Privacy Unbound iappANZ

February/ March 2016

UNLOCKING THE TRUTH ABOUT PRIVACY

ISSUE 68

President's Letter

By Kate Monckton
President
M: 61 409 613 029

Dear Members

Welcome to the first edition of *Privacy Unbound* for 2016. We're only a few months in and there's already been so much happening in the privacy space. I'd like to thank everyone who has volunteered their time by writing some really engaging and interesting pieces in this edition and all the previous ones – without our members and hardworking Board Directors, none of this would be possible.

There are several workshops coming up soon across Australia and New Zealand including a series on Mandatory Data Breach Notification in Sydney, Melbourne and Brisbane. Dates and venues can be found in our Privacy Events calendar on page 23 and watch this space for news of NZ workshops very soon.

The Board is also working on its strategy and planning in the coming months, focusing on membership, sponsorship and of course this year's Summit. We are also looking at introducing a new look format to the Journal.

Check out the photo toward the end of some of our members celebrating International Privacy Day in Melbourne – see if you recognise anyone. Thanks to Grace Guinto at PwC for hosting a Privacy After Hours event to mark the day. If you have an idea for a Privacy After Hours event in your city, please let us know and we can help you get something organised.

By the time I write the next introduction for *Privacy Unbound*, I will have had the honour of attending the IAPP Global Privacy Summit in Washington DC in early April, and look forward to reporting back on the highlights and takeaways for the ANZ region. I know that a couple of our members are also heading stateside for the summit and I would be great to hear from you if you'll also be there – either by email or phone (number above).

If you would like to contribute an article, have a job advert you want to include in our next journal or have any other feedback you would like to share, please contact us at admin@iappANZ.org – we'd love to hear from you!

Enjoy!

Kate

Vice-President's Foreword

By Melanie Marks
Vice-President
melanie.marks@cba.com.au

Dear Members

Welcome back to another year of privacy practice! The iappANZ has a solid year of events and benefits planned for members this year and we look forward to your involvement and feedback.

So, a quick summary of what you'll find in the February-March edition of *Privacy Unbound*...

We kick off with a view from our regulators. Firstly, new Zealand Privacy Commissioner, **John Edwards** tells **Katherine Gibson** (Director, Gibsons Law Limited in Auckland) about his key focuses in 2016, including projects and the international agenda – and a visit from UN Special Rapporteur on the Right to Privacy, Professor Joseph Cannataci during Privacy Awareness Week.

Australia's Privacy Commissioner and Acting Information Commissioner, **Timothy Pilgrim** outlines the hot issues for Aussie privacy professionals this year (spoilter alert: big data, data sharing, de identification, and mandatory data breach notification), the basis for the appeal by his Office of the decision of the AAT in *Telstra Corporation Limited and Privacy Commissioner* (more about that later), impacts of the EU GDPR on Australian businesses and early thoughts on implementation of mandatory data breach legislation, should the current draft Bill be passed.

Annelies Moens (Head of Sales and Operations, IIS) and **Malcolm Crompton** (iappANZ Board Director and Managing Director of IIS) share some insights to their recent report on the APEC Cross-Border Privacy Rules System. Presented at recent APEC Steering Committee meetings in Lima, Peru, the report is focused on stakeholder views on the benefits of the CBPR for APEC economies and businesses.

Whilst, high-profile data breaches have placed the issue of cyber risk firmly on the agenda for boards, law makers and regulators in Australia, cyber risk insurance has not been as widely embraced as may have been expected. In this article, **Leah Mooney**, Minter Ellison Special Counsel highlights findings from a recent cyber risk survey of c-suite and senior executives in the information technology, legal and risk sectors.

According to **Anna Johnston**, Director, Salinger Privacy, we need to talk about Ben Grubb. In case that's not enticing enough, this article critiques the approach taken in the *Telstra* case by AAT Deputy President Stephanie Forgie in concluding that mobile network data is about connections between mobile devices and not about an individual. As Anna asks: "*How far could you take this argument? Could banks start arguing that their records are only 'about' transactions, not the people sending or receiving money as part of those transactions? Could hospitals claim that medical records are 'about' clinical procedures, not their patients?...*" **Peter Leonard** (Partner, G+T) also reviews the ATT's "novel and controversial" decision, noting that the vexed issue of how to work out when device information is personal information is a key issue that arises for many Internet of Things ('IoT') applications now entering the market and gives us a view of the appeal to the Federal Court of Australia anticipated to commence in August 2016.

Did you know that 28 January 2016 was *International Data Privacy Day*, which – like APAC Privacy Awareness Week – purports to raise awareness among businesses and consumers about the importance of protecting the privacy of their personal information, new trends/regulations in the privacy realm and to promote privacy and data protection best practices? Turn to page 17 to see pics from Privacy After Hours in Melbourne, coordinated and hosted by **Grace Guinto** from PwC in conjunction with the global IAPP organisation and local iappANZ team to celebrate International Data Privacy Day.

Finally, maybe your New Years' Resolution is to join the New Zealand Privacy Commissioner's Office or the Digital Trust & Privacy team of the Commonwealth Bank? Turn to page 19 for job ads.

Happy reading.

Melanie

A reminder about iappANZ membership:

Membership benefits

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

Also, 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. If you don't want us to confirm your membership details to iapp in accordance with iappANZ's privacy policy, please let me know by emailing me at emma.heath@iappanz.org.

Thanks

Emma Heath, iappANZ General Manager

And remember.....

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=.gdr_1281574752237_1

Follow us on Twitter at: https://twitter.com/iappANZ

Q&A with John Edwards
Privacy Commissioner (New Zealand)

with Katherine Gibson

1. What are some of the key focuses for your team for 2016?

This year we will be continuing to focus on 'making privacy easy' for agencies and individuals, as well as preparing for upcoming law reform.

In the dispute resolution space, we are continuing to make changes to our processes to give people access to more timely remedies. Our investigators are continuing to focus on early resolution through phone conversations when possible, leaving formal, written investigations for the more sensitive or complex cases. This is a continuation of a process we started last year, and we expect it will give more people faster access to remedies.

.

