President’s Letter

By Anna Kuperman
President
M: 0419 803 263

Dear Members

A big thanks to all of our members who took the time to complete a recent short survey circulated by our General Manager. I am told that we had an exceptional response rate, which I think reflects on the levels of member engagement and participation we have at iappANZ. Please be assured that we take all of your input on board both in our sub-committee and Board discussions and aim to respond to your suggestions in how we interact and run events for our members.

On this note, I attended our Privacy in Pharma event, hosted by Baker & McKenzie earlier this month, which I expected to be a small intimate gathering of pharma folk dealing with privacy in their day to day working lives. Well, it turned out to be much larger than that, with people from the medical software industry, Medicines Australia, health compliance regulatory and policy functions. There was a great energy in the room facilitated by moderator, Malcolm Crompton and a good deal of specialist knowledge shared by panellists, Jessica Kanevsky (Legal Counsel, Abbvie), Greer Harris (Regional Privacy Office, AsiaPac, AstraZeneca) and Anne Marie Allgrove (Partner, Baker & McKenzie).

We welcome suggestions from our members on any topic or specialist area that they feel they can share in a similar, so that we can spread the valuable knowledge our members have and their practical experience to benefit those working in this space.

Now to some overt marketing! You will have started receiving Summit updates from us leading up to our Privacy@Work (18 November 2015) in Melbourne. For those of you who have attended our previous Summits, you know what to expect! Great content, global & regional insights, hearing from peers across functions, industries and countries and contributing to knowledge sharing and member connections. From my own experience, I attended my first iappANZ Summit in 2011 so this will be my 5th Summit, and each time there is without fail, new knowledge gained, new friends made and new learnings to bring back to the working hub.

Last month, we announced our three exceptional keynote speakers and NOW, I am excited to give you a further sneak peek into our 2015 contributors. There will be more to read in coming weeks so I will keep this one short & sweet! This is only
half of it! Register for Early Bird Pricing to secure your seat at one of the most pre-eminent forums for professionals working in the privacy sphere in ANZ. We have limited spaces at Zinc, Federation Square so don’t miss out.

- **Timothy Pilgrim**, Acting Australian Information Commissioner
- **Russell Burnard**, Government Chief Privacy Officer, Internal Affairs, New Zealand
- **Ben Carr**, Chief Privacy Officer, Telstra
- **Adrian Anderson**, former GM, AFL Football Operations and Media, Sports Law Barrister
- **Peter Leonard**, Partner, Gilbert + Tobin and Board Director of iappANZ
- **Anne Marie Allgrove**, Partner, Baker & McKenzie
- **Steve Wilson**, Digital Identity, Innovator & Analyst, MD Lockstep Consulting
- **Ron Bartsch**, Leading Aviation Expert & Chairman, UAS International
- **Dr Grant Davies**, Victorian Health Services Commissioner
- **Patrick Gray**, Information Security Journalist, Risky Business Podcaster and Blogger
- **John Pane**, Regional Lead Privacy Compliance + Data Protection APAC, Johnson & Johnson
- **Michael Rivette**, Barrister
- **Sam Stover**, Cyber Security Specialist, iSight Partners

Happy reading!

Anna
Adrian Wood, Director of WHITEHACK opens this edition of Privacy Unbound with some findings from the inaugural Australian Cyber Security Centre’s (ACSC’s) threat report, released late in July. As a pen tester, Adrian gives us an insider’s look at real world attacks and why security must become a front and centre issue for consumers and government alike.

Credit reporting providers are set to obtain comprehensive credit reporting information from credit reporting bodies, with authorisation from the ACCC now likely. In her article, Minter Ellison Associate Tarryn Wood outlines the ACCC’s current position on the Principles of Reciprocity and Data Exchange (PRDE) proposed by the Australian Retail Credit Association (ARCA) which will enable more sharing of credit reporting information, including consumer credit liability information and repayment history information. Some concerns remain about the potential for a two tier system under the principles.

CEO of Healthlink and Board Director of iappANZ, Tom Bowden examines the challenges to patient confidentiality and privacy in a digitised world. Technology offers boundless opportunity to bring about better health outcomes for patients through more effective information sharing, yet many healthcare IT projects are plagued with privacy hurdles. Tom offers some international examples of digital patient record initiatives (most of which - with the exception of Scotland - have had limited success). What lessons can we learn from Scotland? Turn to page 8 to find out.

Timothy Pilgrim has assumed the role of Acting Australian Information Commissioner, exercising all of the functions and powers under the Privacy Act 1988 (Cth) as well as those under the Freedom of Information Act 1982 (Cth). In this contribution, Timothy reflects on complaint numbers from FY15, shares his views on the impact of the hacking of the Ashley Madison website on Australian consumers and outlines the focus that his team will have in relation to data retention, national security and law enforcement as well as eHealth over the coming year.

Did you know that in New Zealand, the use or disclosure of publicly available personal information is now only permissible if it is fair or reasonable? Katherine Gibson, Legal Counsel for Centrix Group in Auckland and principal of Gibsons Law, sheds light on this quietly introduced amendment to the New Zealand Privacy Act 1993, introduced to combat the ease with which personal information can become publicly available from open websites and social media sites and cause privacy harms.

Peter Leonard, G+T Partner and iappANZ Board Director looks at the access regime that will apply to the data that communication service providers must retain under the changes to the Telecommunications (Interception and Access) Act 1979 (Cth) and consequential changes to the Telecommunications Act 1997 (Cth) that were passed by the Australian Parliament with bipartisan support earlier this year. In particular, he opens the door for us on an important debate that we privacy professionals should be having about balancing the potential ability for civil litigants to also access the data, against the potential for privacy invasive subpoenas to require the disclosure of an ever richer set of data about ourselves.

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

Last but not least, it is a mere 3 months until the iappANZ’s annual privacy summit “Privacy@Work”. This year we’ll be taking over Zinc at Federation Square in Melbourne to bring you world leading keynote speakers, Bojana Bellamy, Marie Shroff and Hilary Wandall as well as a raft of amazing people from all walks of privacy life and beyond. Turn to page 24 for all the information you need to book your ticket.

