Privacy Unbound iappANZ

March/April 2015

UNLOCKING THE TRUTH ABOUT PRIVACY

ISSUE 61

President's Letter

By Anna Kuperman
President
M: 0419 803 263

Dear Members

iappANZ is thrilled to be a Privacy Awareness Week 2015 (3-9 May) partner and will be supporting the *Privacy everyday* message with an excellent line up of local and international talent in a privacy road-show across Sydney, Melbourne, Auckland & Wellington. Attendance is free for our members and we hope to see many of you at our events (list of our events in the Journal calendar and on our website http://www.iappanz.org/).

In this edition, you will see an introduction to our guest speaker Professor Fred Cate who will present at each of our PAW events across ANZ. Professor Cate works at the forefront of privacy, security, and other information law and policy issues. He has spoken throughout the United States and in Belgium, Canada, China, Finland, France, Germany, Italy, Japan, Switzerland, Taiwan, Trinidad & Tobago, and the United Kingdom. He is the author of more than 100 articles and books, including *Privacy in the Information Age* and *Privacy in Perspective* and he appears regularly in national media.

Now for a little teaser. I invite you to take a look at *lively debate held at Indiana University* back in 2012 which featured some passionate arguments on the nature, status, and future of cloud security by Professor Cate and a senior IT leader (Waggener). Much has changed and evolved since then – but you have the opportunity to ask Professor Cate what he thinks of these issues now at our events.

We are pleased to announce that Sarah Davis, Group Commercial Legal Director from the Guardian Media Group (UK) will be joining our Sydney Q&A panel on 8 May to share her insights on privacy issues in the media industry. Sarah has been Group Commercial Legal Director for GMG plc since April 2010 with responsibility for all commercial, corporate and regulatory activity across the group. GMG is the owner of Guardian News & Media Ltd one of the UK's leading media organisations, publisher of The Guardian, The Observer and theguardian.com and global online presence with dedicated sites in the US and Australia. We welcome Sarah to our expert panel.

For our New Zealand based members, you are fortunate to be truly spoilt for choice this PAW and I'm not just talking about iappANZ events. The Office of the New Zealand Privacy Commissioner has published a calendar of PAW events at https://privacy.org.nz/forums-and-seminars/privacy-week/privacy-week-2015-events/. With special thanks to KPMG, iappANZ will be running an event in Wellington (6 May) featuring Russell Burnard, Government Chief Privacy Officer, Department of Internal Affairs and in Auckland (7 May) featuring Joy Liddicoat, Assistant Commissioner (Policy & Operations).

For more information on Privacy Awareness Week visit the PAW website.

Vice-President's Foreword

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

Happy reading, Anna Kuperman

In December 2013, the *Sydney Morning Herald* reported on the impending introduction of the Australian Privacy Principles as part of a set of reforms to the Privacy Act 1988. In an article about how poorly many Australian websites were performing in relation to online privacy, Nigel Phair reported:

> *"...The introduction of privacy principles mean organisations will have to update their privacy policies and risk management protocols. If they combine the principles with best practices for responding to a data breach, they'll need to have a cultural rethink in the collection, storage, use and dissemination of information which personally identifies customers."*

Similarly, in the lead up to their introduction, the international director of IT security and risk association ISACA, Jo Stewart-Rattray, told *The Age* that organisations needed to have their houses in order:

> *"Hoping for the best is never the best approach... Companies need to understand where they currently sit in relation to the new privacy legislation in order to understand where the gaps lie and what needs to be undertaken to fill in those gaps ... Business owners and IT will need to work together to ensure that personal information is appropriately protected."*

This is a special, retrospective edition of *Privacy Unbound*. We start with comments on the anniversary by Australian Privacy Commissioner, **Timothy Pilgrim.** Privacy Commissioner Pilgrim looks back at the year that was and shares some insights into what the next 12 months hold. iappANZ members **Medibank Private, Acxiom, Telstra** and **Microsoft** then share their experiences and insights on significant changes, challenges and opportunities presented by the reforms.

David Templeton turns our minds to the challenges of ascertaining consent in relation to privacy from minors. Can we take a risk based approach to privacy and minors? What questions should organisations be asking themselves?

Ella Biggs outlines *Hammond v Credit Union Baywide*. The decision marks a significant development in New Zealand's privacy law: it is the first time the Human Rights Review Tribunal has considered the *Privacy Act 1993* in the context of social media. It also marks a record-breaking award of damages to a victim for a breach of their privacy.

In that context, **Katherine Gibson** provides her observations about the *Hammond v Credit Union Baywide* case also.

Emma Hossack and **Anthony Tanti** discuss one of the most misunderstood (and poorly performed) aspects of the information life-cycle – disposal as well as the role of the National Association of Information Destruction (NAID), which has been established to educate business and government on the importance of proper and secure information destruction and the importance of using a qualified service provider.

This month we profile **Professor Fred Cate**. Professor Cate's illustrious career as well his views on privacy are introduced in this edition by Privacy Unbound Co-Editor **Veronica Scott**. If you haven't yet registered to hear world leading privacy guru Professor Cate speak, turn to our Privacy Events page for all the details of his whistle stop tour Down Under and in the Land of the Long White Cloud.

Will any of these authors be the winner of this year's writing prize? If you'd like to know (and perhaps assess them for yourself), turn to page 18 for the rules!

Minter Ellison is advertising for a *Senior Lawyer/ Senior Associate in Privacy and Administrative Law* and the Office of the Australian Privacy Commissioner (OAIC) is recruiting for an *Adviser, Regulation and Strategy*. Want to know more? Better read on...

We hope you enjoy this edition of Privacy Unbound.

Melanie

A message about iappANZ membership benefits

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

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

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

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

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

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

Emma Heath, iappANZ General Manager

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

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

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

Our LinkedIn group is:
http://www.linkedin.com/groups?gid=1128247&trk=anetsrch_name&goback=.gdr_1281574752237_1

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

March 2015 – first anniversary of privacy law reforms

by Timothy Pilgrim, Australian Privacy Commissioner

This month, the Office of the Australian Information Commissioner (OAIC) marked the first anniversary of the most significant changes to Australian privacy laws in over 25 years. I know there are many iappANZ members who have been working hard over the last year to assist their organisation to make the transition to the new Australian Privacy Principles.

Over the past 12 months, the OAIC's focus has been on developing guidance and working with organisations, agencies and the wider community to ensure that everyone has the tools and information they need to understand and implement the changes.

We have seen a large increase in the number of privacy complaints, privacy enquiries and data breach notifications. We received 4,016 privacy complaints in the 12 month period following the commencement of the changes, a 43% increase on the previous 12 months. During this period, the OAIC also received 14,064 privacy enquiries, and 104 voluntary data breach notifications. I believe that this growth can be explained by an increased awareness of privacy issues amongst regulated entities and the community, brought about, at least in part, by the changes to the Privacy Act.

I have commenced 13 privacy assessments since the changes commenced, using my new power to conduct assessments of privacy compliance for both agencies and organisations. This includes a targeted assessment program of the online privacy policies of 21 entities. These assessments are looking at whether the policies are clearly expressed and up-to-date, cover the content and contact requirements and are available in an appropriate form. More assessments are planned in 2015.

I have been particularly impressed with how organisations and agencies have responded positively to the challenge of implementation over the last 12 months. This is recognition that good privacy practices are good for business, particularly in building customer trust.

My focus for the next 12 months will be on governance. I have been talking for a long time about the need to build privacy into 'business as usual processes', and how essential it is to include it in business and project planning. My messages around this aren't going to change, but we're a year into these new privacy laws so I'd like to start talking about more than just basic compliance, and shift the conversation to ongoing governance. A key component of a successful end-to-end privacy program is regular monitoring. This will ensure that privacy policies, procedures and guidance are being followed and that they remain relevant to the privacy risks that a particular business or agency faces.