We are also focussing on improved privacy practice in the private sector. To this end, we've recently launched our transparency reporting pilot. This is a project to encourage private sector agencies to publicly report the number of personal information requests or demands they have received from government agencies, and how many of those requests they complied with.

The trial report – launched in February – proved the concept by surveying 10 agencies and reporting the (anonymised) results. The headline result was that there were 12,000 requests made during the 3 month trial. We will be encouraging other private sector agencies to do their own transparency reporting this year.

Finally, the Minister of Justice has indicated that reforms to the Privacy Act – first recommended by the Law Commission in 2011 – are on the horizon, so we are working with a number of other agencies on these reforms, as well as preparing to make necessary changes across our website, guidance material and a variety of other publications

2. You want to "make privacy easy" for agencies as well as individuals. What projects do you have in the pipeline this year to achieve this?

In May this year we will release a tool that helps people request their personal information from agencies that hold it. We expect this will be valuable for many people, as more than half of our complaints each year are about access requests.

We will be releasing new online education modules to help people understand their privacy rights and obligations. A module on privacy for employers is in the pipeline, as is a module on credit reporting. These will complement the existing modules, which are Privacy 101, Health 101 (overviews of the Privacy Act and Health Information Privacy Code, respectively), a guide to Approved Information Sharing Agreements and a guide to Privacy Impact Assessments.

We will continue our regional outreach strategy, sending staff to cities and towns outside the main regions to speak to groups such as Chambers of Commerce and District Law Societies. These visits help us engage with people who don't come across our radar as often, and gives opportunity to promote things like the tools we develop and our online education modules.

3. Privacy has an ever increasing international dimension. What is on your international agenda for this year?

Our office is gearing up for another full year of international activity as the field of privacy and data protection continues to evolve at a fast pace. New Zealand's privacy laws are just one part of a world-wide picture of privacy protection. Privacy is protected as a human right at the highest international level and it is important to have regular and ongoing contact with our international privacy colleagues to keep up with privacy developments.

We will also be playing our part with the Global Privacy Enforcement Network (GPEN) and the Asia Pacific Privacy Authorities (APPA). Our involvement in APPA is an important part of our international engagement and we'll be contributing to the APPA Forums in Singapore in July and Mexico in November or December. We'll also be involved in the *OECD Ministerial Meeting on the Digital Economy: Innovation, Growth and Social Prosperity*, in June 2016 in Cancun, Mexico.

We have a continuing role in organising the annual International Conference of Data Protection and Privacy Commissioners. Our office is currently the secretariat for the ICDPPC which will be held in Marrakesh in October. I am the Chair and we will have quite a bit of work to do in preparing the programme for the closed session in Morocco.

We will be hosting the United Nations Special Rapporteur on the Right to Privacy during Privacy Week this year. Professor Joseph Cannataci is the world's first privacy investigator at this international level. We'll be looking forward to hear what he has to say at our public Privacy Forums in Wellington (11 May) and Auckland (12 May). He then heads to Australia.

4. We are looking forward to the visit from the UN Special Rapporteur on the Right to Privacy during Privacy Week in May this year. What do you hope Professor Joseph Cannataci's visit will achieve?

Since taking up the role in July 2015, Prof Cannataci has spoken about government and corporate surveillance on the Internet and overreaching intelligence gathering. He says proper oversight is the only way and he champions a universal Geneva Convention-style law that safeguards people's online information.

For privacy authorities and anyone who works to ensure the security and integrity of personal information, the creation of a UN rapporteur role devoted to privacy is a singular universal elevation of privacy rights. It's more than symbolism; it's a reflection of the growing international convention that privacy is a value that needs special attention in changing world.

We are looking forward to finding out more about Prof Cannataci's views and we believe he will have some thought provoking ideas to add to our ongoing national discourse on privacy, oversight and transparency.

5. If you had to choose one area of focus for Privacy Professionals for 2016 this year, what would it be?

We're big on dispute resolution. Last year, we closed 827 complaint files and of these, nearly half were achieved with a settlement between the parties involved. A big portion of our complaints relate to agencies failing to meet their obligations to provide access to personal information when requested. This is particular focus for us in 2016.

Our closing times for complaints are getting faster, and our focus is on continuous improvement. For example, in 2014, a quarter of our files (24%) were older than 6 months. This reduced to 19% by 2015, and by January 2016, only 10% of our file load was over 6 months. We'll keep working at it.

In an access complaint, a successful resolution might include providing the information a customer requested – or perhaps a portion of the information. In other complaints we see resolutions with an apology or an acknowledgement, a change in an agency's processes, staff retraining, or a compensatory payment. It's usually a better option than expensive and time consuming legal action. Many New Zealanders have learned the hard way about the time, cost and emotional drain of litigation, and the substantial delays inherent in the court process. Dispute resolution is an area that we will continue to concentrate on and it is perhaps an area that many other privacy professionals could pay closer attention to.

John Edwards is the New Zealand Privacy Commissioner
Katherine Gibson is Director, Gibsons Law Limited in Auckland (http://www.gibsonslaw.co.nz)

Q&A with Timothy Pilgrim, Privacy Commissioner and Acting Information Commissioner (Australia)

with Melanie Marks

1. What do you see as the hot issues and challenges for privacy professionals in 2016?

The regulatory framework for privacy is now well established in Australia. Many organisations, agencies and individuals have a good understanding of their rights, responsibilities, and privacy processes. But privacy will continue to develop and change, particularly as technology advances. So we must all step up to the challenge of managing our privacy, and meeting our responsibilities to others; including our clients and customers.

Big data, data sharing, de-identification, and mandatory data breach notification are all key issues for the year ahead.

From its beginnings, big data has presented significant privacy challenges. But the best responses lie in bringing big data into a privacy-by-design framework. The OAIC is developing guidance to assist organisations and agencies to take a privacy-by-design approach in a big data context.

Big data has changed and will continue to change many privacy management practices, but the *Australian Privacy Principles* are flexible, and can support good business processes, if approached the right way. Big data is big business. But businesses that rely on big data, analytics and data aggregation, which is rapidly becoming most businesses, *must* take a transparent and accountable approach to the use of this technology, or they will risk serious customer mistrust and regulatory attention.

