipate much more in months to come.

That's all from me – keep watching for more announcements on the PRIVACY@WORK program.

Anna Kuperman
President
M: 0419803263
This month’s Privacy Unbound kicks off with Anna von Dietze outlining the progress made in the EU data protection reform process with the Council of Ministers of the European Union agreeing on its favoured draft of the General Data Protection Regulation (GDPR). The GDPR will significantly change the EU privacy landscape and require businesses to reconsider, and most likely change, their privacy practices. As an Australian or New Zealand privacy practitioner, now is the time to understand the impact of the changes introduced by the GDPR.

Australian Privacy Commissioner Timothy Pilgrim shares the view from the road as he visits Hong Kong to attend the 43rd Asia Pacific Privacy Authorities (APPA) Forum. Timothy outlines this year’s emerging regional issues and their significance for APPA and his Office.

On page 11, we profile Charles Alexander. Charles is a stalwart of the Australian privacy profession, founder of the privacy team at Minter Ellison Lawyers in Sydney and member of iappANZ. Charles has made a significant contribution to the profession through his involvement in the Privacy Committee of the Business Law Section of the Law Council of Australia. Read this article to find out what drew Charles into the privacy profession and what he sees as the biggest challenges for lawyers working in the field. I’d like to personally thank Charles for leading me into the world of privacy as my first supervisor.

Marta Ganko outlines key insights from the inaugural Deloitte Privacy Index, which sought to determine how leading consumer brands in the Australian market performed against privacy best practice. A survey of 1000 Australian consumers was supplemented by website and media analysis to reach a view on which industries and which entities performed best.

This month we have case notes from the two sides of the Tasman:

- A recent decision of New Zealand’s Human Rights Review Tribunal (Taylor v Orcon Limited [2015] NZHRRT 15) emphasises the obligations on agencies to ensure the accuracy of any personal information that is disclosed to debt collectors and credit reporting agencies. Ella Biggs and Steven Li explain how this decision is a timely reminder to all organisations of their obligations under the New Zealand Privacy Act; and

- In her outline of Ben Grubb and Telstra Corporation Limited [2015] AICmr 35 (1 May 2015), iappANZ Board Director Olga Ganopolsky recaps on the decision that has rocked the Australian privacy community and clarifies why the determination remains pertinent under Australia’s current privacy regime.

Will any of these authors be the winner of this year’s writing prize? If you’d like to know (and perhaps judge them for yourself), turn to page 21 for the rules!

Last but not least, this is your cue to get your early bird ticket to the year’s biggest and most memorable privacy event, iappANZ’s annual privacy summit “PRIVACY@WORK”. This year we’ll take over Zinc, Federation Square in Melbourne to bring you world leading keynote speakers, Bojana Bellamy, Marie Shroff and Hilary Wandall as well as a raft of amazing people from all walks of privacy life and beyond. Turn to page 24 for information on how to get your early bird ticket.

We hope you enjoy this edition of Privacy Unbound.

Melanie
A message about iappANZ membership:

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 global body, the International Association of Privacy Professionals (iapp), 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.

You can access benefits available to you through your iapp account. 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.

In this context, 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 emma.heath@iappanz.org. I hope that access to these additional privacy resources will be of benefit to your work as a privacy professional.

Increase in membership fees from 1 August 2015

Please note that iappANZ is introducing a membership fee increase and a new tiered fee structure as of 1 August 2015. Members who would like to take advantage of the current membership fee need to complete their membership renewal by 31 July, 2015.

More details are on page 23 of this issue of the journal. Please email admin@iappanz.org if you have membership queries.

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&goback=qdr_1281574752237_1

Follow us on Twitter at: https://twitter.com/iappANZ
EU data protection reforms - on the home stretch

by Anna von Dietze

On 15 June 2015, a significant milestone was reached in the EU data protection reform process when the Council of Ministers of the European Union (“Council”) agreed on its favoured draft of the General Data Protection Regulation ("GDPR"). With the GDPR widely expected to set a new gold standard for privacy and privacy increasingly becoming a global challenge, now is a good time for Australian and New Zealand privacy professionals to turn their mind to the European privacy reforms which are set to gain momentum in the second half of 2015.

Non-Europeans can often find the European legislative process somewhat mystifying – so in this article, I explain the shift from a data protection directive to a regulation and provide a summary of the legislative process to date as well as the steps ahead. I also briefly outline some of the major concepts and provisions of the GDPR.

From directive to regulation

Presently, the EU Data Protection Directive 95/46/EC (“Directive”) is the legal instrument setting out the data protection principles and obligations to be implemented into national laws by the 28 EU member states. A directive is a legislative act which sets out, in a rather abstract form, the general goals to be achieved by all member states through national implementing legislation. As the member states have a great deal of freedom in deciding how to transpose any given directive into national law, generally, significant divergences exist between the relevant national laws, as is the case with the Directive.

These divergences, coupled with the view that the Data Protection Directive is no longer meeting the challenges of technological developments and globalisation, prompted the European Commission ("Commission")¹ to conclude in November 2010 that the Directive required revision. Extensive consultations followed. In January 2012, the Commission (which has a quasi-monopoly for initiating EU legislation) released its legislative proposal recommending that the Directive be replaced by the GDPR².

In contrast to a directive, a regulation is a binding legislative act that is directly applicable in each of the 28 EU member states without requiring national implementing legislation. Naturally, therefore a regulation guarantees a greater level of harmonisation across the EU – and this goes some way towards explaining why it has taken three and a half years to get this far.

The GDPR manoeuvring its way through the EU law making process

Once finalised within the Commission in 2012, the GDPR proposal was transmitted simultaneously to the European Parliament ("Parliament") which represents the EU citizens, and the Council which represents the EU member states. It entered the so-called “ordinary legislative procedure” meaning that the Parliament and Council: having equal rights and obligations - need to jointly adopt the legislation by eventually approving an identical text. This process involves up to three readings in each of the two institutions as well as informal inter-institutional negotiations, called “trilogues”.