The OAIC will be assisting organisations and agencies to build a culture of privacy to ensure that they are proactive in meeting their compliance requirements. We will be encouraging organisations and agencies to realise that it is more effective, and ultimately cheaper, to embed privacy in day-to-day processes than it is to respond to issues such as data breaches as they arise. To help you do this, look out for our new Privacy Management Framework to be released during Privacy Awareness Week, which is nearly upon us.

It is great to see that so many iappANZ members have registered as partners. I look forward to seeing you at the events during the week and hearing about the ways in which you have marked the week in your organisation.

One year on – iappANZ member perspectives

with Melanie Marks, iappANZ Vice President

Now that the dust has settled, iappANZ members generously reflect on and share their experiences about implementing the new Australian Privacy Principles.

medibank PRIVATE

"I think we do a good job of choosing the paths we go on by asking the simple but fundamental questions: Would our customers expect us to do this and what would they say if they knew?"

What has been the most significant change in your organisation, brought about by the reforms?

We have a quite a mature privacy framework within Medibank and we used the opportunity presented to us by the changes to the Act to reinforce internally the value of privacy to our customers and to the organisation. As an integrated healthcare company, offering health insurance and health care along with a number of complementary services, our people have always intrinsically understood the value of confidentiality and security.

The message we emphasised last year was our role as custodians of our customers' and providers' information. I think that one of the subtle but significant changes we have seen is a much deeper understanding that although information has been entrusted to us, its ownership always remains with the individuals who choose to give it to us, and they have final say over what we do with it.

What areas present the biggest challenges operationally?

As we try to add value to our interactions with our customers and work to design innovative products which can delight them, we need to understand their needs better. Like most organisations, we have mountains of data which sit in silos across the business. In trying to bring it all together so we can turn data into information and ultimately, knowledge and insights, the biggest challenge is to ensure that we are clear as to the boundaries we should stick to. There are a myriad of tools, ideas, and opportunities out there in relation to leveraging information – not all of them are worthy of being pursued. I think we do a good job of choosing the paths we go on by asking the simple but fundamental questions: Would our customers expect us to do this and what would they say if they knew?

The answers to these questions guide our thinking and we don't pursue anything we would not be happy to explain.

How have these changes enabled Medibank Private to better fulfil the mantra of "privacy everyday"?

One of the changes to the Act which we welcomed was the introduction of privacy planning under APP1. From a pure cost and effectiveness perspective, we have always adopted a 'Privacy by Design' approach to how we develop our offerings. For us, the seamless integration of privacy controls into the business as usual activities is a necessary precursor to their sustainability and effectiveness. APP1 allowed us to have a tangible obligation under the Act around which to articulate our approach to embedding privacy into everything we do.

*Thank you to **Gerard Noel**, Senior Compliance Adviser | Group Privacy Officer, Medibank Private Limited for these insights.*

What has been the most significant change in your organisation, brought about by the reforms?

Acxiom has always taken a proactive approach to data privacy and my view is that the reforms have only helped to enhance Acxiom's existing position on privacy. It definitely expedited an audit of all areas of the Australian business taking place prior to the introduction of the new privacy laws on 12 March 2014, so the reforms definitely sharpened our focus on reviewing Acxiom's existing practices and processes. Probably the one area to call out given Acxiom's role in assisting organisations with their direct marketing practices, was to ensure that the new requirements included in APP 7 with respect to direct marketing were adhered to, particularly given the new rules regarding personal information from third parties, such as Acxiom.

> ***"I am not in all places at all times. I therefore need to ensure that whether it is a new product launch, the disclosure of personal information overseas or an enquiry made by a consumer into their personal information, that the proper rules and processes are adopted and in the event of any uncertainty that this is escalated to me. It is of critical importance that each team within the organisation recognises the role they play in ensuring privacy compliance."***

What areas present the biggest challenges operationally?

Operationally, I believe one of the biggest challenges is to ensure employees within your organisation understand when to escalate an issue. At the end of the day, while I am the Privacy Officer for Acxiom Australia and New Zealand, I am not in all places at all times. I therefore need to ensure that whether it is a new product launch, the disclosure of personal information overseas or an enquiry made by a consumer into their personal information, that the proper rules and processes are adopted and in the event of any uncertainty that this is escalated to me. It is of critical importance that each team within the organisation recognises the role they play in ensuring privacy compliance.

How have these changes enabled Acxiom to better fulfil the mantra of "privacy everyday"?

Privacy is at the heart of Acxiom's business. Acxiom adopts a 360 degree approach to privacy, as it impacts on most, if not all business units at some level within our organisation and is built into Acxiom's DNA. The legislative reforms have therefore ensured internal compliance which is demonstrated by activities such as conducting Privacy Impact Assessments, incorporating privacy by design, operating consumer care teams, having a global privacy team and a Privacy officer for each of Acxiom's main regions. Acxiom has also hosted 3 external Privacy Roundtable Privacy events in the US, Japan and Sydney to demonstrate thought leadership in privacy and to address issues which are equally important to Acxiom, its clients and partners. Privacy is not only a focus for Acxiom's Australia and New Zealand operations, but also a corporate focus for the organisation globally.

*Thank you to **Julie Dennis**, General Counsel – Legal & Compliance, Acxiom for these insights.*

What has been the most significant change in your organisation, brought about by the reforms?

We've always taken the view that these reforms were evolutionary not revolutionary. One year on, I think that has proven to be the case. The reforms did bring about a renewed focus on privacy and with that we saw more mature and comprehensive conversations around privacy issues, both internally and with our business customers, suppliers and customers.

What areas present the biggest challenges operationally?

One of the biggest implementation challenges has been around interpreting and operationalising some of the requirements which rely on "reasonableness tests". (continued over)

"… with regards to Australian Privacy Principle 8, we believe there is room for further thought around creating more efficient, certain and practicable ways of working with international clients, suppliers and partners where personal information is involved."

For example, with regards to Australian Privacy Principle 8 we believe there is room for further thought around creating more efficient, certain and practicable ways of working with international clients, suppliers and partners where personal information is involved. With the digital economy underpinned by borderless infrastructure and the pace of change in technology being so rapid, it's often difficult for Australian businesses to harmonise the variety of international compliance frameworks covering the protection of personal information to the satisfaction of all stakeholders involved.

How have these changes enabled Telstra to better fulfil the mantra of "privacy everyday"?

Independent of the regulatory changes, there has been a marked change across our organisation around the need to drive a stronger privacy culture and build more privacy controls into everything we do. This is largely due to the rapid changes in how our customers communicate with each other each day, the growth in data across the digital economy and maturing customer expectations around privacy. This has meant that privacy has become a regular agenda item on management and executive meetings and has led to; enhancements to our project management methodologies; a stronger commitment to "privacy by design" ideals; and a greater investment in controls that protect our customers data. With regards to the regulatory changes, the formalisation in APP1 of the need to have a Privacy Framework in place has meant that it's a more structured part of our overall compliance program.

*Thank you to **Ben Carr**, Chief Privacy Officer, Telstra for these insights.*

"Increasingly privacy is a core component of the sales discussion, from much earlier on in the process. It's been a really positive change – with privacy being seen as part of the value of a service as opposed to a box to tick."

What has been the most significant change in your organisation, brought about by the reforms?

The amended Privacy Act has opened up a really constructive conversation with our clients on how best to protect personal information in cloud services. The new Act made it even more explicit that if an enterprise or Federal Government agency collects personal information, they are ultimately responsible for protecting the privacy of that information, even if they use a third party service to host or store that data. This has put a lot of focus on transparency: What do cloud providers do with the data? Do they use it for marketing or advertising purposes? Where do cloud providers host the data? We've really welcomed that extra focus on transparency over the last 12 months, because it's drawn attention to what cloud providers will commit to in their contracts and not just what they say in their marketing brochures.