.

Connected to the issue of big data is de-identification, which is vital to get right. De-identification is a key tool to maximise the utility and value of information assets while at the same time safeguarding privacy. Businesses and government are collecting more data than ever before, and they are using it in broader and more varied ways than we would have thought possible, even five years ago.

Advances in technology means that methods of de-identification have evolved substantially over the last few years and, when executed correctly following a robust risk assessment, deidentification can be an excellent privacy solution. But, as we have seen in a few high profile privacy cases, de-identification is not always being fully or correctly integrated with technology solutions, and this can create significant and large scale issues from seemingly small mistakes.

De-identification is also becoming more complex — it is a dynamic area which is more intrinsically bound up in developments in big data, data matching, and aggregation, and it is essential that all organisations that collect personal information are keeping their finger on developments in this area. You can expect to hear a lot more from me, and the OAIC, on the subject of de-identification and Big Data this year.

Finally, as I have said many times, mandatory data breach notification is an important step in protecting the personal information of Australians, and I feel that it can be achieved without an unnecessary burden on businesses. However, assuming the legislation is passed, there will be a period of adjustment while the changes are implemented and integrated into processes and policies, and OAIC looks forward to assisting with that integration.

2. The Information Commissioner has appealed the decision of the AAT in Grubb v Telstra. What is the basis for the appeal? When can we expect the matter to be heard by the Federal Court?

My determination in this matter found that an individual's metadata could be personal information under the *Privacy Act 1988*, in circumstances where the metadata is information about an individual whose identity is apparent or can reasonably be ascertained from that metadata.

I found in this instance that customer metadata held by Telstra constituted personal information and that Telstra was obliged to give customers access to this information on request.

That decision had implications for the operational practices of organisations and agencies handling personal information and Telstra sought review in the AAT, which took a different approach to the meaning of personal information under the Privacy Act and set aside my determination.

That decision in turn equally has implications for the information handling practices of organisations and agencies and I think it is important to obtain the certainty of a court finding to provide clarity to the thousands of Australian entities who handle information of this nature. It's for this reason that I have sought to have the Federal Court review the AAT's decision.

The appeal will be heard and determined by a Full Court, and although a date has not yet been set, we anticipate that the matter will be listed for hearing during the Full Court and Appellate Sitting period in August 2016.

3. How might the EU GDPR affect Australian businesses with dealings in Europe?

There are significant differences between the European Union General Data Protection Regulation (**EU GDPR**) and the EU Directive, and any Australian business that has dealings, or a customer base, in the EU would be well advised to familiarise themselves with it.

The GDPR has a wider jurisdiction than the EU Directive, and now includes something similar to the Australia link in the APPs — it covers any business that offers goods or services to, or monitors behaviour of, EU residents. New obligations also apply to any business (such as cloud providers) that process data on behalf of another business that is covered by the GDPR. The GDPR also includes requirements similar to APP 1, including privacy by design. Businesses should also be aware that they may be required to appoint a data protection officer, in particular circumstances, which the regulation spells out.

The GDPR also introduces a mandatory data breach notification scheme. While Australia also has a proposed scheme, the EU model varies from the Australian model in a number of respects. Accordingly, any business that trades in the EU should ensure that they familiarise themselves with the EU requirements. It is also worth noting that the fines for breaching the GDPR have been raised, up to 4% of annual worldwide turnover, or €20mil.

For individuals, the privacy protections have been expanded — for example, the GDPR includes the right to data portability, any organisation that is covered by the GDPR must try to verify parental consent for individuals below 16 for use of online services, and, importantly, the GDPR includes the right to be forgotten.

4. **One of the requirements for establishing a successful mandatory data breach notification regime is ensuring that the regulator is adequately resourced. If the proposed legislation is enacted, what sort of volume of notifications do you expect to receive and how will the OAIC organise itself to respond to them?**

If the proposed scheme is enacted, the OAIC's initial focus will be on providing guidance to assist affected organisations to give effect to the scheme. However, where needed I can access a range of regulatory powers (including conducting investigations in response to complaints or on my own initiative) to ensure compliance.

While it is impossible to put a precise figure on how many notifications will be made under the proposed scheme, looking at the experience of other jurisdictions that have moved from voluntary to mandatory schemes, we would expect the volume of notifications to increase well above the number we are currently receiving.

Timothy Pilgrim is the Australian Privacy Commissioner and is also the Acting Australian Information Commissioner.

Melanie Marks is Vice President of iappANZ and Executive Manager - Digital Trust and Privacy at Commonwealth Bank

APEC Cross-Border Privacy Rules System: New Report on Stakeholder Views

by Annelies Moens and Malcolm Crompton

At recent SOM I Meetings in Lima, Peru, Information Integrity Solutions presented the much anticipated Report on stakeholder views on the benefits of the Cross-Border Privacy Rules System (**CBPR**) for APEC economies and businesses. The Report authors, Annelies Moens and Malcolm Crompton reported on consultations with government, business and regulator stakeholders from a sample of economies, including, Japan, Singapore, Mexico, Canada and the USA. The purpose of the Report was to raise awareness of benefits and serve as a catalyst for further economy specific cost/benefit analyses.

The Report found that stakeholders were identifying significant trade benefits as well as internal business benefits. From a government stakeholder perspective CBPR has the potential to advance global trade and economic growth policy objectives. Governments generally have policies to further economic growth and prosperity and this has been a fundamental objective of APEC since its inception. For trade to increase, views were that a trusted environment is required, especially when more and more trade involves personal information. CBPR is a scalable set of standards that can potentially also alleviate localisation pressures.

From an internal business perspective, CBPR plays a role towards having one global compliance system. Having one standard with one interpretation can potentially help overcome cultural differences that would otherwise make cross-border data flows even more complex. Business stakeholders considered that a simplified compliance system allows businesses to focus on better privacy rather than complex layers of compliance. One company has also benefited greatly from its CBPR certification through lowered cost and time in getting EU Binding Corporate Rules for its existing global privacy program.