During Parliament’s first reading of the GDPR proposal, several parliamentary committees thoroughly reviewed the Commission’s proposal, issued opinions and suggested amendments. In January 2013, the Civil Liberties, Justice and Home Affairs Committee (the lead committee) through its lead rapporteur (MEP Albrecht³) issued a draft report generally supporting the Commission’s reform proposal but nonetheless suggesting 350 amendments to the Commission’s final text. This report formed the basis for further discussions in Parliament and, in March 2014, having considered a total of almost 4000 amendments tabled by members of Parliament (which shows the enormous level of interest and lobbying in relation to the GDPR), Parliament formally adopted its compromise text⁴ of the GDPR which was then forwarded to Council for consideration.

---

¹ The Commission is the EU’s executive body. It represents the interests of the EU as a whole (as opposed to representing the interests of individual countries). The Commission is composed of 28 Commissioners (one from each member state) each assigned responsibility for a particular policy area.

² The proposal also stipulates that in parallel to the GDPR, a directive for the processing of personal information in the law enforcement context be adopted. But this directive is outside the scope of this article.

³ MEP means Member of the European Parliament. A lead rapporteur of a parliamentary committee is responsible for drawing up a draft report on behalf of his/her committee suggesting amendments to a proposed text and plays a lead role in the various stages of the legislative procedure.

While Council had already been working on the Commission’s proposal in parallel to Parliament and, throughout 2013 issued several papers, reports and proposed amendments, it could only formally conduct its first reading after having received Parliament’s first reading position. Since then, during five meetings between June 2014 and June 2015, Council has reached its position on each of the chapters of the GDPR under the mantra that “nothing is agreed until everything is agreed” (which is often referred to as the “partial-general approach”). On 15 June this year, Council finally reached its long-awaited “general approach” when it adopted its position on the last outstanding chapters of the GDPR⁵. Given that Council represents the interests of the 28 member states, reaching this general approach was a difficult process with the one-stop-shop principle and the consistency mechanism proving as major sticking points.

The Council needed to reach this “general approach” before the next phase of the legislative process could commence. Now that Council has reached its general approach, Council and Parliament, with the participation of the Commission, can proceed to negotiate to reach final agreement on the text of the GDPR in the so-called “trilogue” discussions.

During the trilogue, representatives of the three institutions will meet several times to discuss the various chapters of the GDPR in order to agree a package of amendments acceptable to both Council and Parliament, with the Commission acting as mediator. If Council and Parliament succeed in agreeing a final text of the GDPR during these trilogue discussions, each of the three institutions then has to formally approve such agreement. If the trilogues do not result in a compromise text being agreed, the proposal will enter the next reading stage and the legislative process could go on for much longer.

Parliament has issued an ambitious draft timetable for the trilogue discussions. The first trilogue meeting took place on 24 June 2015 and will be followed by five further trilogue meetings scheduled between now and December 2015. So, the aim is clearly to reach final agreement on the GDPR by the end of 2015. But once formally adopted, the GDPR is expected to only come into effect after a two-year transitional period.

### Major concepts and provisions of the GDPR

As significant divergences still exist between the respective Commission, Parliament and Council drafts of the GDPR, it is too early to predict how the final version of the GDPR (which will apply to both the private and public sectors) will shape up. In general, Parliament tends to favour strong rights for individuals while Council tends to take a more business-friendly approach.

Nonetheless, certain key concepts and principles of the GDPR have emerged during the process so far, including the following:

- **Territorial scope** – The European legislative institutions largely agree that the GDPR should have a wide extra-territorial scope. It will apply to the processing activities of businesses established within the EU, as well as to the processing activities of non-EU businesses offering goods or services to individuals within the EU or monitoring their behaviour to the extent personal data of EU subjects is processed. This expected to be a significant change for non-EU companies with EU customers.

- **Enforcement powers** – National data protection authorities (“DPAs”) will be equipped with much broader enforcement powers, including powers to impose fines of up to €1 million or 2% of an annual worldwide turnover for compliance failures (or higher if Parliament prevails on this point). This is significantly higher than the levels of fines currently available under national legislation and is expected to be a major compliance driver. Individuals will also have a right to compensation for damages suffered as a result of processing carried out in breach of the GDPR.

- **One-Stop-Shop and consistency mechanism** – Where a business has multiple establishments in the EU, the DPA of the country of the business’ main establishment is the “lead DPA” and will regulate all of the business data processing activities throughout the EU as a “one-stop-shop”. However, in order to ensure consistent enforcement of the GDPR across the EU, where an enforcement action affects processing activities in more than one member state, (subject to an urgency exception) the lead DPA needs to coordinate with the DPAs of the other affected member states (and potentially the European Data Protection Board) in order to reach a consensus regarding the enforcement measures. As these are two of the most contentious concepts of the GDPR, their details are still unclear. The requirement for consensus may also impact on how quickly the lead DPA can respond and have an impact on the timing of regulatory investigations.

- **Accountability** – The principle of accountability will strongly feature in the GDPR. In order to comply with this principle, businesses will, for example, need to build a culture of privacy from the top down, follow a privacy-by-design approach, implement certain security measures, conduct audits and privacy impact assessments (“PIAs”), maintain internal records

---

documenting privacy measures and appoint DPOs (although there is still considerable disagreement as to when the requirement to appoint a DPO will apply). These concepts should be familiar to Australian privacy professionals, following the commencement of new Australian Privacy Principle 1 last year and the launch of the Australian Privacy Management Framework a couple of months ago.

- **Stronger rights for data subjects** – Under the GDPR, data subjects will retain their existing rights to access, rectification, erasure and objection (subject to minor amendments generally in favour of data subjects) but will also obtain new rights, including rights of data portability, the right to be forgotten and certain rights in relation to profiling. In order to foster transparency, the GDPR also sets out stricter requirements for privacy notices which will inevitably become more detailed. On the flipside, only one notice will be required across the EU.