What areas present the biggest challenges operationally?

Building a consistent global platform for our customers can sometimes lead to challenges in articulating local compliance with various privacy regimes around the world. That's why we've been a really strong supporter of global standards, including the recently finalised data protection standard for cloud providers, ISO/IEC27018, that provides clear guidance to customers on cloud providers' privacy practices. We've had our major enterprise cloud services verified against this standard – which is another mechanism for customers to assure the practices of cloud providers like Microsoft and to ensure that they can meet their requirements under the Privacy Act.

How have these changes enabled Microsoft to better fulfil the mantra of "privacy everyday"?

We take a strong 'privacy by design' approach to all of our products and services and the clear guidance within the amended Act has enabled us to have a detailed conversation with our customers about our approach. Increasingly privacy is a core component of the sales discussion, from much earlier on in the process. It's been a really positive change – with privacy being seen as part of the value of a service as opposed to a box to tick.

*Thank you for **David Masters**, Corporate Affairs Manager, Microsoft for these insights.*

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

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

Privacy and young customers

by David Templeton

Introduction

Ahead of the Victoria University (Wellington) May 2015 Identity Conference **"Enabling Digital Identity and Privacy in a Connected World"**[1] sponsored by iappANZ, it's timely to turn our minds to youth privacy issues. This is because this conference will feature Professor Dr Simone van der Hof as a key note speaker.

Professor van der Hof is a leading academic, holding a number of leadership positions including chair of Law at Leiden University. Significantly, Professor van der Hof has a particular interest in an EU research programme, **EU Kids Online.**[2]

EU Kids Online findings may eventually inform both better protection for young internet users and higher quality in their online participation, recognising that children are entitled to be online[3].

EU Kids Online[4] provides a valuable collection of insights into the concerns that young people tend to harbour about the internet, and the perception of risk within various age groups. From a young age (ie under 10 years) nasty content and contact risks top the list of concerns. Cyberbullying and social network abuse is also a concern. Some practices that seem to matter to adults, like direct marketing and cross border data transfers do not feature.

At the same time, elsewhere in Europe, an interesting conversation has begun about whether privacy law might become more 'risk based'. Risk based regulation can produce more efficient outcomes by empowering industry to manage risk in a manner that is more cost effective by being proportionate to the nature and degree of relevant risks.

As food for thought goes, these developments are pure carbohydrate. They've led me to think about the position in Australia, from the perspective of online business and younger users.

Kids are prolific internet users. They have access to multiple devices (including computer, tablet, mobile telephone, gaming console). Their activities are often unsupervised, and only a proportion of parents manage their children's browsing with content restriction software. As they move into their teens, they quickly acquire the skills to navigate profile creation, social media and purchasing interfaces. Increasingly, children have access to secondary credit cards (via their parents), gift cards which grant the holder credit on various web stores and debit cards acceptable for online purchases. So the child customer is a very real phenomenon.

From a business perspective, capacity to give consent and access to information are two key challenges presented by the youth market.

Capacity and consent in privacy law – 15 years of age

Key areas in which customer consent is likely to be required include:

- Secondary uses of personal information
- Direct Marketing, in which Australian Privacy Principle 7 might have you seeking consent to direct marketing
- Collection and use of any sensitive information
- Sending information overseas where informed consent can take you out of the accountability net

Capacity to consent in privacy law is technically a common law question, resting on a medical consent case decided in 1985[5]. At common law capacity to consent is attributed to minors who can fully comprehend all (medical as well as social) risks and implications of a procedure. The resulting law is not particularly easy to apply in practice.[6]

The Information Commissioner's Guidelines to the Australian Privacy Principles give practical assistance[7]. They recognise that minors have capacity to consent "when they have sufficient understanding and maturity to understand what is being proposed"[8] and that making an assessment of capacity is not always easy. On the surface, this will be a challenge for your website.

Where you can't undertake an individual assessment, the Commissioner invites you to assume that individuals aged 15 or over have capacity, so long as nothing in the transaction suggests otherwise.[9] So in an online transaction, the Commissioner seems likely to presume that a user under the age of 15 years lacked capacity.

This leads to the following questions:

1. ***Do you refuse to deal online in any way that requires privacy consent from anyone who identifies as less than 15 years of age?***

This is probably a safe course. However this is not a widely adopted business model.

2. ***Should you ask customers their age?***

[1] http://www.identityconference.victoria.ac.nz

[2] See at: http://lsedesignunit.com/EUKidsonline/html.

[3] The United Nations Convention on the Rights of the Child has been said to confer rights to participate as well as rights to protection on children in relation to the internet. An interesting discussion is offered by Livingston & O'Neill in "*Children's Rights Online: Challenges, Dilemmas and Emerging Directions" 2014* at page 27

[4] See: https://lsedesignunit.com/EUKidsOnline/html5 The same research has been undertaken in Australia producing similar results: What bothers Australian kids online? Children comment on bullies, porn and violence: http://www.cci.edu.au/reports/WhatBothersAuskidsFIN.pdf

[5] *Gillick v West Norfolk and Wisbech Area Health Authority* [1985] (1985) 3 All ER 402; approved in Australia in 'Marion's Case' (1992) 175 CLR 189

[6] See the commentary in the NSW Law Reform Commission Report 119, 2008 "Yong People and Consent to Health Care"

[7] The Guidelines implement the recommendations of the ALRC "For Your Information" (ALRC Report 108) 68.112.

[8] Guidelines to the Australian Privacy Principles B.5.1

[9] Ibid B.5.2

Notoriously, a number of US online businesses have managed to escape COPPA10, the law that effectively deems 13 to be the age above which individuals can give effective privacy consents by just not asking.

The question of whether or not to collect age rests on a number of factors, but in this context, if you ask age and your customer is 15 or older, you can assume capacity.

3. *Is age verification necessary?*

Most businesses will have no easy way to verify age in an online transaction[11], so this is not easy to achieve. It would address the risk of younger consumers lying about their age (not that that would ever happen!).

4. *Should you obtain parental consent?*

For some services, parental consent might well be desirable and especially at ages younger than 15. Uses that clearly present issues include publication of images and storage of contact details, but there really isn't any closed list and each innovation you launch on the web requires careful assessment. As noted above, electronically verifiable parental consent is not easy in Australia.

5. *Can you adopt a risk based approach to consent from younger users, in circumstances where the matters that the law recognises as necessary to be understood are simpler and perhaps lower in risk than might otherwise be the case?*

There is no real adoption of risk based regulatory principles evident in Australian privacy law. However, the EU is actively debating whether privacy regulation should look to drive prudent but economically efficient practices by becoming more "risk based"[12]. Risk based regulation typically requires conformity to a prescriptive framework of policies and processes for assessing risk and imposes obligations to implement appropriate and responsive mitigants.

This opens up the possibility of future regulation in our region moving in the same direction, and raises the question of the extent to which the Commissioner will consider an organisations' overall approach to privacy risk management in matters where the Commissioner has discretion, such as compensation and penalties[13].

A risk based approach could assist in managing capacity to consent issues by allowing business to empower younger users to make an informed decision about consent, for example by tailoring disclosures by age group. It might still be the case, however, that higher risk choices should be removed from younger users if their age-group might generally not be capable of comprehending or assessing privacy consequences, no matter how clearly explained.

Access to information

In the context of young people's privacy, parental access rights are a difficult area. Parents are generally shocked to discover that organisations might refuse them access to their dependent children's information on the basis of privacy.

The Privacy Act 1988 gives a parent, as a "responsible person", access rights to a child's personal information in limited and relatively dire circumstances. Businesses dealing directly with younger customers, whether online or not, may wish to consider how they want to balance the interests of child and parent and be clear in their privacy policies.

...and in conclusion

Younger online customers pose a range of risks to business.

It is critical to map out the risks and issues from the perspectives of the child customer, their parents, your business model and the regulatory framework in order to understand the implications of your business decisions.