We hope you enjoy this edition of Privacy Unbound.

Melanie
A message about iappANZ membership:

Membership benefits

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

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

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

You can access benefits available to you through your iapp account. Simply login to your MyIAPP account using your email address as the username. If you do not yet have a password or have forgotten yours just click on the “Reset your password” link and instructions on how to create a new password will be sent to you. 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.

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

Increase in membership fees from 1 August 2015

Please note that, as advised in our previous edition of Privacy Unbound, iappANZ has introduced a membership fee increase and a new tiered fee structure as of 1 August 2015. More details are on page 23 of this issue of the journal. Please email admin@iappanz.org if you have any membership queries.

Emma Heath, iappANZ General Manager

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

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

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

Our LinkedIn group is: http://www.linkedin.com/groups?qid=1128247&trk=anetsrch_name&goback=.qdr_1281574752237_1

Follow us on Twitter at: https://twitter.com/iappANZ
The ACSC signals business and government must move beyond regulatory compliance to address real world cyber threats

by Adrian Wood

The inaugural Australian Cyber Security Centre (ACSC) threat report was released on 29th July.¹ The report is a collaborative effort of several Federal Government departments, including the AFP and Intelligence agencies. It paints a pretty bleak outlook for cybersecurity beyond 2015: an increase in attacks, attackers, their ‘sophistication’ and their destructive capacity. It calls for vigilance and a proactive approach to cybersecurity from all aspects of the Australian community. This article look at some of the key take home messages from the report for privacy professionals.

First, the report outlines the growing sophistication of cyberattacks, and highlights the difficulty governments and business face in detection. The agencies collaborating on this report freely admit to gaps in both their ability to understand the threats and to building relationships with business in order to improve collaborative understanding of cybersecurity and the ability of the public and private sectors to identify and react to malicious activity.

Second, the report correctly identifies that greater emphasis needs to be placed on the ICT security community, academia and decision makers, in order to keep pace with the changing threat landscape.

It could be argued that the security community has been ‘jumping up and down’ for years, and only in recent years have things like dedicated IT Security majors and masters joined the offering of a select few universities here in Australia. There is a lot of work to be done by academia to prepare more information security professionals for the increase in cyber security issues.

Third, whilst the report focuses on high risk areas of critical national importance, or the usual suspects, such as banking and finance, energy, communications, defence and transport, it reveals some interesting deductions that will hopefully ring true:

- the ACSC relies largely on self-reporting; and
- even in the high risk areas which are subject to compliance and legislative frameworks, cyber security is not receiving the investment it should; and
- detection rates are not a reflection of the number of issues.

To demonstrate, if CERT (Computer Emergency Response Team) responded to 153 attacks in 2014 on critical infrastructure, how many attacks went unnoticed due to a plethora of issues, from failure to detect through to simply a failure to (voluntarily) report?

I believe failure to detect and the implications of this are a key issues that needs to be addressed.

As a penetration tester, I am cynical when it comes to this number of detections. From experience, most businesses, even those that meet their information security and privacy protection obligations, are still extremely vulnerable to real-world attacks, and thus their ability to detect and report is hamstrung, as outlined in the ASCS report.

What I call a ‘real-world attack’, is described in reports such as this as a ‘sophisticated attack’. I think there is a problem with referring to real-world attacks as ‘sophisticated’ because of the impact this has on the mindset of information security and privacy professionals, and also the impact it has on decision makers.

My reasoning is this - that the underlying methodology behind real-world or ‘sophisticated’ attacks has not changed in a really long time. Yes, the codebase for some attacks becomes more complex (thereby increasing the barrier to entry to ‘hack up’ your own attack). The numbers don't lie. The number of attacks recorded increases year-by-year. So calling it ‘sophisticated’ is really an inaccurate representation of the situation. For one, the term ‘sophisticated’ makes it sound like dealing with the issue is far more complex and expensive at the organisational level than it really is. Dealing with a ‘real-world’ issue also sounds far more palatable than dealing with a ‘sophisticated’ one. If we identify that ‘sophisticated’ attacks are the real threat facing business and redefine them as ‘real world’ attacks, there will be greater opportunity for movement in a positive direction.

The underlying theme of both this piece and the ACSC report is that security must, in the eyes of regular Australians, government and business become a front-and-centre issue at all organisational levels. It must also move beyond compliance. Fast. The nature of real-world attacks is that current compliance standards probably won’t save you from a breach.

To say that is probably a bold claim, sure. However, if one looks at what is typically required to be compliant to any regulatory standard in this country, you’ll find that the types of attacks penetration testers see (and do) and what is outlined in the ACSC report don’t reflect what is required in order to attain compliance. This means that an organisation can invest a significant sum of money in compliance but still be vulnerable to this real world attacks.

What is needed?

Organisations need to be more innovative in their approach to cyber security; most are still using the same approaches and techniques they were using 10 or 15 years ago, but at a much greater cost. Network and application monitoring has made some truly amazing advances in the past few years, and most are seriously underutilized and understood. We need a rapid shift in the way we approach network monitoring to reflect new innovations that make network and application security management easier.
Will this report result in a further call for a tightening of regulatory requirements for privacy and security? It seems that the approachable language of the report coupled with pressure from issues such as the increase in high-profile breaches, proposed changes to European data protection laws (i.e. GDPR) and the call (again!) for an introduction of a mandatory data breach notification scheme in Australia, might be a forebear for such action to be called for from a wider section of the community. Hopefully though, the platform is not used as leverage for a future reduction of individual liberties and privacy.

A call for businesses to be ‘proactive’ alone will not be enough, when it has already been demonstrated time and again by privacy professionals the financial and PR loss that can be incurred from a breach that results in the loss of private information due to a failure to take security seriously at all levels. I look forward to reading the latest proposal regarding mandatory data breach notification due later this year.