- **Data processors** – Unlike the Directive which only applies directly to data controllers, the GDPR will impose certain obligations, restrictions and sanctions directly on data processors, including obligations to implement appropriate security measures, conduct PIAs, appoint DPOs, document processing operations, etc. The GDPR further prescribes the terms to be included in written controller/processor contracts. This is a significant change, which may surprise Australian and New Zealand privacy professionals, given that companies processing personal data on behalf of other companies have long been directly regulated under privacy legislation in this part of the world.

- **Valid grounds for processing** – Under the Directive, each data processing activity requires a valid ground justifying such processing. While this concept, as well as the processing grounds (such as consent, performance of a contract, fulfillment of a legal requirement and legitimate controller interests), will be retained under the GDPR, demonstrating that a processing ground exists will become harder in some instances. For instance, the requirements in relation to consent will be significantly stricter. Further, the definition of “sensitive information” is expanded to include genetic data and data concerning criminal activities. Also the conditions on which sensitive data may be processed, will be narrowed.

- **International transfers** – The Directive heavily restricts the transfer of personal data from the EU to non-EU countries. This can cause headaches for Australian privacy professionals wishing to ensure that transfers of EU personal data to Australia are lawful (while looking wistfully across the Tasman to New Zealand with its “EU adequacy”). These restrictions will be retained under the GDPR in principle, subject to small changes which will in general be welcomed by businesses. For example, transfers based on EU Model clauses or Binding Corporate Rules will no longer need to be notified to, or authorised by, local DPAs which will significantly reduce the cost and resources involved. Further, in addition to making adequacy decisions in relation to countries, the Commission will be able to make adequacy decisions in relation to specific territories or industry sectors within a country which could significantly broaden the list of locations to which EU data may be transferred (e.g., it will be possible to designate single US states as offering an adequate level of protection). Finally, the GDPR adds to the existing derogations with respect to ex-EU transfers by permitting limited data transfers outside the EU where necessary for the legitimate interests of the controller/processor under certain strict conditions.

- **Data breaches** – Under the GDPR, there will be a general obligation to report data breaches to DPAs and, sometimes, affected individuals. Currently, only a few member states have mandatory breach notification obligations, while others encourage voluntary reporting of serious data breaches (if that). Again, this development is in line with developments in other parts of the world, including Canada and Australia.

- **Risk-based approach** – Council is pushing hard for the GDPR to take a risk-based approach, meaning that compliance measures will need to be proportionate to the specific processing activities and related risks. This will allow businesses to exercise discretion in determining how they will comply with their obligations – which would be a welcome development from a business point of view. However, Parliament is likely to try to limit the effect of the risk-based approach to prevent it from undermining privacy protection.

- **Exceptions for SMEs** – Importantly, SMEs will be exempt from a number of the obligations under the GDPR (a benefit not currently available under the Directive). Most importantly, SMEs will be exempt from the obligation to appoint DPOs, provided data processing is not their core business activity and they will not need to conduct PIAs unless specific risks arise.
Final remarks

With trilogues underway, the heavily lobbied and negotiated GDPR has hopefully entered the home stretch. While not throwing overboard the existing core principles of data protection, the GDPR will significantly change the EU privacy landscape and require businesses to reconsider, and most likely change, their privacy practices. With Parliament and Council coming from very different angles, the political negotiations are not over yet. But over the coming months, we should see where the parties will land on the contentious issues and by the end of 2015 – unless things go terribly wrong - we should have a pretty clear picture of what the GDPR will look like, and what impact it might have on the development of global approaches to privacy and data protection.

Anna von Dietze, CIPP/E, CIPM & CIPP/US is a German-born solicitor qualified in Germany, Australia as well as England & Wales with professional experience in both Australia and Germany. Anna’s areas of expertise include international data protection law, contract law, e-commerce and consumer protection law. Anna is currently on leave of absence from the Sydney office of a leading international law firm, due to a relocation to Germany and family commitments.
Report from Hong Kong:
On the road with the Australian Privacy Commissioner

By Timothy Pilgrim

I recently attended the 43rd Asia Pacific Privacy Authorities (APPA) Forum which was held in Hong Kong. While there, I also addressed a number of conferences, including the International Conference on Big Data from a Privacy Perspective, the 7th Annual Sedona Conference International Programme on Cross-Border Discovery and Data Protection Laws, and the Internet Society of Hong Kong’s Privacy and Innovation conference. This was an excellent opportunity to speak to, and hear from, some influential thinkers in the privacy arena.

The APPA meeting was attended by representatives from 15 privacy authorities and included observers from Government, industry and civil society. The US Federal Communications Commission attended the meeting for the first time, creating important links for both APPA generally and Australia specifically, into communications regulation in the US, furthering our already productive relationship with the Federal Trade Commission, which is a member of APPA.

The meeting discussed a wide range of current privacy issues, and particularly focussed on common themes that have emerged across the region, including big data, legal reforms, law enforcement, mandatory data breach notification, privacy training as well as child and youth privacy programmes. Members also shared a wide range of reports on investigations and data breaches.

During the two days of the APPA meeting, we continued discussions on the importance of big data in the current privacy environment, and we agreed that the Office of the Australian Information Commissioner will take the lead in progressing the APPA region’s examination of big data and privacy.

Big data is one of the key challenges for privacy moving forward, as I outlined in my speech to the International Conference on Big Data from a Privacy Perspective. Big data is big business – it is estimated that the amount of data globally is growing by fifty percent each year, with ninety percent of the world’s data generated in the last two years. And all this data we are creating is increasingly valuable and sought after.

Big data analytics has great power to amass, aggregate and analyse this data. As a result, big data has the potential to bring about enormous social and economic benefits. But as a regulator I, and others, can see that with all the opportunities of this new technology also comes the potential to significantly impinge on individual privacy.