David Templeton is a Senior Manager at ANZ, currently specialising in digital channel design. David is also the Secretary of iappANZ

[*Ed note: for those interested in reading more on this issue – see the March 2015 fact sheet from the Canadian Privacy Commissioner: (Fact sheet: Collecting from kids? Ten tips for services aimed at children and youth* https://www.priv.gc.ca/resource/fs-fi/02_05_d_62_tips_e.asp)

---

[10] In the United States, the *Children's Online Privacy Protection Act* (**COPPA**) regulates collection of personal information from children under 13 years of age under a regime which, among other measures:

- Gives parents control of their children's uploaded information up to age 13
- Requires comprehensive privacy policies
- In many cases, requires notice to parents and verifiable parental consent (which is revocable) before collecting information from children under 13.

COPPA has been criticised for its requirement that a web publisher have actual knowledge of a person's age before being regulated, enabling websites to avoid COPPA altogether by not asking users their age.

[11] Options for electronic verification of age are limited for organisations that lack access to the Commonwealth Document Verification Service.

[12] For a helpful discussion see Hunton & Williams: http://www.informationpolicycentre.com/privacy_risk_framework/

[13] Risk based regulation is gaining favour in our region. Anti-money laundering laws are partly risk based and in NSW, State guidelines direct NSW regulators to adopt a risk based approach in dealing with non-compliance: http://arp.nsw.gov.au/c2014-06-quality-regulatory-services-initiative-%E2%80%93-guidance-nsw-regulators-implement-outcomes-and

Privacy rights and social media – the decision in *Hammond v Credit Union Baywide*

by Ella Biggs

The New Zealand media has taken great joy in reporting on the recent Human Rights Review Tribunal's (the *Tribunal*) decision in *Hammond v Credit Union Baywide*,[1] and not only because of the numerous baking puns that the facts give rise to. This decision marks a significant development in New Zealand's privacy law: it is the first time the Tribunal has considered the Privacy Act 1993 in the context of social media. It also marks a record-breaking award of damages to a victim for a breach of their privacy, with the Tribunal awarding over $168,000 to Ms Hammond.

Facts

Ms Hammond had resigned from her position at New Zealand Credit Union Baywide (*NZCU*). She attended a dinner party for a friend and former colleague at NZCU, who had also recently resigned from her position. To cheer her friend up, she baked a cake and iced it with what the Tribunal describes as "earthy" phrases,[2] which criticised their former employer. Ms Hammond took a photo of the cake and uploaded it onto her private Facebook page.

NZCU's Human Resources Manager, upon hearing of the photo, requested that a junior employee access the photo from her Facebook page, as the junior employee was a Facebook friend of Ms Hammond. A screenshot was taken by the Manager, and this was then disclosed to four recruitment agencies in the area, as well as Ms Hammond's new employer. Under pressure, Ms Hammond resigned from her new employment, and struggled to find employment in the area at the same level as her previous job for 10 months.

Ms Hammond claimed that NZCU's had breached privacy principles 1 – 4 (the *Collection Principles*) and 11 (the *Disclosure Principle*) in the Privacy Act, which amounted to an interference with her privacy, and sought damages. NZCU admitted to breaching the Disclosure Principle, but denied breaches of the Collection Principles, or that its breach amounted to an interference with Ms Hammond's privacy.

Breach

NZCU conceded at the Hearing that, in downloading the screenshot of the cake from Ms Hammond's Facebook page, it had collected her personal information. However, the Tribunal did not engage in substantive discussion regarding whether, in doing this, NZCU had contravened the Collection Principles. This was because Ms Hammond had not provided sufficient evidence that the alleged breaches of the Collection Principles had caused her detriment or damage, had adversely affected her rights, or had resulted in significant humiliation, as are required to make out an interference of privacy under section 66 of the Privacy Act.

Accordingly, the case fell to be determined under the Disclosure Principle alone, which NZCU admitted it had breached. The question for the Tribunal was whether the breach of the Disclosure Principle amounted to an inference with Ms Hammond's privacy in contravention of section 66. For readers who aren't familiar with section 66, its key provisions in this context are as follows:

> ***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.*

Finding

In answering the question regarding NACU's breach of section 66 in the affirmative, the Tribunal appeared to base its analysis on the express intent of the employees at NZCU that the disclosures caused harm to Ms Hammond. It was found that, as a result of the disclosures, Ms Hammond suffered loss and had her rights adversely affected. It was also found by the Tribunal that she had established significant humiliation.

[1] [2015] NZHRRT 6
[2] Ibid [163].

Damages

In considering the award of damages, the Tribunal undertook a detailed analysis of its previous awards for breaches of the Disclosure Principle and its awards for emotional harm. In referring to the particular circumstances of Ms Hammond's case, including the "sustained campaign by NZCU to inflict as much harm and humiliation [on Ms Hammond] as possible" (rather than an inadvertent disclosure) and the 10 months Ms Hammond spent unemployed as a result of this, the Tribunal found that Ms Hammond had suffered damage "of a different order"[3] to the Tribunal's prior highest award for a breach of the Disclosure Principle (of $40,000). Accordingly, a damages order exceeding $168,000 was made. The Tribunal has discretion to award damages up to a maximum of $200,000.

Analysis

Although notable for its record-breaking damages award, this decision is also interesting in its approach to privacy in the context of social media.

As is clear from the Tribunal's reasoning, this decision is about the intentional disclosures of Ms Hammond's personal information by senior staff at NZCU; the Tribunal does not consider at all whether a post on Facebook is itself personal information. The Tribunal's approach to the personal information, which had already been shared by Ms Hammond to her 150 Facebook friends, is interesting. The Tribunal considered the application of the privacy principles in the context of social media to be a "straightforward exercise", and much was made of Ms Hammond's private Facebook settings: "Ms Hammond took care to ensure that the photograph of the cake uploaded to her Facebook page could only be accessed by her 'friends'".[4]

However, this approach appears to overlook the developing understanding that, if information is shared on social media (regardless of the privacy settings), it is no longer "private". This has been considered in New Zealand in the employment law context, where the question was aptly asked: "How private is a written conversation initiated over the internet with 200 'friends', who can pass the information on to a limitless audience?".[5] There is also a line of authority in the United States that "photographs on a social networking site are neither privileged nor protected by any right of privacy, regardless of any privacy settings that the user may have established".[6]

The Tribunal's decision, while significant in terms of the damages award, does not appear to engage substantively, and appears to be out of step, with principles that have been developing in this area both in New Zealand and internationally.

Ella Biggs works as a solicitor in Wellington, New Zealand, and is a member of iappANZ

[3] Ibid [182].
[4] Ibid [179.6].
[5] *Hook v Stream Group* [2013] NZEmpC 188 per Inglis J.
[6] *Nucci v Target Corporation* 4d 14138 (Fla App, 2015).

"Press delete"
Privacy at the end of the information life cycle

by Emma Hossack in conversation with Anthony Tanti

All information has a life cycle. It is created, captured, transmitted, processed, stored and eventually, and inevitably, it is disposed of or deleted.

When information is personal information, and when it is also medical, financial or particularly private in nature, these life cycle stages pose inherent privacy and security challenges. However, the most logical and effective strategy to protect such information is by identifying these stages and addressing their respective privacy and security vulnerabilities.

Of all stages of the information life cycle, disposition is one of the most misunderstood and overlooked. Organisations that vigilantly protect information when in use or in storage, seem to either lose interest or lose sight of the need to protect that information when it is time for it to be disposed of. Disposal is also one of the stages of the information life cycle that is often outsourced to an external service provider. As security becomes an increasingly important issue, the qualifications of these external service providers becomes equally important.

The National Association of Information Destruction (**NAID**) is an international body representing thousands of such service providers around the globe. NAID's primary mission is to educate business and government on the importance of proper and secure information destruction and the importance of using a qualified service provider.