Adrian Wood is the Director of WHITEHACK, an information security consultancy based in Australia. He is also an adjunct network security analyst at the University of New England, Armidale. He can be reached at adrian@whitehack.com.au
Comprehensive credit reporting now a step closer as principles look set to be approved

by Tarryn Wood

Almost 18 months after its introduction, comprehensive credit reporting may be a step closer to becoming a reality after the ACCC indicated that it is likely to authorise the Australian Retail Credit Association Ltd (ARCA) to implement the Principles of Reciprocity and Data Exchange (PRDE).

The ACCC can authorise conduct that might otherwise fall foul of the competition provisions of the Competition and Consumer Act 2010 (Cth) if it is of the view that the public benefit outweighs any public detriment, including any lessening of competition.

ARCA, whose members include many of the major credit reporting providers and credit reporting bodies, and other supporters of the PRDE, say that the provisions will provide the public benefits of reciprocity, consistency and enforceability, and they will also enhance responsible lending and risk management capability across the industry.

In announcing its intention to grant authorisation, the ACCC said that it believes that the PRDE ‘will help overcome a reluctance in the industry to share consumer credit information, facilitating a more complete exchange between credit providers and each credit reporting body. This will lead to increased competition both between credit reporting bodies and between lenders and assist lenders to comply with their responsible lending obligations at less cost.’

Under ARCA’s proposal, credit providers (CPs) would agree to only obtain credit reporting information from credit reporting bodies (CRBs) who are signatories to the PRDE, and CRBs would agree to generally only supply comprehensive credit reporting information (ie, consumer credit liability information and/or repayment history information) to CPs who are signatories to the PRDE. CPs who were not signatories would still be able to exchange negative credit reporting information with CRBs and they are not obliged to sign up to the PRDE.

However an oddity of the PRDE is that it also contains a provision that would allow signatory CRBs to receive comprehensive credit reporting information from CPs that are not signatories, and to provide them with comprehensive credit reporting information received from other non-signatory CPs. As highlighted by Dun & Bradstreet in its submission to the ACCC, this could result in two parallel streams of information, where a CRB may return significantly different information for a consumer depending on whether the CP making the enquiry is a signatory or a non-signatory.

To date, most submissions received by the ACCC appear to generally support the authorisation of the PRDE. There has however been some opposition from consumer groups, which appears to flow from their opposition to a comprehensive credit reporting regime at large. Veda, Australia’s largest CRB, has also expressed concerns and submitted that a comprehensive credit reporting regime would be better governed by a private system of bilateral agreements between CRBs and CPs, with a set of non-binding principles of reciprocity. ARCA has however countered that this proposal would benefit Veda while putting the other CRBs and CPs at a disadvantage.

Submissions in relation to the ACCC’s draft determination to grant authorisation closed on 14 August 2015.


Tarryn Wood is an Associate at Minter Ellison.
Applying the Hippocratic Oath to patient privacy in an Electronic Age

by Tom Bowden

Whatever, in the course of my practice, I may see or hear (even when not invited), whatever I may happen to obtain knowledge of, if it be not proper to repeat it, I will keep sacred and secret within my own breast. From the Hippocratic Oath - 500 B.C.

There is growing awareness that the key to successful healthcare information technology is designing systems that protect patient privacy. Information technology has advanced so quickly during the past two decades that it is now possible to do previously unimaginable things. Data transmission speeds and data storage costs have improved exponentially and enormous advances have been made in fibre-optics, device miniaturisation and satellite data transmission. The cost of using information technology has plummeted and what can be achieved with it is increasing at breath-taking speed.

Today the key limitation to using technology in healthcare is the lack of widespread understanding of how to maintain a patient’s privacy in an ever more connected and computerised world.

We need to find ways of giving a patient confidence that he or she is being given the best possible healthcare, while at the same time feeling comfortable that his or her personal information is not being seen by others. There is a lot at stake here. There is clear evidence that patients will withdraw from the all-important doctor patient relationship if they are concerned that their medical details may be more widely divulged than they would wish for.

A real or perceived withdrawal of confidence in the integrity of the doctor-patient relationship will cause patients to be less forthright about problems and symptoms. This lessens the physician’s ability to diagnose and cure. So it is ‘mission critical’ that ways to improve healthcare delivery without compromising privacy are found.

Why is Information Technology viewed as so important in healthcare?

Today there is a great deal of pressure to make healthcare more efficient because of the growing cost of supporting an older population, combined with better and ever more expensive treatment options. Healthcare has become one of the major costs to governments everywhere and the cost of healthcare as a proportion of government expenditure continues to expand in all OECD countries.

There has been an increasing focus on the potential of information technology to make healthcare delivery more efficient. Significant investment has been made in information technology, spurred on by a US Government sponsored RAND Corporation report in 2005, “Health Information Technology - Can HIT Lower Costs and Improve Quality?” This very authoritative report concluded that, properly implemented and widely adopted, health information technology would significantly improve healthcare quality and achieve annual savings for US healthcare of $77 billion or more.

Less apparent however was any evidence of how best to utilise technology to achieve these purported savings. Since that time, there have been significant investments made. However very few national or even regional initiatives have been highly successful. The predominant approach continues to be the ‘joining up of healthcare information’ with a focus on making information about a patient available wherever and whenever that information might be needed.

There are a number of challenges facing large healthcare IT projects, but perhaps the biggest is privacy: ensuring that patient-related information is readily accessible whenever it is needed, but delivered in a manner which ensures the patients’ privacy is not compromised, ever.

There is a lot at stake here. If patients become concerned that their personal information may become known to people that don’t have appropriate reasons for accessing it, they can become reluctant to be as open as perhaps they should be. A 2011 survey of 10,000 US consumers in 49 states by The New London Consulting Group showed that 27.6% of respondents would postpone seeking care for a sensitive condition if they had privacy concerns. As the New London Consulting Group report concludes
“Accurate information is the bedrock upon which physicians assess medical conditions and hence determines the treatment patients receive. When this information is withheld or even falsified, fundamental treatment assumptions are impacted.”

The problem is easy to identify but what is the answer?