Data protection authorities have already signalled an intention, through the Mauritius Resolution on Big Data and the Declaration on the Internet of Things (IoT), to closely monitor these developments, and this is reflected in the APPA Forum’s engagement with this issue. In our involvement in this issue, we recognise the benefits that can come from both big data and the IoT in terms of health management and disease prevention, emergency responses, crime prevention and even traffic management, but also the challenges that are associated with these new technologies.
The conferences that I attended during the week raised a range of issues, but key among them were challenges around the intersection of innovation and privacy, and looking at whether privacy law restricts innovation. And my answer to that is no, it shouldn't. Big data is itself an innovation, and if we can innovate to use data that we never previously had access to, we can innovate to embed and strengthen privacy at the same time. I think it's fair to say that social innovation is not true innovation if it harms the rights and freedoms of the people it is aiming to serve. And there are so many ways to develop and enhance interactions between big data and privacy — we just have to work to make them a reality.

Timothy Pilgrim is the Australian Privacy Commissioner
iappANZ member profile: Charles Alexander

In this month’s edition we profile Charles Alexander. Charles is a stalwart of the Australian privacy profession, founder of the privacy team at Minter Ellison Lawyers in Sydney and member of iappANZ.

In 2002-2003, Charles was instrumental in the establishment of what is now the Privacy Committee of the Business Law Section of the Law Council of Australia. Since then, Charles has been actively involved in that Committee, which plays an important role in national debates about the development of privacy law.

Charles has recently retired from the partnership of Minter Ellison, where he has worked for the past 29 years (back to when the firm was Minter Simpson). At Minter Ellison, Charles represented privacy clients across many different industry sectors, including in education, aviation and media. Charles continues to advise on privacy issues, including as a consultant with Minter Ellison (part time) and also for the Association for Independent Schools.

We managed to convince Charles that being profiled in this month’s issue of the journal was a good idea (this took some doing!) Our conversation with Charles went something like this ....

How did you get into privacy law? Was it choice or chance?
CA: It was a bit of both! In 2000 after the private sector amendments were made to the Privacy Act, it became obvious that privacy law was something we should be thinking about and developing as a practice area. I raised this with my partnership – and the response was “do you want to do it?” My answer was yes! This was an interesting new area of law that clients were going to need help with.

What aspects of the Privacy Act do you get asked about the most?
CA: Recently, questions about overseas transfers have been a constant. There are also many questions about what you need to do to comply with the collection notice provisions in APP5, and also what you need to include in your privacy policies and procedures under APP1. Of course, if you go further back, the questions were even more basic: “tell us what we need to do?”

What (if any) features of overseas privacy regimes would you like to see as part of our law here?
CA: That’s an easy question – I’d like to see the distinction of ‘data controller’ and ‘data processor’ as part of our laws here. It makes a lot of sense. The absence of this type of distinction in our laws makes the application of the law more confusing for many people.

What do you see as the biggest challenges for privacy professionals right now?
CA: One challenge is constantly changing technology which makes things possible that weren’t before. Another big challenge is determining what is “reasonable”; there are a lot of situations that require judgment calls, and minds can differ about this. ‘Black letter’ lawyers would find it very hard to understand how we privacy professionals approach this issue, where so much depends on the circumstances. I do think that the Privacy Commissioner has been as helpful as he can in trying to provide guidance in this area, but you still need to make judgement calls.

What tips for young players?
CA: Before you can start advising, you need to work out what personal information you’re collecting, and what you’re doing with it. Undertake that factual investigation. You can’t put in effective measures to comply with the Privacy Act if you don’t know what you’ve got and how you’re using it. A good professional organisation will devote time and effort to undertaking that analysis – and that’s where you need to start.
Can you share with us something quirky about you?

CA: I like open plan offices! Putting a team together in one area brings about a sense of community and oneness – and we can all pop up like meerkats when we have something to share. After all these years in offices, I find myself a convert to the open plan!

Charles Alexander in conversation with Carolyn Lidgerwood. After 30 June, Charles can be contacted at Cds.alexander@icloud.com
Transparency is opportunity

by Marta Ganko

“Privacy is today where security was a decade ago. It’s bolted-on rather than built-in from the beginning.”
Gartner Inc, Privacy Hype Cycle, 18 July 2014

Privacy compliance is difficult to assess given the constantly changing regulatory landscape of privacy. The traditional compliance-only approach to privacy within organisations is now being challenged not only through increased consumer awareness, but also by regulators who are encouraging better governance and privacy practices within organisations, including building privacy into the design of new products and solutions.

Organisations are also facing an ethical challenge of ensuring that the value of personal information that can be obtained from consumers is realised, while ensuring that customer privacy expectations are maintained alongside a fulfilling customer experience.

Deloitte set out to determine how leading consumer brands in the Australian market perform against privacy best practice by surveying over 1000 Australian consumers. This survey was supplemented by website and media analysis. The resulting Privacy Index also includes an insight into internal practices within organisations from the brands across 11 industry sectors.

**Deloitte Australian Privacy Index 2015 Ranking**

The best performing industries assessed by the inaugural Deloitte Privacy Index were transparent – a key indicator of trust. They also had the best governance policies and procedures, and were up to date with current regulatory change.

The best performing industries or sectors are listed below:

1. Government
2. Banking & Finance
3. Social Media
4. Health & Fitness
5. Retail
6. Insurance
7. Technology
8. Energy
9. Travel & Transport (airlines, agencies, hotels, taxis)
10. Telecommunications (mobile, internet, phone)

What were the strengths of the organisations that did well?

Organisations that did well have:

- an online privacy policy which is both easily understood by the consumer and layered, and which is often supported with extra materials
- fewer third party cookies tracking consumer behaviour
- cookies which do not stay on the consumer’s device for a long time
- a trusted brand according to consumers
- few or no major privacy events reported in the media.
Key Themes

**Transparency builds trust**

- Of the just under 20% of survey respondents notified of a breach, 34% said they trusted that organisation more.
- 73% of this cohort who received a privacy breach notification did not trust the organisation any less following the notification.