NAID was established in the United States over 20 years ago in an effort to raise the standards of what was traditionally a highly unregulated industry. It has since grown to be the only industry information destruction trade association recognised globally, with close to 2,000 members serving 5 continents. NAID AAA Certification is currently a service provider requirement for hundreds of US government agencies and thousands of private sector organizations across U.S. Canada and Europe. NAID AAA Certification is increasingly finding recognition in Australia and New Zealand also.

The local chapter of the association, NAID-ANZ, now represents many of the largest document destruction companies in Australia and New Zealand and is expanding rapidly as customers become more aware of information security.

NAID's AAA Certified organisations are audited to assess compliance to rigorous standards, including verification of employee background screening and training, access control, written policies and procedures, and regulatory compliance. NAID audits are conducted by trained third-party Certified Protection Professionals (CPPs, the highest level of accreditation awarded by ASIS International).

Another key feature of NAID Certification is that it relies on both scheduled and unannounced audits to verify compliance. There is never a time when a NAID Certified location knows it will not be audited, either in the field or at its facility.

This differs markedly from traditional audits schemes. For instance, SCEC accreditation of data destruction available through the Australian Security Intelligence Organisation (ASIO) currently requires a single scheduled audit, with no guarantee of any future scheduled or surprise audits. NAID's 14 years of experience monitoring compliance has proven that unannounced audits are critical to enforcing ongoing compliance.

Recent changes to the Australian Privacy Act emphasise the need for independently accredited services. Outgoing NAID-ANZ Director Anthony Tanti notes that in his own business he has seen requests for NAID AAA Certification spike substantially.

"*Government departments that we've serviced for years are now asking us about NAID, people are becoming more aware of their own privacy responsibilities*," said Tanti. "*It also helps that they can monitor our compliance or request audit reports from NAID free of charge.*

"*We're finding that more organisations are requesting site visits, they want to witness their documents being shredded, NAID AAA means that we're always open to visits and provide a wholly transparent service. It's where the industry should be*," Tanti adds.

Unfortunately, document destruction is still often viewed as an extension of the waste and recycling process which puts organisations and personal information at risk. Both globally and in Australia, NAID has commissioned disturbing research showing the extent of the problem. One such project in Sydney in 2011, modeled on similar NAID studies in Toronto, Madrid and London, demonstrated the extent of the problem. Licensed private investigators targeting organisations required by law to protect personal information, including solicitors, doctors, hospitals, banks and government offices, found a significant percentage had discarded extremely confidential information with apparently no regard for the law or the consequences to them or their clients.
Last year NAID conducted research in Australia and New Zealand, purchasing a large number of used computer hard drives on the second hand market. The drives were generally obtained from computer recyclers and eBay. Forensic analysis showed that approximately 40% of second hand

computer hard drives still contained personal information. A significant portion of those drives had been owned by businesses or government offices with a legal obligation to protect the information.

All personal information resulting from these studies is properly destroyed by a NAID Certified vendor.

Tanti maintains that the solution to this issue is not that complicated.

"*Organisations need to first make proper disposal of personal information a priority, this includes training your employees and outlining their responsibilities*" says Tanti. "*The process needs to be as simple and convenient as possible; your security policies are only as good as your worst employee on their worst day*".

"*Buying a shredder and hoping employees use it is not the answer," adds Tanti. "Neither is blindly hoping that no one finds it in the waste or recycling bins left outside for collection, an easy target for identity thieves or your competitors.*"

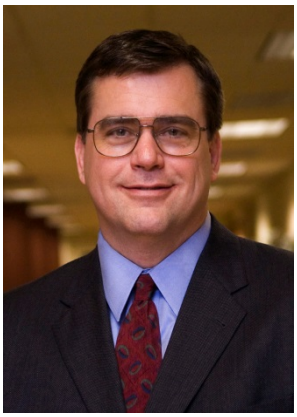
Tanti notes that management also have to play a larger role, "*Find out about where your document destruction bins are going, ask your current or potential provider about site visits and witnessing the shredding, and don't take no for an answer. It's important that organisations begin to demand transparency*".

Through its certification process, NAID-ANZ is set to mirror the success of NAID globally in educating the Australian consumer market, and imposing higher standards to the existing unregulated local industry. The NAID website[1] allows organisations to find their nearest AAA Accredited provider as well as information about the industry locally and abroad.

Anthony Tanti is an international board director of NAID

Emma Hossack is CEO of Extensia (a shared electronic health record company) and also CEO of Edocx (an information logistics and storage platform). Emma is also the Vice-President of the Medical Software Industry Association and a board member of iappANZ.

[1] http://www.naidonline.org/naus/en/



Introducing Professor Fred Cate

iappANZ is delighted to announce that we have confirmed Professor Cate as our guest for Privacy Awareness Week this year. Professor Cate will speak at a range of iappANZ privacy events in Melbourne, Wellington, Auckland and Sydney.

We couldn't introduce Professor Cate without sharing parts of his resume with you, because Professor Cate's privacy credentials are in a class of their own. But we also wanted to take the opportunity to extract some privacy observations and some personal data from Professor Cate too! Both follow below.

Resume snapshot

Professor Cate is a Distinguished Professor and C. Ben Dutton Professor of Law at the Indiana University Maurer School of Law.

He is managing director of the IU Center for Law, Ethics, and Applied Research in Health Information, and a senior fellow and former director of the IU Center for Applied Cybersecurity Research (a National Center of Academic Excellence in both Information Assurance Research and Information Assurance Education).

Professor Cate is a senior policy advisor to the Centre for Information Policy Leadership at Hunton & Williams LLP and is a member of:

- the U.S. National Academy of Science's Forum on Cyber Resilience,
- the U.S. Department of Homeland Security's Data Privacy and Integrity Committee Cybersecurity Subcommittee,
- the National Security Agency's Privacy and Civil Liberties Panel,
- the OECD's Panel of Experts on Health Information Infrastructure,
- Intel's Privacy and Security External Advisory Board,
- the Board of Directors of The Privacy Projects,
- the Board of Directors of the International Foundation for Online Responsibility, and
- the Board of Directors of the Kinsey Institute for Research in Sex, Gender and Reproduction.

Previously, Professor Cate chaired the International Telecommunication Union's High-Level Experts on Electronic Signatures and Certification Authorities, and also served as a member of:

- the U.S. Department of Defense Advanced Research Projects Agency Privacy Oversight Board,
- the National Academy of Sciences Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention,
- the U.S. Federal Trade Commission's Advisory Committee on Online Access and Security, and
- Microsoft's Trustworthy Computing Academic Advisory Board, and as counsel to the U.S. Department of Defense Technology and Privacy Advisory Committee and reporter for the third report of the Markle Task Force on National Security in the Information Age.

Professor Cate has testified before numerous congressional committees and speaks frequently before professional, industry, and government groups.

He is the author of more than 150 articles and books, serves on the Advisory Board of BNA's *Privacy & Security Law Report*, and is one of the founding editors of the Oxford University Press journal, *International Data Privacy Law*. He is a member of the American Law Institute, a fellow of the American Bar Foundation, and past president and a fellow of Phi Beta Kappa, and has appeared in *Computerworld*'s three most recent listings of the world's "Best Privacy Advisers."

Privacy Q&A

iappANZ board director and Privacy Unbound editor Veronica Scott put the following questions to Professor Cate:

1. What is the issue that you'd be most worried about today if you were a Chief Privacy Officer of a global company?

The proliferation of data and data-based services and systems. It has never been easy for a privacy professional to keep up with what his or her company (or government agency) is doing with data, but I have to think it will be impossible in the future. Personal data are collected and used in so

many unexpected ways—cars, clothing, thermostats—and with the expansion of the Internet of Things, the challenge of just being aware promises to grow exponentially. On top of this are suppliers and service providers and government agencies and other third parties who companies interact with.