From a regulatory perspective, CBPR can enable regulators to potentially improve resource allocation, by enabling them to focus resources and efforts on systemic, high profile and high impact privacy issues, rather than first line complaint handing if Accountability Agents in the CBPR System are effective.

Overall the Report finds that awareness and understanding of CBPR is low. The extent to which businesses and economies find value in the CBPR depends on:

- Each economy's underlying domestic law
- Underlying domestic law of current and future trading partners
- Requirements of stakeholders

The independence and professionalism of Accountability Agents, Privacy Enforcement Authorities and the Joint Oversight Panel are integral to the credibility of the system and impacts overall regulatory benefits. The authors recommended the following next steps:

1. APEC member economies and businesses use the preliminary assessment in the Report to start the process of conducting a full cost/benefit analysis from their own perspectives
2. An urgent review and update of CBPR documentation take place – to make it accessible and easy to understand
3. Consideration be given to stronger and more visible promulgation of CBPR

The IIS report is available at from the IIS website (under "Publications" and "APEC") and at this link.

Annelies Moens is Head of Sales and Operations at Information Integrity Solutions and can be contacted at amoens@iispartners.com

Malcolm Crompton is Managing Director at Information Integrity Solutions and can be contacted at mcrompton@iispartners.com

Perspectives on cyber risk: how resilient are you?

by Leah Mooney

A number of recent high-profile data breaches have placed the issue of cyber risk firmly on the agenda for boards, law makers and regulators. Against this backdrop there has been an increase in the availability and uptake of specialist cyber risk insurance policies as organisations increasingly choose to allocate risks through securing insurance.

However a recent cyber risk survey by MinterEllison of c-suite and senior executives in the information technology, legal and risk sectors revealed that, while cyber risk is front-of-mind for Australian organisations, cyber risk insurance has not been as widely embraced as may have been expected given the rise of cyber risk to prominence in recent times.

The Survey

MinterEllison conducted a survey (**the Survey**) at the end of 2015 in order to provide an overview of Australian organisations' risk posture in relation to cyber attacks and cyber resilience capability. Two different surveys were distributed: one directed at the chairmen, directors and chief executive offices (**Board Survey**) and another directed at chief information officers, chief information security officers, general counsel and other risk-related managers (**CIO Survey**). A total of 159 responses, comprising 81 responses to the Board Survey and 78 responses to the CIO Survey, were received and evaluated.

Only 29% of survey respondents confirmed their organisation held specialist cyber risk insurance. A further 32% were unsure of whether cyber risk was addressed in their existing insurance arrangements.

Cyber Risk Insurance

While specialist cyber risk (or security and privacy) insurance policies are relatively new products in the Australian market, most 'blue-chip' insurers now offer this cover. Most of the available policies are hybrid products providing cover for first party losses (such as the cost of hiring technical experts to identify and address the cause of the data breach and engaging public relations professionals to conduct reputational repair services) and regulatory costs (such as fines or penalties, and notification and monitoring expenses) in addition to third party liability cover for any claims arising from any data breaches.

The reasoning behind the decision on the part of many organisations not to secure specialist cyber insurance is unclear. Possible contributing factors include a lack of awareness of the availability of cyber insurance cover, an organisation's appetite for risk and the possible expectation of coverage under the organisation's existing suite of policies.

Organisations should exercise caution in seeking to rely on their existing suite of traditional insurance policies for cover in the event of a data breach as these policies are not designed to respond to cyber risks. By way of example, references to 'property' in traditional insurance policies (such as fidelity and crime policies) are generally references to tangible property and therefore these policies are unlikely to provide protection in the event of a data breach.

Cyber Resilience

While organisations should certainly consider the benefits of a specialist cyber risk insurance policy, insurance is just one component of a balanced cyber risk response. The Survey also revealed that organisations can do more to improve their cyber resilience capabilities.

A significant number (27%) of CIO Survey respondents reported that their organisation did not have a data breach response plan in place. Further, more than half (56%) of CIO Survey respondents reported that they only conducted information security training for personnel on an ad hoc basis. Accordingly, there is room for Australian organisations to improve their cyber resilience.

A useful starting point is the development of a cyber resilience plan. This process should include:

- Undertaking a contractual review to identify the allocation of risks and responsibilities;
- Identifying critical systems, data and services;
- Investing in employee training; and
- Understanding and implementing antivirus software, firewalls and data encryption.

The Office of the Australian Information Commissioner also recommends that all organisations covered by the *Privacy Act 1988 (Cth)* have in place a data breach response plan setting out the framework for responding to a data breach. Given a significant number of respondents to the CIO Survey (27%) reported that their organisation did not have a data breach plan in place, this is an area for organisations to improve their cyber resilience.

For the complete results of that survey in our *Perspectives on cyber risk report* click here.

Leah Mooney is a Special Counsel at Minter Ellison and can be contacted at leah.mooney@minterellison.com.

How Stephanie's broken down car is undermining your privacy

by Anna Johnston

We need to talk about Ben.

Specifically, about Ben Grubb, the tech journo who triggered an on-going legal case, the resolution of which might yet either reinforce or undermine Australia's privacy laws. (We'll get onto Stephanie and her troublesome car shortly.)

Actually, we really need to talk about the word 'about' – what it means for information to be 'about' Ben. Because it is that one little word – *about* – which has caused such a ruckus.

When is information 'about' Ben, and when is it 'about' a device or a network?

First, the background. When the Australian Government was preparing in 2013 to introduce mandatory data retention laws, to require telcos to keep 'metadata' on their customers for two years in case law enforcement types needed it later, Ben Grubb was curious as to what metadata, such as the geolocation data collected from mobile phones, would actually show. He wanted to replicate the efforts of a German politician, to illustrate the power of geolocation data to reveal insights into not only our movements, but our behaviour, intimate relationships, health concerns or political interests.

While much fun was had replaying the video of the Attorney General's laughable attempt to explain what metadata actually is, Ben also worked on a seemingly simple premise: "the government can access my Telstra metadata, so why can't I?"