**Tendency towards disconnect between reality and consumer’s perception**

- While social media brands are not viewed favourably by consumers, they tend to be more transparent regarding how they use the information they collect.
- While banking & finance, and insurance industries are perceived positively by consumers, other industries did better in the website analysis due to the transparency of their information use and education on how they use that information.

**Organisations are beginning to put privacy governance structures in place**

- More than 75% of responding organisations indicate they have a privacy officer role.
- >50% of these organisations have performed at least one Privacy Impact Assessment.
- Of these organisations, 60% have performed more than five assessments.

**Other key findings**

- Australian consumers are most concerned about their credit card details (67%), their passport number (46%), and their driver’s licence number (43%). They are also most reluctant to share these three items due to their sensitivity.

- Banking & finance and government are the top two most trusted industries when it comes to safeguarding personal information.

- The insurance industry is trusted less with personal information than banking & finance.

- Overall 67% of the 1000+ consumers surveyed have never had a privacy issue with a brand.

- The remaining 33% have had a privacy issue with an organisation, but only 14% have complained.

- Social media and the telecommunications sectors accounted for 58% of the complaints regarding privacy.

- Social media had 32% of the complaints and 28% of people listed the same social media organisation as the organisation they trusted the least with their personal information.

**Trends**

*Notifying customers of data breaches*

- The survey results show that consumer trust is built through transparency. This is especially pertinent given the legislative developments regarding mandatory data breach notifications. Organisations can begin positioning themselves by implementing a governance structure and framework to monitor and measure how information is used across the organisation.
Big data insights versus consumer ethics

- Deriving new insights and opportunities from an organisation’s available data, is an important focus for many organisations. However, when does that intelligence go too far in terms of what a consumer would reasonably expect, based on the original information they provided?

Privacy compliance to Privacy-by-design

- Many organisations have worked towards complying with the updated privacy requirements. However, a pure compliance approach may be risky. A better way to meet privacy requirements over the longer term is to embed privacy into everything an organisation does.

Getting the privacy basics right

- Despite a steady increase in serious cyber-attacks, the vast majority of reported data breaches involve accidental loss or release of data, communications being sent to the wrong person, missing basic security controls and a lack of training and awareness of staff. Organisations must be in a position to justify the preventative measures they have taken, so that if they were to have a data breach they are able to confidently say, they took reasonable action to prevent it.

Getting started

Organisations can begin by assessing how customer data is managed as well as their internal privacy capabilities. To start the conversation in your organisations, here are a few thoughts:

- Does the way you use customer information align with your organisation’s values and/or strategy?
- How does your organisation achieve transparency to customers about what it does with personal information?
- Would a customer expect you to use or disclose their information in the way that you do?
- How do you monitor privacy compliance, customer expectations and the changing privacy regulatory landscape?

Marta Ganko is a Privacy SME at Deloitte Australia. Marta can be contacted at: mganko@deloitte.com.au.


If you would like further information about the Deloitte Australian Privacy Index 2015 or privacy in general please contact Tommy Viljoen, partner in Risk Advisory.
Case Note from New Zealand:

Another large damages award from the Human Rights Review Tribunal:

*Taylor v Orcon Limited [2015] NZHRRT 15*

by Ella Biggs and Steven Li

A recent decision of the Human Rights Review Tribunal (the Tribunal) emphasises the obligations on agencies to ensure the accuracy of any personal information that is disclosed to debt collectors and credit reporting agencies. This decision is a timely reminder to all organisations of their obligations under the New Zealand Privacy Act 1993 (the Act).

**Facts**

Orcon, a telecommunications company, issued a bill to a customer, which the customer disputed and refused to pay. Without resolving the customer’s dispute, Orcon disclosed the customer’s personal information to a debt collection agency and, subsequently, to a credit reporting agency. The debt was registered on the customer’s credit report by Veda.

The customer was unable to secure rental accommodation for his family or secure a loan from a finance company (at least partly) as a result of his negative credit report. The customer brought proceedings against Orcon on the grounds that the use of inaccurate personal information amounted to an interference with his privacy.

For a breach of an information privacy principle to amount to a breach of the Act, it needs to amount of an “interference with privacy” in accordance with section 66 of the Privacy Act, which requires the following:

66 Interference with privacy
(1) … an action is an interference with the privacy of an individual if, and only if, —
(a) in relation to that individual,—
   (i) the action breaches an information privacy principle; ….and
(b) in the opinion of the Commissioner or, as the case may be, the Tribunal, the action—
   (i) has caused, or may cause, loss, detriment, damage, or injury to that individual; or
   (ii) has adversely affected, or may adversely affect, the rights, benefits, privileges, obligations, or interests of that individual; or
   (iii) has resulted in, or may result in, significant humiliation, significant loss of dignity, or significant injury to the feelings of that individual.

**Outcome**

The Tribunal found in favour of the customer.

The Tribunal found that Orcon breached information privacy principle 8 by disclosing inaccurate and disputed information about a customer. Principle 8 requires agencies to take reasonable steps before the use of customers’ personal information to ensure that the information is accurate, accurate, up to date, relevant and not misleading.

The Tribunal was particularly critical of Orcon providing inaccurate personal information to a debt collection and credit reporting agency. The Tribunal emphasised that, where an organisation provides personal information to a debt collection or a credit reporting agency, it bears a heavy burden to ensure the information is accurate, up to date, and not misleading. This is because there is little or no opportunity for an individual to challenge this information until after the adverse credit report had been published (for example, in this case, the customer was only made aware of the disclosure of inaccurate information by Orcon once their application for rental accommodation was denied).