2. What's on your radar about privacy laws in Australia and New Zealand?

I am no expert about privacy laws in Australia and New Zealand, but two features strike me about the unique position you occupy. One is as a "third way" approach to data protection that is different from either Europe or North America. The other is as a key player in the evolution of Asian and Pacific Rim approaches to data protection.

3. Do you actually read privacy terms and conditions before buying an online service or downloading an app?

Never. I have tried. Really. But even when I am involved in writing them I can't force myself to go back and read them.

4. Opt outs- can they work?

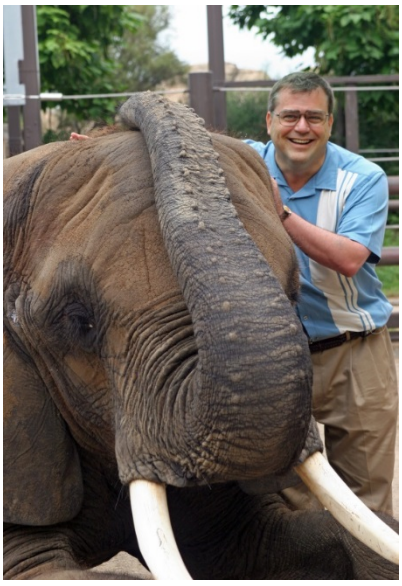
Yes. But I fear that the whole opt-in vs. opt-out debate misses the more fundamental point that basing privacy on consumer choice often leads to weakening privacy. There are many, well-documented reasons for this, but the simplest is that most individuals are willing to trade privacy protection that may benefit them in the future for immediate conveniences or other benefits now.

5. What books are you currently reading? / Favourite apps and why?/ Your favourite city?

Better than books or apps or cities, I suspect that the most revealing thing about me is that my wife, Beth, and I bought an African elephant 15 years ago. She was living alone and needed the support of a herd, so we arranged for her to live at the Indianapolis Zoo, which has a large matriarchal herd and is the world's leader in using artificial insemination to help replenish the numbers of this endangered species. Her name is Tombi, she is 37, she is very friendly, and Beth spends almost every Sunday morning caring for her; I tend to take more pictures than do real work. (below is a picture of me giving Tombi a hug.)

Then four years ago, we rescued an orphaned baby brown bear from Alaska, ultimately bringing him to the Indianapolis Zoo . Our hope was that he might bond with a young female brown bear who had recently lost her brother and was becoming increasingly listless as a result. This sort of thing usually happens only in fairy tales, since bears tend to live alone as adults, but after a lot of work and patience by dedicated zoo staff, today they are inseparable. His name is Mi-kal, which we are told means "playful," and never was a bear better named. (below is a picture; that is Mi-kal on his back, and Kiak standing.)

So you might well imagine that one reason Beth and I have loved visiting Australia, and why I am so excited about getting to visit New Zealand on this trip, is the opportunity to admire the local wildlife.



Professor Cate can be contacted at fred@fredhcate.org.

The swearing cake case – more than just a damages case …

by Katherine Gibson

One of your employees (who is in the process of leaving your company) has posted a photo on Facebook of a cake she has made for one of your former employees. The cake is iced with your company's logo and has expletives directed at your company which you consider are obscene and defamatory of your business and you believe the photo is upsetting your staff. What do you do? What would you as a privacy professional advise the company to do?

Largest ever damages award

Let's face it – the facts make you want to read more – and the case gained significant media attention and public comment. Not just because it was about a swearing cake, but because the Human Rights Review Tribunal awarded Karen Hammond (the cake maker who posted the photo on Facebook) $198,000 in damages for the company's subsequent unlawful disclosures of the photo.[1]

This award of damages was ground breaking for New Zealand's Privacy Act 1993. It included a sum of $98,000 for humiliation, loss of dignity and injury to feelings, more than double the previous highest award for this category of damage for unlawfully disclosing personal information in breach of the Act (the previous award was $40,000).

But there is more to this decision than the size of the damages award…

A bit more on the facts

The company, trading as NZCU Baywide, probably wishes they had sought some expert privacy advice when they learnt of the cake photo and found they were unable to access the photo due to Ms Hammond's Facebook privacy settings (only those accepted by her as friends had access to the photo).

But they didn't.

Instead, the Tribunal said Baywide subjected a junior employee to "*unfair pressure, if not [bullying]*"[2] to access the photo via her personal Facebook page. Having obtained a copy of the photo they then sent it to multiple recruitment agencies to warn them against employing Ms Hammond with "*the specific intent that Ms Hammond thereafter be unable to find employment in the [region]..*".[3] At the same time they disclosed information to Baywide staff about Ms Hammond's resignation. And that was not all they did. The company also sent the photo to Ms Hammond's new employer, and pressured him to dismiss her. The Tribunal said this made her position at her new job untenable and so she resigned.

The cake

The cake had been made by Ms Hammond for a dinner party for one of Baywide's ex-employees (Ms Gooding), to cheer her up after Ms Gooding had quickly departed Baywide and became unemployed. There was no dispute about whether the photo contained personal information, but the descriptions of the cake varied widely.[4]

The Baywide executives said they found the language on the cake to be offensive and obscene, and that any staff seeing the cake was likely to feel insulted and offended.[5] This is a reasonable view to hold given the cake was iced with such words.

In stark contrast, however, the Tribunal said:[6]

> *A private dinner party was arranged to express support for Ms Gooding and in that context Ms Hammond made a cake which, while iced with words some would find offensive, was a commentary on how someone who had done so much for NZCU Baywide had been treated unfairly. The message was intended to give Ms Gooding strength."*

The Tribunal considered that the making of the cake was "*an act of kindness on the part of Ms Hammond for a close friend*".[7]

---

[1] Hammond v Credit Union Baywide [2015] NZHRRT 6.
[2] Para 118.
[3] Para 181.2.
[4] For the purposes of this point, I note the cake said "NZCU F### YOU" and "C###".
[5] Paras 78, 81, 96.
[6] Para 179.5.
[7] Para 181.4

Polar views of the same cake. The lesson – when faced with such situations, regardless of whether there may be issues of brand damage, defamation, or perhaps unethical behaviour, the Privacy Act must be complied with. The conduct of the complainant is not relevant to whether there has been an unlawful disclosure. But that does not stop you pursuing other legal or practical avenues.[8]

But a Facebook post is public…isn't it?

We often hear (or may even advise) that posting information on Facebook is essentially putting the information out there in the public domain. Not so according to this decision. Whilst not expressly stated by the Tribunal, this decision supports the view that if personal information is controlled via appropriate privacy settings, the public information exceptions in the Act will not apply.

It is unfortunate that this issue was not analysed or considered in the Tribunal's written decision - accessing information from social media sites is common place and the private/public debate is likely to be a live issue in many privacy complaints.[9] This does beg the question when does the number of "friends" on a person's social media site reach a point whereby it changes from a private communication to a publicly available publication, or if it ever does under the Act?

In the New Zealand employment context at least it has been recognised that Facebook is not a strictly private forum, even when protected by privacy settings. The Employment Court when commenting on the use of Facebook posts in employment processes asked the obvious question *"After all, how private is a written conversation initiated over the internet with 200"friends", who can pass the information on to a limitless audience?"*[10]

Disclosure of information where recipient already knows the information

The decision is at odds with the generally accepted view that there is no disclosure of personal information under the Act if the information is already known to the recipient.

Baywide had accepted it had unlawfully disclosed personal information, except where they had sent the photo to Ms Hammond's new employer, who had seen the cake before it was taken to the party. Baywide argued there was no breach in this instance because the information disclosed was already known to the recipient – the photo of the cake was the same as what the employer had already seen. The Tribunal did not agree with this submission and held that there is no such exception in the Act, and that the focus of the relevant information privacy principle[11] is on the disclosure by the agency and not what may or may not be already known by the recipient.[12]

The Tribunal's decision does not refer to any jurisprudence or commentary when considering this issue. Notwithstanding this, there is now a Tribunal precedent that is contrary to the commonly held view that there is no disclosure of personal information under the Act if the recipient already knew the information.