As yet there are no clear-cut answers about how best to use information technology to inform healthcare delivery. A number of initiatives have been undertaken around the world and very few of them can claim any measure of success. Some examples of these initiatives are:

- The UK National Health Service (NHS) implemented a highly ambitious shared record system called the Summary Care Record (SCR). It failed and was halted in 2011. Efforts to resurrect the SCR are still under discussion, with the latest development being that 700,000 people have opted out of the government’s proposed “care.data” initiative. This is an enormous blow to the ongoing efforts of the NHS to create shared electronic health records and is clear evidence of an unprecedented growth of concern about individual privacy.

- The US still has one of most fragmented healthcare systems in the world despite $36 billion in taxpayer funded investment to develop electronic medical records systems over the past five years. While significant efforts have been made to improve the level of IT use in healthcare, there is still a very long way to go and efforts to exchange patient information and create shared electronic health records have been particularly slow.

- In Holland, efforts to turn a highly successful regional initiative into a national shared electronic health records system have stalled because of insufficient support from the general public.

- In Denmark, which has long been regarded as the world’s most advanced user of healthcare IT, a national scandal over the covert expansion of a national shared GP records database has meant that the database has been turned off completely since November 2014. There is an ongoing public debate as to whether the initiative will ever be restarted.

- Australia’s personally controlled electronic health record (PCEHR) has been extremely problematic and its viability is still uncertain. The PCEHR’s future success will depend upon whether the Australian people accept an opt-out privacy model which is being proposed.

In all of these countries, patient privacy is one of the major stumbling blocks. In most cases it appears to be the predominant barrier to making meaningful progress.

Where to from here?

Only one country appears to have been particularly successful in integrating medical records across providers on any scale, and that country is Scotland1, where general practices’ computer systems provide information each day to inform emergency care providers about patients’ underlying allergies, current illnesses and use of medicines. That information is used as part of every after-hours or emergency department admission. The Scottish Emergency Care Summary (ECS) appears to have been successful for a number of key reasons:

- It has been implemented at a local level, rather than nationally.
- Only a small subset of patient data is shared (not the entire record).
- The system was set up by GPs for use by GPs.
- Considerable effort has gone into ensuring that patients and healthcare providers are supportive of information sharing and will work together to ensure that patient privacy is respected.

---

1 Dr Libby Morris spoke about the Scottish experience at the iappANZ Summit in November 2014.
What can we learn from the Scottish experience?

We now know that information from a patient’s existing medical record can be useful in an emergency situation and that if all of the parties involved in sharing that information can work together carefully, a trusting environment can be established.

The Scottish experience also indicates that primary responsibility for the care of patient data should be given to the patient’s own doctor, rather than to some form of national or regional system.

After all, responsibility for confidentiality of a patient’s personal information has been the responsibility of the individual patient’s personal physician for more than 2,000 years. Ensuring that information sharing is carefully managed in an environment of trust is of paramount importance. Doing that job well is key to maintaining the doctor patient relationship and essential to the overall integrity of the health system itself.

Tom Bowden is a Board Director of IAPPANZ and sits on its New Zealand sub-committee. Tom is also CEO of Healthlink in New Zealand.
What’s on the privacy agenda for the Office of the Australian Information Commissioner?

By Timothy Pilgrim, with Melanie Marks

Q1: We understand that Professor John McMillan AO has been farewelled from his position of Australian Information Commissioner. What does this mean for the OAIC?

The OAIC has farewelled Professor John McMillan AO, who brought a wealth of experience to his role as the inaugural Australian Information Commissioner. Professor McMillan is taking up his new role as Acting NSW Ombudsman and I wish him well.

During his time as the Australian Information Commissioner, Professor McMillan has upheld and promoted government information as a national resource, recognising its importance in aiding better policy and decision-making. In the spirit of the Freedom of Information Act, he also worked to embed a culture of openness and transparency in Australian Government agencies, and to streamline and support access to government information.

With Professor McMillan’s departure and the completion of my term as Australian Privacy Commissioner on 19 July, I have been appointed as Acting Australian Information Commissioner for a period of 3 months. In this capacity, I will continue to exercise all of the functions and powers under the Privacy Act as well as those under the Freedom of Information Act.

Q2: What can you tell us about the complaint numbers for FY15 compared to the preceding year?

While there was a decrease in privacy complaints received in this financial year comparative to last financial year, complaint numbers continue to remain high. The significant increase in complaints received in 2013-14 was partially attributable to privacy law reform, changes to credit reporting and two significant data breaches that occurred during the 2013–14 financial year. However, the 2840 privacy complaints that we received in 2014-15 represent an 89% increase on the 2012–13 financial year, showing that community awareness and concern about privacy remains high.

Q3: With mandatory data breach notification legislation looming, has the OAIC seen an increase in voluntary notifications in FY15?

The OAIC received 110 voluntary data breach notifications in the 2014–15 year, which is a 53% increase on the 2013–14 year. And our Enquiries line is certainly keeping busy — we received a total of 18,062 enquiries in the 2014–15 year, of which 12,251 related to privacy and 1,902 related to FOI (with the remainder relating to administrative or access issues).

Q5: Since your last article in Privacy Unbound, the world has seen the high profile hacking of adult dating website Ashley Madison. What impact will this event have on consumers in Australia?

High-impact data breaches continue to hit the headlines, with one recent large-scale breach being the hacking incident of the adult dating website ‘Ashley Madison’. This follows close on the heels of the Adult Friend Finder hack that occurred a couple of months ago. Incidents like these highlight the increased security risks that may be faced by organisations that deal in sensitive personal information.

Given the significant impact that these incidents may have on the privacy of Australians, the OAIC has reached out to the companies involved to seek further information.

Large-scale data breaches are deeply concerning, as the amount of sensitive personal information stored and shared online continues to increase, and the risk of serious harm to individuals also increases. In situations where a data breach affects a company that operates across national borders, it is important for regulators to operate collaboratively. As such, I contacted my colleagues in other relevant jurisdictions to minimise duplication and promote international consistency.
Q6: What are some of the key focuses for your team over the coming year?