The Tribunal also found that the breach of principle 8 amounted to an interference with the customer’s privacy. This was because Orcon’s failure to ensure the accuracy of the customer’s personal information (that he allegedly owed money to Orcon) led directly to the customer’s rental applications being denied.

---

*The information privacy principles are set out in section 6 of the Privacy Act (NZ).*
The customer was awarded $25,000 in damages and Orcon was ordered to provide its staff with privacy training. The $25,000 comprised $10,000 for the loss of the benefit of the customer’s good credit rating, and $15,000 for humiliation, loss of dignity, and injury to feelings.

Analysis
This decision emphasises the obligations on agencies to ensure that any personal information disclosed to credit reporting agencies is accurate and up to date. It appears from this decision that the Tribunal will take a particularly strong approach to protect individuals from inaccurate credit reports – as illustrated by the large damages award.

This decision is also significant for its discussion of causation, when determining whether Orcon’s breach of principle 8 amounted to an interference with the customer’s privacy. A clear causation standard has not previously been recognised under the Privacy Act.

In its decision, the Tribunal found that it is not necessary for the breach to be the sole, main, direct, indirect, or “but for” cause of the loss or harm to the individual. The Tribunal concluded that the breach must have had (or may have had) a real influence on the occurrence (or possible occurrence) of the particular form of harm.

Following the Tribunal’s decision, the Commissioner commented that the Tribunal’s decision to set the causation standard at an “attainable” level will mean that it “will be getting tougher on respondents who have breached one of the [privacy] principles” under the Act.²

Ella Biggs and Steven Li work as solicitors in the litigation team at Chapman Tripp, Wellington. Ella is also a New Zealand sub-committee member of iappANZ.

² See the statement on the Privacy Commissioner’s blog, available at: https://www.privacy.org.nz/blog/taylor-v-orcon/
Case Note from Australia:

**Definition of personal information and metadata**


by Olga Ganopolsky

On 1 May 2015, the Privacy Commissioner published his Determination in this case, finding that Telstra Corporation Limited (Telstra) interfered with the complainant's privacy by failing to provide the complainant with access to his personal information held by Telstra and therefore in breach of National Privacy Principle (NPP) 6.1 (now in Australian Privacy Principle 12.1) of the *Privacy Act 1988* (Cth) (the *Privacy Act*).

Telstra was ordered to provide the complainant with access to his personal information held by Telstra in accordance with his request (except the inbound call numbers).

What began as a reasonably typical access request became an important decision on the what personal information means under section 6 of the Privacy Act (as it stood at the time of the access request and the subsequent complaint - i.e. prior to the reforms to the Privacy Act that came into effect on 12 March 2014 including the amended definition of personal information).

This case note sets out why the determination remains pertinent under the current privacy regime.

**Background**

On 15 June 2013 the complainant claimed a right of access under the *Privacy Act* to 'all the metadata information Telstra has stored' about him in relation to his mobile phone service, including (but not limited to) cell tower logs, inbound call and text details, duration of data sessions and telephone calls and the URLs of websites visited. The request specifically addressed metadata, with Mr Grubb stating that he wanted information that would 'include which cell tower I’m connected to at any given time, the mobile phone number of a text I have received and the time it was received, who is calling and who I’ve called and so on. I assume estimated longitude and latitude positions would be stored too'.

Telstra agreed that Mr Grubb could access outbound mobile call details and the length of his data usage sessions via online billing. Telstra refused to provide information regarding location and details of the numbers that called and sent SMS to Mr Grubb's mobile phone service. Over a period of 18 months Telstra agreed to release some additional items of information. Telstra maintained that longitude and latitude data and data generated on the Telstra network is not personal information within the meaning of the Privacy Act and should therefore not be provided as part of an access request under the Privacy Act.

**The law and the arguments**

Before the 12 March 2014 reforms, the definition of ‘personal information’ was “information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion”.

The issue was whether metadata was personal information and specifically whether the information was of such a character so as to be ‘about an individual’. Detailed evidence was provided by Telstra as to what constitutes Network data and how it is used by Telstra.

---

1 Under the post reform (post 12 March 2014) section 6 of the Privacy Act provides that personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:
   (a) whether the information or opinion is true or not; and
   (b) whether the information or opinion is recorded in a material form or not

2 Telstra used the metadata and communication data interchangeably and defined it as ‘information about an electronic communication – a footprint left after accessing the internet, sending an email, or making a phone call. It might, for example, include customer registration details, the date, time and duration of a communication, the phone number or email address of the sender and recipient, the amount of data up/downloaded, or the location of a mobile device from which a communication was made’.
Telstra expressly noted that, Internet Protocol (IP) address information, Uniform Resource Locator (URL) information, Cell tower location information beyond the cell tower location were not items of personal information as defined.

Telstra argued that:

- customers’ identity is not apparent from Telstra’s network data nor can it reasonably be ascertained from that metadata;
- none of the network data is linked in such a way as to identify an individual customer and that “it would be very difficult and require a great deal of forensic effort for Telstra to identify and gather the network data that relates to [the complainant]. There is no likely scenario in which Telstra would do this in the ordinary course of its business”.

This argument was rejected by the Privacy Commissioner on the grounds that:

- the term ‘about an individual’ may apply to other information about that individual, including information about who has called the complainant. Calls being made to the complainant’s mobile service reveal information about the complainant as well as the incoming caller;
- *The Macquarie Dictionary Online* (2013) the word “about” means “in regard to, concerning or connected with”; and
- documents which themselves do not contain any obvious features identifying an individual may take on the quality by virtue of the context to which they belong.  

### Significance of the Determination

We understand that Telstra intends to appeal the decision. Regardless of the outcome of any pending reviews or appeals, this determination will remain an important illustration of the approach being taken by data protection regulators to the scope of the definition of personal information and hence what is regulated and protected under the applicable privacy legislation.