Exercising his rights under what was then NPP 6.1, Ben sought access from his mobile phone service provider, Telstra, for his personal information – namely, "all the metadata information Telstra has stored about my mobile phone service (04...)".

At the time of his request, 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".

(Since then, the definition of 'personal information' has changed slightly, NPP 6.1 has been replaced by APP 12, and the metadata laws have been passed, including a provision that metadata is to be considered 'personal information' under the Privacy Act. Nonetheless, this case has ramifications even under the updated laws.)

Telstra refused access to various sets of information, including location data on the basis that it was not 'personal information' subject to NPP 6.1. Ben lodged a complaint with the Australian Privacy Commissioner. While the complaint was ongoing, Telstra handed over a folder of billing information, outgoing call records, and the cell tower location information for Ben's mobile phone at the time when Ben had originated a call, which is data kept in its billing systems.

What was not provided, and what Telstra continued to argue was not 'personal information' and thus need not be provided, included 'network data'. Telstra argued that that geolocation data – the longitude and latitude of mobile phone towers connected to the customer's phone at any given time, whether the customer is making a call or not – was not 'personal information' about a customer, because on its face the data was anonymous.

The Privacy Commissioner ruled against Telstra on that point in May 2015, finding that a customer's identity *could* be linked back to the geolocation data by a process of cross-matching different datasets. Privacy Commissioner Timothy Pilgrim made a determination which found that data which "may" link data to an individual, even if it requires some "cross matching ... with other data" in order to do

so, is "information ... about an individual", whose identity is ascertainable, meaning "able to be found out by trial, examination or experiment". The Privacy Commissioner ordered that Telstra hand over the remaining cell tower location information.

Telstra appealed the Privacy Commissioner's determination, and in December 2015 the Administrative Appeals Tribunal (AAT) found in Telstra's favour. Now here is where it gets interesting.

We knew that the case would turn on how the definition of 'personal information' should be interpreted, and I for one expected that the argument would centre on whether or not Ben was 'identifiable' from the network data, including how much cross-matching with other systems or data could be expected to be encompassed within the term 'can reasonably be ascertained'.

And at first, that looked like how the case was going. The AAT judgment goes into great detail about precisely what data fields are in each of Telstra's different systems, and what effort is required to link or match them up, and how many people within Telstra have the technical expertise to even do that, and how difficult it might be. But then – nothing. Despite both parties making their arguments on the topic of identifiability, the AAT drew no solid conclusion about whether or not Ben was actually identifiable from the network data in question.

Instead, the AAT veered off-course, into questioning whether the information was even 'about' Ben at all. Using the analogy of her own history of car repairs, Deputy President Stephanie Forgie stated:

"A link could be made between the service records and the record kept at reception or other records showing my name and the time at which I had taken the care (sic) in for service. The fact that the information can be traced back to me from the service records or the order form does not, however, change the nature of the information. It is information about the car ... or the repairs but not about me".

The AAT therefore concluded that mobile network data was about connections between mobile devices, rather than "about an individual", notwithstanding that a known individual triggered the call or data session which caused the connection. Ms Forgie stated:

"Once his call or message was transmitted from the first cell that received it from his mobile device, the data that was generated was directed to delivering the call or message to its intended recipient. That data is no longer about Mr Grubb or the fact that he made a call or sent a message or about the number or address to which he sent it. It is not about the content of the call or the message. The data is all about the way in which Telstra delivers the call or the message. That is not about Mr Grubb. It could be said that the mobile network data relates to the way in which Telstra delivers the service or product for which Mr Grubb pays. That does not make the data information about Mr Grubb. It is information about the service it provides to Mr Grubb but not about him".

Well. That was a curve ball I did not see coming.

This interpretation seems to conflate *object* with *subject*, by suggesting that the primary purpose for which a record was generated is the sole point of reference when determining what that record is 'about'. In other words, the AAT judgment appears to say that what the information is *for* also dictates what the information is *about*.

In my view, this interpretation of 'about' is ridiculous. Why can't information be generated for one reason, but include information 'about' something or someone else as well? Why can't information be 'about' both a person and a thing? Or even more than one person and more than one thing?

Even car repair records, which certainly have been created *for* the primary purpose of dealing with a car rather than a human being, will have information *about* the car owner. At the very least, the following information might be gleaned from a car repair record: "Jane Citizen, of 10 Smith St Smithfield, tel 0412 123 456, owns a green Holden Commodore rego number ABC 123".

If we accept the AAT's view that the car repair record has no information 'about' Jane Citizen, then Jane has no privacy rights in relation to that information, and the car repairer has no privacy responsibilities either. If Jane's home address was disclosed by the car repairer to Jane's violent ex-husband, she would have no redress. If the car repairer failed to secure their records against loss, and Jane's rare and valuable car was stolen from her garage as a result, Jane would have no cause for complaint. Jane won't even have the right to access the information held by the car repairer, to check that it is correct.

How far could you take this argument? Could banks start arguing that their records are only 'about' transactions, not the people sending or receiving money as part of those transactions? Could hospitals claim that medical records are 'about' clinical procedures, not their patients? Could retailers claim their loyalty program records are 'about' products purchased, not the people making those purchases?

Surely, this is not what Parliament intended in 1988 when our privacy laws were first drafted – or indeed, when they were updated in 2014, when the amendments were claimed to bring Australia's privacy protection framework into the modern era.

In this era of Big Data, it is the digital breadcrumbs left behind in operational or transactional systems which can yield the business insights with the most value – and are thus in need of privacy protection.

The Privacy Commissioner is appealing the AAT's decision to the Federal Court. I can only hope the Federal Court can see that information created for an operational purpose might *also* contain both deliberate and incidental information 'about' individuals – individuals who expect their privacy to be protected, no matter how or why the records were created in the first place.

The alternative is to let Stephanie's broken-down car throw a major spanner in the works of privacy protection in Australia.