**Data retention, national security and law enforcement**

In the May budget, the OAIC was given additional funding to undertake privacy oversight of the implementation of mandatory telecommunications data retention scheme. The OAIC will also be looking at the implementation of the *Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014* (Foreign Fighters Act) which introduces changes to the handling of personal information. To this end we have put together a new national security team, working on privacy assessments and advice.

In relation to the mandatory data retention scheme, we will be working with telecommunications service providers to help ensure that privacy protections are built into their practices, procedures and systems.

Over the last few months we have worked closely with Department of Immigration and Border Protection (DIBP) as they undertake privacy impact assessments on changes to the collection and handling of personal information under the Foreign Fighters Act. Over the next year we will be conducting assessments of DIBP’s handling of personal information under that legislation.

**eHealth**

The OAIC has just signed a new memorandum of understanding with the Department of Health for the 2015–16 year, and in the coming months, we will work with them as they start on the implementation of trials for changes to the eHealth system, including trialling a change from opt-in to opt-out consumer participation. Following on from our submission on the Department of Health’s *Electronic Health Records and Healthcare Identifiers: Legislation Discussion Paper*, we will work with Health on a variety of matters, including commenting on the privacy aspects of draft legislation as it becomes available, providing privacy advice on issues related to the trials, and developing guidance for participants covered by the trials. We are also continuing our assessment work on the eHealth system.

We are also working on a completely new suite of privacy resources for healthcare professionals and for individuals. Following initial consultation with peak bodies, this guidance, including 10 business resources and 2 consumer fact sheets, will be going out for public consultation shortly.

Timothy Pilgrim is now the Acting Australian Information Commissioner. Melanie Marks is a Board Director of iappANZ.
I know it is personal information, but it is publicly available so of course I can use it …

By Katherine Gibson

Not necessarily so in New Zealand, due to a quietly introduced amendment to its Privacy Act which now requires an enquiry into whether the use or disclosure of publicly available personal information is unfair or unreasonable. If it is, the publicly available exception cannot be relied upon. What does this mean for you as a privacy professional advising on the publicly available information exceptions?

A relatively quiet change

The change came in the form of the Harmful Digital Communication Act 2015, which was largely heralded as legislation to stop cyber bullying and provide a simple process for victims of cyber bullying to remove abusive material from the Internet. The Act also amended s56 of the Privacy Act 1993, the provision exempting personal information relating to domestic affairs from the Privacy Act. This exemption no longer applies where the collection, disclosure or use of the personal information would be highly offensive to an ordinary reasonable person – an appropriate response to handling personal information in the domestic context.

At the same time, amendments were made to the often relied upon publicly available information exceptions in the Privacy Act when using and disclosing personal information. It was considered necessary to update the Privacy Act to respond to the ease with which personal information can become publicly available from open websites and social media sites which may cause privacy harms.

It is surprising that the amendments went largely unreported until they came into force. There was no public debate about them. It may be that the changes will have little impact on the use and disclosure of information publicly available and so they did not warrant much attention. The Privacy Commissioner has said that the amendments will only apply to a small portion of cases as the legal thresholds are quite high. Only time will tell, but I predict that the changes will present challenges to privacy professionals. Notions of fairness and reasonableness require frameworks to work within. Whilst the current Act does have similar tests in the collection principle and so the jurisprudence here may offer some assistance, it is likely that there will be different issues to consider for unfair or unreasonable use or disclosure.

The new publicly available information exceptions – what are they?

Personal information obtained for one purpose cannot be used for another purpose, or disclosed, unless the agency believes on reasonable grounds that the information is sourced from a publically available publication and in the circumstance it would not be unfair or unreasonable to use or disclose the information.

The onus is on the agency/person relying on the exception to show that the use or disclosure is not unfair or unreasonable. What are the relevant considerations that you should take into account when advising on whether the exception is invoked? They may include:

1. Was there a reasonable expectation of privacy by the individual concerned that this information will not be used or disclosed in this way?
2. What is the purpose of the use or disclosure?
3. Is the information sensitive? The more sensitive the information is, the more likely the use or disclosure of it may be unreasonable or unfair.
4. If filming or photographs are involved, was the filming/photography overt or covert?

The devil is always in the detail. So let’s apply the new law to some well-known facts.

---

1 Information Privacy Principles 10(a), 11(b).
3 Agency fro the purposes of the NZ Privacy Act includes a private and public sector entity.
The Christchurch office workers’ romp

Earlier this year there was significant publicity over the filming of two work colleagues having sex at their workplace in Christchurch. It was at night and the lights in the office made it easy for people from a bar across the road to see them. Some in the bar filmed and photographed the couple, and the photographs and recordings were uploaded onto social media sites and mainstream news websites. The couple were identifiable.

The film and photographs quickly became publicly available. Before the amendments, those sharing this information could point to the public information exception in the use and disclosure principles. Would this be the case now? Is it not unreasonable or unfair to share this information? Let’s consider some of the issues.

Was it reasonable for the couple to expect privacy and that what took place would not be filmed or revealed to anyone? It is not a public place, but is it a place where a reasonable person could expect not to be seen? It was an office place for a number of other workers. It is not at home behind closed doors, where privacy could reasonably be expected. But it was at night and perhaps all their workmates had left for the day and so they probably assumed they were in a private place. They were not thinking of the bright office lights (obviously) that allowed them to be seen from outside the office building. Would a reasonable person expect that they would be seen from outside the office? At least one privacy commentator at the time was reported as saying that in these circumstances (open windows, lights on, in a location across the road from a bar) there could be no reasonable expectation of privacy.

What was the purpose of uploading and sharing the information? Curiosity? To embarrass the couple? Just having a laugh? Some would say they deserved it as it showed their employers and their partners what they were up to. Are such moral and social issues relevant to whether the use or disclosure is unfair or unreasonable?

How sensitive is the information? To some, not sensitive at all. To the couple concerned, undoubtedly it was sensitive.

It is clear the couple did not know they were being filmed, but it was hardly covert filming in the sense that hidden cameras were used. The filming taking place was obvious to those in the bar and the filming took place from what was generally a public place.