The key impacts are:

- The scope of what is personal information will be determined by the very particular context relating to the information and its uses. In this case, it was not decisive that Telstra does not actually use the metadata to identify individuals. What was relevant was that Telstra had the technical capacity to do so and was not expressly precluded by legislation or agreement from doing so.

- The scope of the definition is expanding. noting that what is ‘about an individual’ may apply not only to an item of information that identifies the individual, but to other information about that individual. The apparent limitation in the pre-reform definition, that the ability to identify is to be assessed by reference to the information in question appears not to have been relevant. Given that the post reform definition of personal information has expressly jettisoned this limitation, the ability to identify by reference to other data or analytical tools at one’s disposal (e.g. publically available data) will remain relevant and potentially decisive.

- Just because information is ‘shared’ information about another individual, will not automatically preclude it from being about an individual in question. In this determination, the information about who is calling the complainant is personal information about the complainant.

### Conclusions

The scope of what is personal information and therefore regulated will remain a live issue for privacy practitioners and their respective clients. It will be particularly pertinent for large organisations that carry on a variety of diverse businesses and therefore collect and generate a large volume and variety of information on a daily basis as part of their ongoing business activities. The Determination has

---

1. *WL v Randwick City Council (GD)*
a profound impact on the how these organisations administer and address their respective responsibilities under the Privacy Act. This is particularly so in the post reform environment, where organisations are accountable for the personal information they hold and have a new obligation under APP 1 to 'implement practice, procedures and systems' that will ensure that the organisation complies with its obligations.

At the core of that ability to comply is the ability to determine the scope of what is to be addressed in the given practice, procedure or system addressing compliance - which, at least for now, includes metadata.

Olga Ganopolsky is General Counsel - Privacy and Data at Macquarie Group Limited. Olga is also a board member of iappANZ
iappANZ’s writing prize 2015: entries open

Entries remain open 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, Carolyn.lidgerwood@riotinto.com or emma.heath@iappanz.org 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 on 18 November 2015 in Melbourne 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).

No positions currently advertised.
Increase in iappANZ membership fees

As outlined on page 4, iappANZ is introducing a membership fee increase and a new tiered fee structure as of **1 August 2015**. Members who would like to take advantage of the current membership rates (before the increase) need to complete their membership renewal by 31 July, 2015.

The membership fees to apply from 1 August 2015 are set out below (note that fees are in **Australian dollars**):

<table>
<thead>
<tr>
<th>Membership Type</th>
<th>Fee</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard Membership</strong></td>
<td></td>
</tr>
<tr>
<td>Individual</td>
<td>$250 incl. GST</td>
</tr>
<tr>
<td>Corporate</td>
<td>$225 incl. GST per Member</td>
</tr>
<tr>
<td>3-4 Members (10% discount)</td>
<td>$675 incl. GST (3 Members)</td>
</tr>
<tr>
<td>5+ Members (15% discount)</td>
<td>$212.50 incl. GST per Member</td>
</tr>
<tr>
<td></td>
<td>$1062.50 incl. GST (5 Members)</td>
</tr>
<tr>
<td><strong>Government/Not-for-Profit/Senior (60+) Membership</strong></td>
<td></td>
</tr>
<tr>
<td>Individual</td>
<td>$225 incl. GST</td>
</tr>
<tr>
<td>Corporate</td>
<td>$202.50 incl. GST per Member</td>
</tr>
<tr>
<td>3 - 4 Members (10% discount)</td>
<td>$607.50 incl. GST (3 Members)</td>
</tr>
<tr>
<td>5+ Members (15% discount)</td>
<td>$191.25 incl. GST per Member</td>
</tr>
<tr>
<td></td>
<td>$956.25 incl. GST (5 Members)</td>
</tr>
<tr>
<td><strong>Student (University Full-time)</strong></td>
<td>First year complimentary</td>
</tr>
<tr>
<td></td>
<td>$25 for second and remaining years if full-time university study</td>
</tr>
</tbody>
</table>
SAVE THE DATE

WEDNESDAY 18 NOVEMBER, 2015, MELBOURNE

2015 iappANZ Annual Privacy Summit: Privacy@work

iappANZ is delighted to announce three world leading privacy gurus as keynote speakers:

- **Bojana Bellamy (UK)** – President, Centre for Information Policy Leadership, Hunton & Williams LLP. Bojana has over 20 years data protection and privacy executive experience. The Centre is a global information policy think tank and leader in global information policy, privacy and cybersecurity.

- **Marie Shroff (NZ)** – A pre-eminent privacy thought leader, former New Zealand Privacy Commissioner and iappANZ Privacy Hall of Fame inductee, Marie will provide independent comment on significant policy issues.

- **Hilary Wandall (USA)** – Assoc. Vice President, Compliance + Chief Privacy Officer, Merck, a global healthcare company operating in 140 countries. Hilary has broad multi-disciplinary experience in HIV research, genetic and cellular toxicology, internet marketing, corporate law, ethics and compliance, and privacy and data protection.

When: Wednesday 18 November, 9.00am – 6.30pm incl. networking time

Where: ZINC, Federation Square, Melbourne

Earlybird: Until 7 October

Details: www.iappanz.org/events

The only event of its kind in the region, the Privacy@Work Summit will provides a forum for people in the privacy arena to connect and enhance their privacy knowledge. The Summit showcases best practices, illuminates new trends and offers guidance on opportunities in the field of privacy.