Anna Johnston is Director, Salinger Privacy

Salinger Privacy provides specialist privacy consulting and training services. Salinger Privacy publishes a blog, as well as eBooks on privacy law, including an annotated guide to the NSW privacy laws. Find Salinger Privacy at www.salingerprivacy.com.au

A review of *Telstra Corporation Limited and Australian Privacy Commissioner*

Australian Administrative Appeals Tribunal, now under appeal to the Full Federal Court of Australia [2015] AATA 991, 18 December 2015

By Peter Leonard

The Tribunal overturned the earlier determination by the Australian Privacy Commissioner granting journalist Ben Grubb access to certain data relating to Mr Grubb's use of Telstra mobile services. The Tribunal's Decision throws open the vexed issue of how to work out when device information is 'about an individual whose identity may be reasonably ascertained from the information' - a key issue that arises for many Internet of Things ('IoT') applications now entering the market.

In May 2015, the Australian Privacy Commissioner, Mr Timothy Pilgrim PSM, had found that Telstra had breached the Australian Federal Privacy Act 1988 (the 'Privacy Act') by failing to provide Mr Grubb with access to requested metadata relating to his use of Telstra telecommunications services as collected and held by Telstra in various databases for various purposes, some purely technical e.g. operation of the network and monitoring its performance: *Ben Grubb v. Telstra Corporation* [2015] AICmr 35, 1 May 2015. The case required application of the pre-March 2014 definition of 'personal information,' being 'information about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion' (this definition is be contrasted to the current Privacy Act definition of 'personal information,' which is information 'about an identified individual or an individual who is reasonably identifiable').

The Commissioner considered that the question of whether an individual's identity can 'reasonably be ascertained' from information required assessment as to how unreasonably high the level of effort necessary to link an individual through to non-identifying information must be before an entity receiving an access request can say that the access that is requested is not to information from which an individual's identity can reasonably be ascertained. It was not contended that Mr Grubb as an individual could be linked to some network data relating to use by Mr Grubb of his mobile phone through a multi-step process (requiring significant labour input and including manual matching) of tracing and matching records through multiple databases in Telstra's systems. Although Mr Grubb's identity was not apparent in relevant Telstra databases where relevant metadata was held, the device identifiers or IP addresses or other transactional information there held could be traced through from mobile tower records to operational and network databases and on to personally identifying databases (in particular, the Telstra customer billing database). Telstra regularly facilitated requests by law enforcement agencies for lawful assistance as to use of mobile phones by persons of interest by undertaking such tracing and matching processes.

Of course, Telstra's practice of assisting law enforcement agencies as required by law did not of itself answer the question of whether existence of a possibility of tracing from source information to identifying information should lead to a determination as to whether an individual's identity can reasonably be ascertained from the information. The Privacy Commissioner quoted a decision by Deputy President Coghlan in *WL v. La Trobe University* [2005] VCAT 2592 that such consideration requires examination of the complexity of the inquiries that would be needed to ascertain the information and the degree of certainty with which possible connections between that information and the individual's identity could be made. In circumstances where an individual's identity could only be ascertained from health survey information that had to be extracted from different databases, cross-matched and then cross-matched to an external database 'and even then the making of any possible connections would not identify with certainty' the relevant individual, DP Coghlan concluded that this went "beyond what is reasonable" (*WL* at para 52). By contrast, the Privacy Commissioner found that "Telstra's handling of tens of thousands of requests made by law enforcement bodies, together with its recent public statement affirming that customers may access their metadata on request, suggests instead that Telstra has the capacity through the use of its network and records management systems to ascertain the identity of an individual and this process of ascertaining an individual's identity does not exceed the bounds of what is reasonable" (*Ben Grubb v. Telstra* at para 101).

Tribunal Deputy President S A Forgie, in the Administrative Appeals Tribunal's Decision overturning the Privacy Commissioner's Determination, stated that where an individual is not intrinsically identified in information, a two-step characterisation process should

be applied. The first step is determining whether relevant information is "about an individual." The second step is working out whether an individual's identity "can reasonably be ascertained from the information or opinion." If relevant information is not "about an individual" that is the end of the matter. But if information is information "about an individual," the second step must be applied.

It was in relation to the first step that the reasoning of DP Forgie most clearly diverged from the Privacy Commissioner. After noting that the range of what may be considered to be information "about an individual" is infinite and included, for example, information relating to the person's physical description, residence, place of work, business and business activities, telephone number and so on, DP Forgie stated (at para 112):

> "Had Mr Grubb not made the calls or sent the messages he did on his mobile device, Telstra would not have generated certain mobile network data. It generated that data in order to transmit his calls and his messages. Once his call or message was transmitted from the first cell that received it from his mobile device, the data that was generated was directed to delivering the call or message to its intended recipient. That data is no longer about Mr Grubb or the fact that he made a call or sent a message or about the number or address to which he sent it. It is not about the content of the call or the message. The data is all about the way in which Telstra delivers the call or the message. That is not about Mr Grubb. It could be said that the mobile network data relates to the way in which Telstra delivers the service or product for which Mr Grubb pays. That does not make the data information about Mr Grubb. It is information about the service it provides to Mr Grubb but not about him."

Similar reasoning may suggest that, for example:

- a transient or ephemeral device identifier, such as an internet protocol ('IP') address used to establish an internet session and manage interactions between an internet service provider and a user;
- a more pervasive identifier such a mobile phone's unique 15 digit International Mobile Station Equipment Identity ('IMEI') number;
- service records or records of use of a household device; and
- a motor vehicle licence plate;

may not satisfy the first step of this characterisation process, because it is not information "about an individual": rather, it is information about an inanimate object that may be associated with an individual. Or to put it another way, the fact that information about an inanimate object may be retrievable by reference to an identified individual does not of itself make the information about the object information about an individual.

The problem is that the first step has an element of circularity, as had been noted in a number of New Zealand cases. For example, the New Zealand Human Rights Review Tribunal, applying a similar definition of 'personal information' in the case of *Apostolakis v. Sievwrights* (14 February 2005, HRRT 44/03[1]), stated:

> "[59] The matter is further complicated because the answer to the question 'Is this personal information?' can, we suspect, depend on how the question is asked. If one were to approach an observer and ask: 'A owns a building which is insured. Is the fact that the building is insured 'personal information' about A?' the answer might well be 'no, it is information about the building.' On the other hand, if one were to approach the same person but ask 'Is the fact that A has insurance on her building 'personal information' about A?' then the answer might well be 'yes - it is information which tells me something about A's rights in respect of the building that she owns.'