There are likely to be other relevant factors to consider, but the brief analysis above demonstrates that the exercise is not straightforward and that some factual situations will present challenges to advisers. Which side of the line do you fall on this one – unfair or unreasonable, or not?

The swearing cake case

You may recall my article about the swearing cake case that appeared in the March/April 2015 edition of Privacy Unbound. This is a significant case in the development of New Zealand’s information privacy laws, being the largest damages award ever handed out by the Human Rights Review Tribunal for unlawful disclosure of personal information. There has been plenty of commentary on the case.

In the article I referred to personal information about the cake maker taken from the decision of the Human Rights Review Tribunal that I had sourced from the Ministry of Justice website - a publicly available publication. Are the exemptions still applicable? Was the use and disclosure in that article not unfair or unreasonable? The considerations discussed above are probably not the most relevant in the analysis of this issue. Parties to litigation know that Tribunal hearings and decisions are public and the purpose of the article was to discuss important jurisprudence issues and provide commentary. It is difficult in this article to comment on whether the information was sensitive, but it is at the higher end of the sensitivity scale. The pertinent questions include whether it was necessary to use and disclose the personal information to discuss the issues and the substance of the case and whether an anonymised article would have achieved the same result.

---

4 Reports are that the man was married and his wife found out after seeing the images on Facebook.
On a broader level, do the amendments require writers of articles (not written by the media) discussing Court and Tribunal judgments to omit all personal information? I think not, but I will certainly ask myself whether I need to refer to personal information to report on the substance of cases, or the issues being discussed. It will be challenging, after all, privacy is all about personal information.

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 and is a member of iappANZ’s New Zealand sub-committee.

---

5 Media when undertaking their news activities are exempt from the Privacy Act.
Fishing by subpoena in the rising ocean of communications ‘metadata’: a debate yet to start

by Peter Leonard

Mandatory data retention for communications services has engendered criticism and controversy in many countries. Pervasive and extensive communications data collection and retention has been stated by many Governments, including the Australian Government, as necessary to address new threats of internet facilitated terrorism, child exploitation and human trafficking. Criticisms as to pervasiveness have been met with government reassurances as to limitations as to who can access the data and some safeguards as to permitted access and use.

Reflecting these reassurances, the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth) (*2015 Act*) passed through the Australian Parliament with a remarkable degree of bi-partisan support. Amendments to the Bill included a few safeguards suggested by critics of the Bill, but the scope of mandatory data retention remained largely unchanged from the Government’s initial proposals.

Safeguards on the release of mandatorily retained data

A number of the safeguards on access to and use of mandatorily retained data are of particular interest to privacy professionals. This article principally concerns one safeguard which has been the subject of surprisingly little comment. That safeguard is certain conditions imposed upon release of mandatorily retained communications data to persons other than intelligence services and law enforcement agencies empowered by provisions of the *2015 Act* to access that data, particularly in the context of civil litigation. The *2015 Act* revisits the pre-existing safeguards on disclosure, initially (and potentially only as an interim measure) limiting the circumstances in which the mandatorily retained data of telecommunications providers can be disclosed. But that is not the end of the story, it is only just the beginning.

Permitted disclosures under the Privacy Act

Readers will know that the *Privacy Act 1988* exempts certain disclosures of personal information by APP entities in ‘permitted general situations’, including where disclosure:

- “is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim”; and
- “is required or authorised by or under Australian law or a court/tribunal order”. There are many such laws: a variety of Federal, State and Territory Acts empower particular agencies to compel disclosure. For example, section 29 (Power to obtain documents and things) of the *Crime Commission Act 2012* (NSW) provides that an executive officer of the NSW Crime Commission with special legal qualifications may, by notice in writing served on a person, require the person to attend before the Commission at a particular time and place and produce to that officer a document or thing specified in the notice, being a document or thing that is relevant to an investigation.

Subpoenas of communications records in civil litigation

And, of course, subpoenas are frequently issued by courts on third parties, including telecommunications service providers, to produce communications records in a wide range of civil litigation. There are no reliable numbers as to the number of such subpoena each year. Given that over 550,000 requests for information about communications were made by Australian law enforcement agencies in the last reported year, one might suspect that the number of subpoenas for communications data is already very large. We can also confidently expect (absent any restriction) that this number is likely to substantially grow in response to availability of richer and deeper data sets collected by telecommunications service providers to meet mandatory data retention requirements.
Protection of communications information

Information about an individual's communications has long enjoyed a broader ambit of protection against disclosure than 'personal information' as defined under the Federal Privacy Act. Under section 276 of the Telecommunications Act 1997 (Cth), disclosure by a communications service provider of broad classes of information about an individual's communications which are protected by that provision, leads to criminal liability.

However, exceptions to section 276 already in operation before the 2015 Act, allowed service providers to respond to subpoena or other court or statutory compulsion, as well as to elect to make voluntary disclosure if “the disclosure is reasonably necessary for the enforcement of the criminal law” or “a law imposing a pecuniary penalty or for the protection of the public revenue”. In practice, most providers elected not to make voluntary disclosure of information about communications. This reluctance primarily stemmed from concern as to liability that might flow from them making an inherently subjective determination as to what is, or is not, “reasonably necessary”. Another reason for reluctance is that voluntary disclosures generally are not excepted from privacy laws and associated telecommunications codes with privacy-related provisions.

So, before the 2015 Act came into operation, communications service providers usually required either legal compulsion, such as a warrant or other Court order or a statutory notice to produce, or an agency to provide a written authorisation under the Telecommunications (Interception and Access) Act 1979 (Cth) (TIA Act) signed by an authorised officer of that agency.

Application of the Privacy Act to 'retained data'

The ability of communication service providers to disclose any data they are required to retain under the data retention regime has now changed. New section 187LA of the TIA Act provides that the Privacy Act applies to all communications service providers, to the extent that their activities relate to 'retained data'. That data, captured and stored to fulfil the data retention requirements, is taken for the purposes of the Privacy Act 1988 to be personal information about an individual where the information relates to the individual or a communication to which the individual is a party. (This may assist to resolve some of the current debate as to the scope of personal information held by communications providers about users of their services, as per Ben Grubb and Telstra Corporation Limited [2015] AICmr 35 (1 May 2015).)