Come and join us for a full day of insightful information and discussion on the key issues regarding privacy now and into the future. For more information email admin@iappanz.org
## Privacy Events

<table>
<thead>
<tr>
<th>Time, Date &amp; Location</th>
<th>Information</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AUCKLAND</strong></td>
<td>Privacy risk management – what’s it all about?</td>
<td>FREE</td>
</tr>
<tr>
<td>When: 9-11am, 21 July 2015</td>
<td>Speakers:</td>
<td>REGISTER HERE or email <a href="mailto:emma.heath@iappanz.org">emma.heath@iappanz.org</a></td>
</tr>
<tr>
<td>Where: KPMG</td>
<td>• John Edwards, Privacy Commissioner NZ</td>
<td></td>
</tr>
<tr>
<td>18 Viaduct Harbour Ave, AUCKLAND</td>
<td>• Kirk Hope, Chief Executive New Zealand Bankers’ Association</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Paul Holmes, Head of Privacy and Government Services, Accident Compensation Corporation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Arron Baker, Assistant General Manager, Strategy &amp; Assurance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Liana Bunting, Process Lead, VISION 2015, Immigration, Ministry of Business, Innovation &amp; Employment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Jon Duffy, Head of Trust and Safety, TradeMe</td>
<td></td>
</tr>
<tr>
<td><strong>WELLINGTON</strong></td>
<td>Privacy risk management – what’s it all about?</td>
<td>FREE</td>
</tr>
<tr>
<td>When: 9-10.30am, 23 July 2015</td>
<td>Speakers:</td>
<td>REGISTER HERE or email <a href="mailto:emma.heath@iappanz.org">emma.heath@iappanz.org</a></td>
</tr>
<tr>
<td>Where: KPMG, Maritime Tower</td>
<td>• John Edwards, Privacy Commissioner NZ</td>
<td></td>
</tr>
<tr>
<td>10 Customhouse Quay, WELLINGTON</td>
<td>• Kirk Hope, Chief Executive New Zealand Bankers’ Association</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Paul Holmes, Head of Privacy and Government Services, Accident Compensation Corporation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Arron Baker, Assistant General Manager, Strategy &amp; Assurance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Liana Bunting, Process Lead, VISION 2015, Immigration, Ministry of Business, Innovation &amp; Employment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Jon Duffy, Head of Trust and Safety, TradeMe</td>
<td></td>
</tr>
<tr>
<td><strong>SYDNEY</strong></td>
<td>Records &amp; Management Forum</td>
<td>iappANZ members receive a 20% discount off the standard price.</td>
</tr>
<tr>
<td>22 – 24 July, 2015</td>
<td>This Forum will showcase how you can embrace digital advancements as an integral part of your competitive strategy whilst using information management as a primary business enabler. The Forum will focus on the theme of adopting digital processes to optimise business value and feature 17 expert speakers, 11 case studies as well as 2 exclusive workshops.</td>
<td>To lock in your exclusive discount, just contact Akolade on 02 9247 6000 or email <a href="mailto:marketing@akolade.com.au">marketing@akolade.com.au</a> and reference VIP Code: EFXB1.</td>
</tr>
<tr>
<td>8.00 – 5.00pm</td>
<td>Attending and speakers include:</td>
<td></td>
</tr>
<tr>
<td>The Grace Hotel,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>77 York Street, SYDNEY</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### SYDNEY
**Wednesday 5 August 2015**
3.30pm for 4.00pm start, 7.00pm finish

Baker McKenzie Lawyers
L27, AMP Centre
50 Bridge Street, Sydney

See the full program [here](http://bit.ly/1E0KYdQ)
Click here to visit the website: [http://bit.ly/1E0KYdQ](http://bit.ly/1E0KYdQ)

### PRIVACY IN PHARMA Seminar and Q&A

Speakers include:
- **Anne-Marie Allgrove** – Partner, Baker McKenzie
- **Jessica Kanevsky** – Legal Counsel, Abbvie
- **Greer Harris** - Regional Privacy Officer, Asia Pacific, AstraZeneca

*Moderated by Malcolm Crompton*, iappANZ Founding President and Managing Director, Information Integrity Solutions

Free for iappANZ members
$99 plus GST for non-members (deductible from iappANZ member joining fee.)

Registrations – [admin@iappANZ.org](mailto:admin@iappANZ.org)

### MELBOURNE
**Tuesday 13 October 2015 to Thursday 15 October 2015.**
Venue: Atlantic Group V, Shed 14, 15 Central Pier 161 Harbour Esplanade Docklands VIC 3008

AISA National Conference
"Trust in the world of Information Security"

For details please contact info@aisa.org.au

### MELBOURNE
**All day event 8am-6pm**
**Wednesday, 18 November 2015**
Zinc at Federation Square, MELBOURNE

iappANZ annual Privacy Summit

*See page 24 for details of keynote speakers*

*Full program to be published soon!*

**Registration:**

**Earlybird (until 7 October 2015):**
iappANZ member: $637.50 incl. GST
Non-member: $857.50 incl. GST. Note that non-member registration fee includes annual iappANZ membership

---

| Katharine Stuart, Acting Director - Digital Strategy and Solutions, National Archives of Australia |
| Elizabeth Tydd, Information Commissioner & CEO, Information and Privacy Commission NSW |
| Claire Holt, Chief Health Information Manager, Portland District Health |
| Dr Monica Trujillo, Chief Medical Information Officer, UnitingCare Health |
| Kate Harrington, Director - Information Management, Office of Finance and Services NSW |
| Ben Dornier, Director, Corporate Community Services, City of Palmerston, NT |

---

### Gold Sponsors

- Commonwealth Bank
- Facebook
- Google
- Intel Security

### Silver Sponsors

- HealthLink
- HP
- Intechnique
- ITM Solutions
- E Doc
- Palantir
- Surescripts

---
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.

Our global body, 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 six specialised credentials, two of which are particularly relevant to iappANZ members, namely the Certified Information Privacy Professional/ Information Technology (CIPP/IT) and the Certified Information Privacy Manager (CIPM).

To achieve either of these credentials, you must first successfully complete the Certification Foundation. The Certification Foundation covers basic privacy and data protection concepts from a global perspective, provides the basis for a multi-faceted approach to privacy and data protection and is a foundation for the distinct iapp privacy certifications.

What about testing?

Certification testing is available to iappANZ members locally (at iapp-approved computer-based testing centres). The iapp manages certification registrations and materials, and you can set an appointment to sit your exam online at a testing centre 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.*