The expletive cake case – some quick takeouts:

- **Personal information held on a Facebook page that has privacy settings where only "friends" can access it (in this case 150 friends) will not invoke the public information exceptions under the Act. Query however, when does the number of "friends" reach the point where it is becomes public information?**
- **Misconduct of the complainant is not relevant when considering whether there has been an unlawful disclosure of personal information under the Act.**
- **When responding to the Privacy Commissioner about a Privacy Complaint, ensure all necessary internal enquiries are made before formulating the response and the response is accurate. In this case, in response to the question of how Baywide had obtained a copy of the photo they advised the Commissioner that it had been forwarded onto, or shared with management by a staff member (which was not the case on the facts).**
- **The generally accepted view that there is no disclosure of personal information where the recipient already knows the information was not followed by the Tribunal, so any advice on this issue will need to take into account this decision.**

[8] For example, one option may have been writing to Ms Hammond requesting her to remove the photo as it was damaging to the company.

[9] It was not necessary for the Tribunal to make a finding on this point as Baywide accepted that the Facebook page privacy settings meant the page was not accessible to the public at large (Para 131).

[10] *Jarrod Hook v Stream Group (NZ) Pty Ltd* [2013] NZEmpC 188, para 26.

[11] Information Privacy Principle 11.

[12] Para 141.

- **When assessing any settlement of a complaint before it reaches the Tribunal stage, remember to factor in any potential brand damage if unsuccessful - the Tribunal made some harsh findings against Baywide and some of their executives – which are now in the public arena - forever.**[13]

Katherine Gibson is Legal Counsel for Centrix Group Ltd in Auckland, a company providing credit risk management solutions to businesses. Katherine also has her own legal practice, Gibsons Law, where she advises organisations on business issues, including privacy.

[13] The Tribunal found the actions of some of the Baywide senior executives to be "shameful" (para 160).

iappANZ's writing prize 2015: *entries open*

Entries have now opened for this year's writing prize for an article that is published in our monthly Journal editions from February to October 2015. Anyone can enter (you don't have to be an iappANZ member), simply by writing and submitting an article between 500-1500 words that tells us something interesting, new and relevant about privacy.

All articles must be submitted by email, preferably in Word, to [veronica.scott@minterellison.com or an iappANZ email] by 20 October 2015. We will need the author's email address and contact number. You can submit as many articles as you like.

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

More details about the writing prize if you are interested:

- Our Editorial team, Veronica Scott and Carolyn Lidgerwood, plus President Anna Kuperman and Past President Malcolm Crompton, will decide on the winner whose article they judge to be the most interesting, original and relevant to our members.
- Some people won't be eligible for the prize (sorry!). They are: iappANZ board members, contractors and employees and their family members.
- After the winner is announced we will notify them and arrange for the prize to be delivered to them if they are unlucky enough not to be at our Summit.
- There will (sadly) be one prize only. Its value is AUS$250, so that's pretty good really.
- We may need to verify the winner's identity so we don't give the prize to the wrong person.
- If the prize is not claimed for any reason (and we hope this won't happen) the author of the runner-up article as judged by the Editorial team will receive the prize.

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

Employment opportunities for privacy professionals

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

MinterEllison

Senior Lawyer/Senior Associate, Privacy and Administrative law

About Us

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

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

Your role

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

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

What you need

We welcome applications from qualified lawyers with:

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

What we offer

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

- additional week of annual leave for Senior Associates and Special Counsel

- salary continuance insurance
- extensive health & wellbeing programs including a free gym membership
- mobile device plan

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

How to apply

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

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

Australian Government

Office of the Australian Information Commissioner

Adviser, Regulation and Strategy

- Ongoing/non-ongoing, full-time/part-time positions available.
- APS Level 6
- Salary range: $75,965 - $83,652 + 15.4% superannuation.
- Location: Sydney
- Closing Date: Monday 27th April 2015

The following details are from the OAIC website at http://www.oaic.gov.au/about-us/careers/adviser-aps6-rs-april-2015:

Applicant Information

Thank you for your inquiry about working in the Office of the Australian Information Commissioner (OAIC). This document has been prepared to help you apply for these positions. The OAIC expects to fill one or more positions. An order of merit may be created and may be used to fill subsequent positions. Any further job specific information required should be sought from the contact officer Ms Este Darin-Cooper, Director on (02) 9284 9762.

About the OAIC

The OAIC is a statutory agency within the Attorney-General's portfolio. The OAIC works to protect information rights and advance information policy. Changes to federal freedom of information (FOI) law made in 2010 established the OAIC as the body responsible for information policy, privacy protection and FOI. The Office of the Privacy Commissioner, which was the national privacy regulator, was integrated into the OAIC at this time. The Information Commissioner Professor John McMillan is head of the OAIC and is supported by the Privacy Commissioner, Mr Timothy Pilgrim.

The Australian Government announced as part of the 2014–15 Budget that the OAIC will be disbanded.

The OAIC's current functions will be split between four agencies with freedom of information functions being moved to the Administrative Appeals Tribunal, the Commonwealth Ombudsman and the Attorney-General's Department. The OAIC's privacy functions will continue to be undertaken by a statutory Privacy Commissioner and supporting staff from a new office based in Sydney.

The *Freedom of Information Amendment (New Arrangements) Bill* 2014 was introduced into Parliament on 2 October 2014 and passed by the House of Representatives on 28 October 2014. It has not yet passed the Senate. The advertised position will be integrated into the new office if the Bill is passed.

Adviser, Regulation and Strategy

Advisers in the Regulation and Strategy Branch deliver a broad range of strategic policy and regulatory functions under the Commonwealth *Privacy Act 1988*. This is a unique environment in which the OAIC engages closely with both the public and private sectors.

The Adviser is a highly motivated team player with the following attributes:

- ability to provide high quality policy and regulatory advice
- ability to participate in privacy assessments of entities and write assessment reports
- high level analytical and conceptual skills
- awareness of new and emerging information technologies
- excellent communication and editing skills, including the ability to write clearly, in plain English and for different audiences
- strong organisational and project management skills
- the ability to turn ideas into action, and
- a keen eye for detail.

The Adviser, Regulation and Strategy will support Assistant Directors, Directors and the Assistant Commissioner of the Regulation and Strategy Branch to deliver services to the Commissioners, staff of the OAIC, government and the private sector.

Eligibility

Applicants must be Australian citizens, or be eligible for citizenship. Relevant qualifications/experience in one or more of the following areas would be highly desirable: public policy, proactive regulation, information technology, editing, auditing, speech writing.

Position Location

This position is located in Sydney.

Terms and Conditions

Terms and conditions of employment will be in accordance with the OAIC's Enterprise Agreement which can be found here: http://www.oaic.gov.au/about-us/corporate-information/key-oaic-documents/oaic-enterprise-agreement-20112014

General Information

Please read the information for job applicants on the OAIC website, which provides general information on applying for these positions. In that material you will find information about eligibility, the selection process, how to prepare a statement of claims and the Applicant Details form. Any further information required should be sought from the contact officer.

Applications should consist of the following:

- One page covering letter
- Resume or CV
- A statement against the selection criteria.
- Applicant Details Form (.doc) (.pdf).

Applications should be submitted by COB Monday 27 April 2015.
Please note that the Australian Human Rights Commission administers the recruitment function for the Office of the Australian Information Commissioner.

Please send your application to the Human Resources Officer C/- Australian Human Rights Commission:

by email to: oaicjobs@humanrights.gov.au
or
by mail to: GPO Box 5218 Sydney, NSW, 2000

Selection Results

You will be advised of the outcome of the process by email.