The NZ Tribunal concluded that there is no 'bright line' test, suggesting instead that although a person may not be identifiable in the information, if there is a 'sufficient connection' to an individual that connection may justify a conclusion that the information is personal information about that person. However, this reasoning interposes another phrase to be interpreted and applied: at what point does an inanimate object associated with an individual become 'sufficiently connected' to that individual such that the information ceases to be only 'about the object' and becomes 'about the individual'? If information about use of a mobile phone,

[1] available on www.nzlii.org

typically carried on a person through most of their waking hours and intimately associated with (and often creating an electronic record of) a person's life, is not information about an individual, what information recorded by IoT devices is (to use the test suggested by the NZ Tribunal) 'sufficiently connected' to an individual? The AAT in the *Telstra* appeal did not refer to the New Zealand cases, but there does appear to be an underlying concept of closeness of association, or as the NZ Tribunal put it, whether there is a sufficient connection. Applying DP Forgie's reasoning, a distinction might be made between a Fitbit or other personal health device which clearly gathers information about an individual, and cellular network connectivity features of a mobile phone that enable continuous calls notwithstanding handoffs between mobile towers, where relevant location information is collected for call management, not for tracking movement of an individual.

In stating the second stage test, DP Forgie followed generally accepted reasoning in Australia and New Zealand as to whether an individual's identity "can reasonably be ascertained *from*" information as allowing reference to extrinsic materials, but only such extrinsic materials as are *reasonably* available. DP Forgie then gave a striking illustration of how this test might be applied:

> "In dealing with a request [by an individual for access to personal information about them] under the Privacy Act, it does not follow that an organisation need scour the public domain to ascertain whether there is information that can be married with the information or opinion it holds in order to ascertain the identity of the individual. What it means is that the organisation must keep in mind what might be matters of general knowledge. If, for example, the information were along the lines of 'singer and songwriter who died prematurely,' I do not think that it could be said that the identity of that individual can reasonably be ascertained from that information. If the information were 'female singer and songwriter who died prematurely,' I suggest that her identity would also not be reasonably ascertainable. If the information were 'English female singer and songwriter who was known for her eclectic mix of musical genres of soul, rhythm and blues and jazz but who died prematurely in July 2011' [Amy Whitehouse], I suggest that the identity of the individual can be reasonably ascertained from the information which would be regarded as part of the broad body of general knowledge" (at para 107).

DP Forgie then continued:

> "Beyond what might be considered to be general knowledge, I do not think that regard needs to be had to the wide range of information and means of searching information that is available in the public arena in determining whether an individual's identity is reasonably ascertainable from the information or opinion held in an organisation" (at par 108). This proposition appears overstated: release of purportedly de-identified information into the public arena in circumstances where a motivated intruder could be anticipated as able to apply means of re-identifying an individual is generally regarded as a disclosure of personal information.

The reasoning of the Administrative Appeals Tribunal is both novel and controversial. The Australian Privacy Commissioner had appealed the Tribunal's Decision to the Federal Court of Australia. A Full Bench of the Federal Court will hear the appeal, probably in August 2016. One possibility is that on appeal the Decision may stand and the Tribunal's reasoning limited to the specific context before it, namely, working out what information should be made available by a data controller in response to an access request by an individual. In that context, considerations of practicality and cost mitigate against overly broad disclosure requirements. By contrast, decisions by data controllers to release purportedly de-identified data sets into the public arena, where it may be reasonable to expect motivated intruders to seek to re-identify any individual through use of exhaustive searches or strong analytical techniques, might rightly be subject to a test which imposes a higher level of foresight and control. Of course, the words 'reasonably ascertainable' enable a range of context-specific tests to be developed.

As the IoT continues to grow, we may be confident that cases addressing similar questions to those considered in *Ben Grubb v. Telstra* will arise for determination in many jurisdictions.

Peter Leonard is a Partner with Gilbert + Tobin Lawyers in Sydney, and can be contacted at pleonard@gtlaw.com.au

International Data Privacy Day – in Melbourne!

By Grace Guinto

28 January 2016 is the International Data Privacy Day. The purpose of Data Privacy Day is to raise awareness among businesses and consumers about the importance of protecting the privacy of their personal information, new trends/regulations in the privacy realm and to promote privacy and data protection best practices.

In honour of Data Privacy Day, a Privacy After Hours event in Melbourne was held at the Campari House (23-25 Hardware Lane), which was coordinated and hosted by PwC in conjunction with the global IAPP organisation and local iappANZ team. The event was a great way to connect the local privacy professionals and members of the iappANZ, and enable local privacy professionals to network, discuss the latest hot topics in the privacy realm and most importantly, to get to know others who are working in this space locally. It was a great evening with a diverse group of privacy professionals attending the event, ranging from local Victorian government organisations' representatives, legal professionals, information technologists, and consulting firms, who have a range of experiences working locally and abroad in the US, Canada and UK. It was a fun night where everyone enjoyed a relaxing Melbourne evening of beer, nibbles and privacy related wit.

Grace Guinto is a Director at PricewaterhouseCoopers in Melbourne and can be contacted at grace.guinto@pwc.com

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).

CAREER OPPORTUNITY
JOB TITLE: PRIVACY ADVISOR

LOCATION: SYDNEY CBD AREA

JOB NUMBER: 973926

- Career move with Australia's Leader in Financial Services
- World Class Facilities based in Sydney CBD

Here is a great opportunity for an experienced Privacy Advisor to grow their career with the market leader. Are you currently in a Consulting or Legal Firm or Policy Advisor role in Government and looking to build on your privacy experience in a commercial role on the client side? If so, this could be the career move that launches your career.

What will be your responsibilities?