When disclosure of 'retained data' will not be permitted

More significantly, the amendments made by the 2015 Act initially limit the classes of persons who may, using processes outside the 2015 Act, such as issue of subpoenas or exercise of statutory powers, compel disclosure of 'retained data'. The 2015 Act does this through an unusual provision, new section 280(1B) of the Telecommunications Act 1997. This provision is obscurely drafted due to multiple levels of double negatives, but appears to state that circumstances where disclosure would not be permitted (where they would otherwise meet the 'required or authorised by or under law' permitted disclosure under the Privacy Act) are:

- the disclosure is required or authorised because of a subpoena, a notice of disclosure, or an order of a court in connection with a civil proceeding; and
- the information or document is kept by a service provider "solely for the purpose of complying" with the statutory data retention obligation; and (cumulatively)
- the disclosure sought is not for the purpose of any of (a) complying with a written authorisation under the TIA Act; (b) complying with other warrants or authorisations under the TIA Act; (c) certain public interest disclosures provided for in the Telecommunications Act (e.g. an emergency warning, a call to an emergency services number, a threat to life situation, or preservation of human life at sea); (d) providing persons with access to their personal information in accordance with the Privacy Act 1988; and (e) a purpose prescribed by the regulations; or (e) a purpose incidental to any of these purposes.
Implications for the administration of justice

One practical problem with the operation of this complex prohibition will be how to determine, if called into question, whether a service provider is collecting or retaining information about communications "solely for the purpose of complying" with the requirements of the TIA Act, or whether the 'solely for the purpose' test is not met because collection is also for other purposes such as data analytics, service quality monitoring, billing verification or service assurance. The Revised Explanatory Memorandum (REM) states "This provision thereby ensures that telecommunications data that is collected, retained or used for a service provider's ordinary business purposes or other purposes unrelated to the data retention obligation, continues to be available for such [legal] proceedings". In practice this often will not be an easy determination.

The prohibition does not come into operation until the end of the implementation phase on 13 October 2015. During that time, or at any time thereafter, the Minister may prescribe exceptions to this prohibition, by regulation. The REM states that this regulation making provision "enables exceptions to be formulated with the benefit of, and informed by, detailed empirical information about the use and application of telecommunications data in civil proceedings and enables any anticipated practical impediments to the conduct of litigation to be appropriately addressed". The REM continues:

"telecommunications data is currently accessed by parties to many civil proceedings, including proceedings relating to international child abduction, family violence, and personal injury or economic harm as a result of negligence or professional malpractice. As the requirement for access depends substantially on the facts and circumstances of each individual civil proceeding, any limit on the availability of such information would have the potential to prejudice the legitimate rights and interests of claimants or respondents in such proceedings".

So what is the issue?

One principle of judge-developed human rights law is the delightfully named ‘equality of arms’, which is that each party to legal proceedings must have a reasonable opportunity of presenting their case under conditions that do not disadvantage that party as against other parties to the same proceedings. This principle underlies requirements for discovery and inspection of documents, rights to issue subpoenas and other evidentiary rules designed to enable each party to prepare their case and review relevant material that other parties to that litigation may propose to tender. Prohibiting litigants from accessing telecommunications data as an evidentiary source in civil proceedings potentially reduces the ability of litigants to access a probative source of information relevant (either for or against) their claim or response.

This concern led Patrick Fair of Baker & Mackenzie to write an opinion piece, published in the Australian Financial Review of 23 July 2015, that was highly critical of the section 280(1B) prohibition. Patrick asserted:

"Parties to litigation in a civil court are usually able to access evidence that could prove the truth or falsity of facts contested in proceedings. The law requires litigants to make full disclosure of relevant documents. The courts have extensive powers that require litigants and relevant third parties to deliver up evidence. The power exists to help the judge get to the truth. The availability of relevant evidence is critical to the proper administration of justice, being likely to clarify issues in dispute, and may cause a party to settle rather than taking up public resources when the facts are against them. It is not at all clear why it should be assumed that matters being investigated by the police and national security are more important or consequential than every matter that comes before a civil court."

Patrick puts his side of the case well. Litigation lawyers like evidence (and lots of it) and they are rightly suspicious of any artificial restriction upon availability of evidence.

Another viewpoint

But there is another side to this coin and we should rightly pause before arming up the litigators. Subpoenas are issued over the counter by administrative staff in court registries without judicial consideration of their merits. Fishing expeditions by overly broad
subpoena are common. Judicial control is exercised at the ‘back end’, through consideration of whether to allow into evidence material as subpoenaed, and through an ‘implied undertaking’ that restricts use of material subpoenaed other than for probative use in the particular litigation. Rights to object to production in response to subpoena often are not exercised. The relevant evidence may be produced because the person subpoenaed (i.e. a communications service provider) may have no interest in taking active steps to restrict access, or because the person to whom the communications data relates (and who considers that data sensitive) may or may not be a party to the litigation and aware of the issue of the subpoena.

In short, there are not effectively reliable safeguards as to potentially privacy invasive use of subpoena. And let us remember that we are looking forward, not back: this is not ‘just’ an issue of evidence about who was communicating with whom, when.

The ‘digital exhaust’ of our daily lives as recorded through the devices that surround us in the Internet of Things (IoT) maps a rich picture of movements and activities within the home and other private places, as well as everywhere else. As well as the smart phone and personal health devices enabling 24x7x365 identification and tracking of each individual’s movement, exertion level and activity, many other devices are arriving to fill out the picture of that individual’s life. According to Telsyte’s recent Australian IoT @ Home Market Study, by 2019, the average household will have 24 internet-connected devices, up from nine in 2015. As well as the myriad benefits the IoT will bring, the combination of ubiquitous IoT devices, mandatory communications data retention and potentially uncontrolled access by civil litigants is a potent cocktail whose effect we should consider before we consume.