Further details about the role, its duties and the selection criteria are at: http://www.oaic.gov.au/about-us/careers/adviser-aps6-rs-april-2015

PRIVACY EVENTS

Time, Date & Location	Information	Price
SYDNEY Friday, 24 April 2015, 1 – 2 pm Venue: Level 10, 50 Martin Place Sydney CBD	**Privacy Act 1988 Update - Post law reform and beyond** Australian Privacy Commissioner Timothy Pilgrim will examine the significant changes post implementation of the amendments to the Privacy Act 1988. The seminar is being hosted by the Privacy Law Committee of the Business Law Section of the Law Council of Australia and will provide an opportunity to learn more about and consider: • the important changes under the Privacy Act • regulatory guidance on key aspects of the Privacy Act, such as security, • data breach and cross border disclosure of personal information • how the Privacy Act is being applied and administered by the Privacy Commissioner • trends in enforcement of privacy and data protection regulation • challenges presented by the online and social media environment • further developments in this area of the law	Cost: $25 For registration form, email carol.osullivan@lawcouncil.asn.au Queries to Carol O'Sullivan, Business Law Section, Law Council of Australia, C/o 3/31 Hi Tech Drive, Kunda Park QLD 4556. Tel: (07) 5450 1127
SYDNEY Monday 4 May 2015 7.30am-9.30am Westin Hotel, 1 Martin Place, Sydney	**OAIC PAW Business Breakfast – *Privacy, Living in the Future*** Join Privacy Commissioner Timothy Pilgrim at this breakfast hosted by the OAIC to launch Privacy Awareness Week	Check the OAIC's website for further details: http://www.oaic.gov.au/news-and-events/privacy-awareness-week/what-s-on-in-2015
MELBOURNE Tuesday 4 May, 5.00pm (5.30pm start) – 7.00pm Minter Ellison Lawyers L23 Rialto Towers 525 Collins Street, Melbourne CBD	**iappANZ Privacy Awareness Week (PAW) event** ***Privacy – Living in the Future*** **Professor Fred Cate with Timothy Pilgrim (Australian Privacy Commissioner) and Dr Margaret Simons (Associate Professor / Director, Centre for Advancing Journalism, University of Melbourne)** ***"We need to take data security and privacy seriously, and act accordingly, or stop pretending that we do."*** **Professor Fred H. Cate.**	iappANZ members FREE Non-members $99 (Cost deductible from iappANZ membership joining fee) E: emma.heath@iappanz.org or www.iappanz.org

Time, Date & Location	Information	Price
WELLINGTON Wednesday, 5 May, 4.30pm KPMG 10 Customhouse Quay Wellington	iappANZ Privacy Awareness Week (PAW) event: *'Privacy everyday'* • Professor Fred Cate • Russell Burnard, Chief Government Privacy Officer, Department of Internal Affairs	FREE REGISTRATIONS: Abigail Win: awin@kpmg.co.nz
AUCKLAND Thursday 6 May, 7.30am (for 7.45am start), finish 9am KPMG 18 Viaduct Harbour Avenue Auckland	**iappANZ Privacy Awareness Week (PAW) event**: *'Privacy everyday'* • Professor Fred Cate • Joy Liddicoat, Assistant Commissioner (Policy and Operations)	**FREE** **REGISTRATIONS:** **Abigail Win:** **awin@kpmg.co.nz**
SYDNEY **Friday 8 May, 9.30am-11.30am (registrations from 9am)** **Museum of Sydney, cnr Phillip and Bridge Streets, Sydney**	***Privacy Matters Forum* – Privacy Awareness Week (PAW) event** Presented by the Information and Privacy Commission NSW in partnership with the Office of Finance and Services and First State Super. Keynote address by the NSW Customer Service Commissioner Michael Pratt followed by an expert panel discussion on privacy issues (moderated by Philippa McDonald). The forum will bring together leaders, managers and practitioners from across NSW government sectors and business to discuss why privacy should matter to their organisation (because it does to their customers) and the importance of customer-centred service delivery.	FREE – but registrations essential Members of iappANZ can RSVP by 24 April 2015 via this link **https://nswprivacymattersforum.eventbrite.com.au**
SYDNEY Friday 8 May, 3.00pm – 5.00pm Gilbert + Tobin Lawyers L37 2 Park Street Sydney CBD	**iappANZ Privacy Awareness Week (PAW) event** **Panel discussion with:** • Professor Fred Cate • Timothy Pilgrim (Australian Privacy Commissioner) • Dr Elizabeth Coombs (NSW Privacy Commissioner) • Peter Leonard (Gilbert + Tobin) • Sarah Davis (The Guardian)	iappANZ members FREE Non-members $99 (Cost deductible from iappANZ membership joining fee) E: emma.heath@iappanz.org or www.iappanz.org
WELLINGTON	**Identity Conference 2015, New Zealand** *Enabling digital identity and privacy in a connected world*	For full registration details and to register online, visit the conference website

Time, Date & Location	Information	Price
Monday 18 & Tuesday 19 May Museum of New Zealand Te Papa Tongarewa Cable Street, Wellington	**Workstream topics and speakers:** • Service transformation (1) • Cybersecurity • Data analytics • Privacy-by-design • Service transformation (2) • Cybercrime • Transparency and digital citizenship • The world of sensors and the Internet of Things Confirmed workstream speakers are: • **Richard Foy,** Department of Internal Affairs • **Vikram Kumar,** Swerl IO Ltd • **Bianca Mueller,** LawDownUnder • **Roger Dennis,** Sensing City • **Dave Lacy,** ID Care • **Evan Stubbs,** SAS • **Ross Hughson,** My Info Safe • **Kathryn Dalziel,** Taylor Shaw • **Laura Bell,** SafeStack The full conference programme will be published soon.	
Date postponed and to be confirmed **4pm-7pm** Baker McKenzie Lawyers L27, AMP Centre 50 Bridge Street, Sydney	**Pharmaceutical Industry and Privacy** **Speakers include:** **Anne-Marie Allgrove** – Partner, Baker McKenzie **Malcolm Crompton** – Director, IIS **Jessica Kanevsky –** Legal Counsel, Abbvie **Greer Harris** - Regional Privacy Officer, Asia Pacific, AstraZeneca	Free for iappANZ members $99 plus GST for non-members Registrations – admin@iappANZ.org

IAPP Certification

Privacy is a growing concern across organizations in the ANZ region and, increasingly, privacy-related roles are being made available only to those who can demonstrate expertise. Similar to certifications achieved by accountants and auditors, **privacy certification** provides you with internationally recognized evidence of your knowledge, and it may be the edge you need to secure meaningful work in your field.

The International Association of Privacy Professionals (IAPP) says:

> *'In the rapidly evolving field of privacy and data protection, certification demonstrates a comprehensive knowledge of privacy principles and practices and is a must for professionals entering and practicing in the field of privacy. Achieving an IAPP credential validates your expertise and distinguishes you from others in the field.'*

What certifications are available? Are they relevant to my work here?

The IAPP offers four credentials, one of which is particularly relevant to iappANZ members, namely the Certified Information Privacy Professional/ Information Technology (CIPP/IT).

To achieve this credential, you must first successfully complete the Certification Foundation. The Certification Foundation covers basic privacy and data protection concepts from a global perspective, provides the basis for a multi-faceted approach to privacy and data protection and is a foundation for distinct IAPP privacy certifications – in our case, CIPP/ IT. CIPP/IT assesses understanding of privacy and data protection practices in the development, engineering, deployment and auditing of IT products and services.

What about testing?

Although the IAPP website refers to US-based certification testing only, testing is available to iappANZ members locally. The IAPP will continue to manage certification registrations and materials, but you will now be able to set an appointment to sit your exam online at a testing center in Australia or New Zealand.

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)

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