Reporting to the Portfolio Manager – Digital Trust & Privacy, this role delivers Privacy Impact Assessments

ME_128501021_1 (W2007)

and privacy assurance services to the Bank. Responsibilities include:

- Conducting Privacy Impact Assessments and providing other privacy assurance services to customers within the Bank;
- Working with business to design data privacy requirements in systems, projects, products and services;
- Providing SME support to internal customers through meetings and written communication and advice;
- Undertaking ad hoc research and assisting with strategies to drive the digital trust agenda;
- Maintaining awareness of new privacy and network security laws and regulations as well as industry best practices and integrating these into technology and business processes;
- Monitoring legal and policy data privacy developments in countries where the organization operates;
- Enhancing relationships with key stakeholders, internal and external; and
- Participating in and maintaining relationships with industry networks and associations.

Your new team

The Digital Trust & Privacy Team is an integral part of the Digital Protection Group (DPG), which has as its mandate the protection of the CBA Groups' (the Group) platforms, systems, data, assets and reputation from security, privacy, trust and operational risks. Further, the DPG is charged with leveraging our capabilities in the security, privacy and operational risk to create innovative and market-leading products and capabilities, preparing and protecting the Group for our digital future.

The team provides practical privacy advice to teams across the Bank and the Group. Our purpose is to support the Bank in embedding privacy best practice into its DNA as well as leading strategic initiatives that will enhance the Bank's position of trust with customers and the community. The role the team plays is crucial to Bank securing a leading place in the Digital Future.

What are we looking for?

We expect you will have sound experience within Financial Services or another large corporate or leading technology provider, or in a legal or policy advisory practice with recent and extensive experience in privacy and data security. You will of course possess strong knowledge and understanding of current industry practices, laws and regulations as they apply to privacy and data protection. You will be a good communicator with a strong customer focus and demonstrated commercial acumen and experience in service delivery.

At CommBank each of us globally is dedicated to offering outstanding service, excellent advice and intuitive solutions to help our customers manage their finances in the ways they want to.

Regardless of where you work within our organisation, your initiative, talent, ideas and energy all contribute to the impact that we can make with our work. Together we can achieve great things. Sound like you?

SANS Institute: Director, Business Development (Australia)

Locations: based in Melbourne and Sydney

Job title: Director, Business Development (Australia)

Company: SANS Institute

Closing date: COB 1 May 2016

Location: Home-based role. Melbourne or Sydney preferred, other locations considered.

Job description:

To support the continued growth of our programs in Australia and the Asia Pacific region, SANS is seeking to expand our APAC team with the creation of a new role - Business Development Manager (Australia). Reporting directly to the Director, Asia Pacific in Australia and the Managing Director, APAC, the Business Development Manager will work closely with our existing APAC team to:

- Develop new business and relationships with customers in State/Territory and Federal Government agencies, banking and finance, telecommunications, professional services, defence industry and/or ICT security sectors.
- Generate significant new revenue and support business profitability through direct sales and business development activities.
- Manage exiting key customer relationships and other partnerships in Australia in order to grow business.
- Develop and implement marketing strategies to drive revenue growth in Australia using email, print, web and social media.
- Support our local operations as required through contributions to local event logistics and student administration.
- Propose other initiatives to strengthen SANS market profile in assigned markets and sectors.

To succeed in this new role, the Business Development Manager will have:

- Demonstrated success in sales and business development with customers in Government agencies and/or commercial enterprises in industry sectors with an interest or capability in cyber security.
- An extensive network of existing relationships on which to draw in order to engage new business.
- A commitment to excellence in customer service and relationship management.
- A willingness to tackle all the challenges of local service delivery as part of a small, high-performing team, and to travel within Australia (extensively) and the APAC region (occasionally) for business development activities.
- A collaborative, enthusiastic, team-focussed approach to achieving results and contributing to business success.
- The right to work in Australia, with 5 years or more of recent residence in country and knowledge of the local market conditions.
- A satisfactory outcome from all pre-employment background and police history checks we will perform during the selection process.

How to apply details:

For a confidential discussion about the role and how to apply, please call Steven Armitage (Country Director, Australia) on 0402067768, or email sarmitage@sans.org.

Further Information:

About the SANS Institute

The SANS Institute was established in 1989 as a cooperative research and education organization. SANS is the most trusted, and by far the largest source for world-class information security training and security certification in the world offering over 50 training courses. GIAC, an affiliate of the SANS Institute, is a certification body featuring over 25 hands-on, technical certifications in information security. SANS offers a myriad of free resources to the InfoSec community including consensus projects, research reports, and newsletters; and it operates the Internet's early warning system - the Internet Storm Center. At the heart of SANS are the many security practitioners in varied global organizations from corporations to universities working together to help the entire information security community. (www.SANS.org)

iappANZ's writing prize 2016: *entries have opened!*

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 2016. 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 2016. 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 2016 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, Carolyn Lidgerwood and David Templeton, plus President Kate Monckton 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$300, 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.

Privacy Events

Where and when	Event details	Price
SYDNEY **Thursday 31 March** **4.00 – 6.00pm** **Gilbert + Tobin** **L37, 2 Park Street** **Sydney 2000**	**iappANZ Training Workshop** Mandatory Data Breach Notification Law: What is being proposed and impacts Speakers to be announced- check iappANZ.org for more details	FREE to iappANZ members $99 incl. GST for non-members
MELBOURNE **April Date TBC** **3.30pm for 4.00pm start – 6.00pm** **Minter Ellison** **Rialto Towers** **525 Collins Street** **Melbourne 3000**	**iappANZ Training Workshop** Mandatory Data Breach Notification Law: What is being proposed and impacts Speakers to be announced - check iappANZ.org for more details	FREE to iappANZ members $99 incl. GST for non-members
BRISBANE **Thursday 14 April** **12.00pm for 12.30pm start – 2.00pm** **Corrs Chambers Westgarth** **Level 42** **111 Eagle Street** **Brisbane 4000**	**iappANZ Training Workshop** Mandatory Data Breach Notification Law: What is being proposed and impacts Speakers to be announced - - check iappANZ.org for more details	FREE to iappANZ members $99 incl. GST for non-members

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.

FIND OUT MORE at: http://www.iappanz.org/index.php?option=com_content&view=article&id=34&Itemid=5

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**)
David Templeton (**David.Templeton@anz.com**)

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