And so...

Expect many lawyers to seek out the cocktail and to crank up their representations to the Attorney General for exceptions to this prohibition before it comes into effect in October 2015. But determining whether they are right or wrong requires careful thought and a privacy aware debate. That debate hasn’t even begun.

Peter Leonard is a Partner, Gilbert + Tobin Lawyers and a Board Director of iappANZ

---

iappANZ’s writing prize 2015: entries open

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

All articles must be submitted by email, preferably in Word, to veronica.scott@minterellison.com, Carolyn.lidgerwood@riotinto.com or emma.heath@iappanz.org by 20 October 2015. We will need the author’s email address and contact number. You can submit as many articles as you like.

The winner will be announced at our Privacy Summit on 18 November 2015 in Melbourne and their name and details will be published on our website. We also hope to profile the winner in our Journal. So alert your network and get writing!

More details about the writing prize if you are interested:

▪ Our Editorial team, Veronica Scott and Carolyn Lidgerwood, plus President Anna Kuperman and Past President Malcolm Crompton, will decide on the winner whose article they judge to be the most interesting, original and relevant to our members.

▪ Some people won’t be eligible for the prize (sorry!). They are: iappANZ board members, contractors and employees and their family members.

▪ After the winner is announced we will notify them and arrange for the prize to be delivered to them if they are unlucky enough not to be at our Summit.

▪ There will (sadly) be one prize only. Its value is AUS$250, so that’s pretty good really.

▪ We may need to verify the winner’s identity so we don’t give the prize to the wrong person.

▪ If the prize is not claimed for any reason (and we hope this won’t happen) the author of the runner-up article as judged by the Editorial team will receive the prize.

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

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

No positions currently advertised.
Increase in iappANZ membership fees

As outlined on page 4, iappANZ has now introduced a membership fee increase and a new tiered fee structure as of 1 August 2015. The membership fees that apply from 1 August 2015 are set out below (note that fees are in Australian dollars):

<table>
<thead>
<tr>
<th>Membership Type</th>
<th>Fee</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard Membership</strong></td>
<td></td>
</tr>
<tr>
<td>Individual</td>
<td>$250 incl. GST</td>
</tr>
<tr>
<td>Corporate</td>
<td>$225 incl. GST per Member</td>
</tr>
<tr>
<td>3-4 Members (10% discount)</td>
<td>$675 incl. GST (3 Members)</td>
</tr>
<tr>
<td></td>
<td>$900 incl. GST (4 Members)</td>
</tr>
<tr>
<td>5+ Members (15% discount)</td>
<td>$212.50 incl. GST per Member</td>
</tr>
<tr>
<td></td>
<td>$1062.50 incl. GST (5 Members)</td>
</tr>
<tr>
<td><strong>Government/Not-for-Profit/Senior (60+) Membership</strong></td>
<td></td>
</tr>
<tr>
<td>Individual</td>
<td>$225 incl. GST</td>
</tr>
<tr>
<td>Corporate</td>
<td>$202.50 incl. GST per Member</td>
</tr>
<tr>
<td>3 - 4 Members (10% discount)</td>
<td>$607.50 incl. GST (3 Members)</td>
</tr>
<tr>
<td></td>
<td>$810 incl. GST (4 Members)</td>
</tr>
<tr>
<td>5+ Members (15% discount)</td>
<td>$191.25 incl. GST per Member</td>
</tr>
<tr>
<td></td>
<td>$956.25 incl. GST (5 Members)</td>
</tr>
<tr>
<td><strong>Student (University Full-time)</strong></td>
<td>First year complimentary</td>
</tr>
<tr>
<td></td>
<td>$25 for second and remaining years if full-time university study</td>
</tr>
</tbody>
</table>
SAVE THE DATE

WEDNESDAY 18 NOVEMBER, 2015, MELBOURNE

2015 iappANZ Annual Privacy Summit: Privacy@work

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

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

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

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

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

**Where:** ZINC, Federation Square Melbourne

**Earlybird:** Until 7 October

**Details:** [www.iappanz.org/events](http://www.iappanz.org/events)

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

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

<table>
<thead>
<tr>
<th>Time, Date &amp; Location</th>
<th>Information</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MELBOURNE</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Tuesday 13 October 2015 to Thursday 15 October 2015 | AISA National Conference  
“Trust in the world of Information Security”  
| Venue: Atlantic Group V, Shed 14, 15 Central Pier 161 Harbour Esplanade Docklands VIC 3008 |                                                                             |                                                                      |
| **SYDNEY**            |                                                                             |                                                                      |
| Friday 4 September    | Legal wise seminars: Central legal issues in advertising and marketing     | Special iappANZ Member discount.                                      |
| Session 1: 9.00 – 1.15pm | Whether you are a legal practitioner or a marketing and advertising professional, this is the conference for you. These experts know the industry inside out, so be guided by the best on the key legal issues, regulatory landscape and do’s and don’ts. This is not your run of the mill legal session; it is designed to be practical and engaging. We have extracted the central legal issues in advertising and marketing and included them with case studies, real life scenarios and tips. Use this opportunity to ask questions and leave with a complete understanding of the relevant guidelines and associated legalities that are relevant to your everyday work.  
**Session 1: Online Legal Issues in Advertising and Marketing**  
Chair: Matthew Lewis, Barrister, Wentworth Chambers  
**Advertising and Marketing and Current IP issues: A Practical Refresher and Update on Recent Cases.** Presented by Alison Jones, Senior Associate, Corrs Chambers Westgarth.  
**The Practical Side of Inbound Marketing: Case Studies and Scenarios.** Presented by Tony Eades, Director of Brand Strategy, The Brand Manager  
**Cautioning Through the Social Media Minefield.** Presented by Dan Brush, Special Counsel, Colin Biggers & Paisley  
**Are You Liable for What Others Leave On Your Website?** Presented by Steven Brown, Chairman, Etienne Lawyers | Session 1 : $360  Session 2: $360  
(Regular price $460 per session)  
Phone registration only - call : 02 9387 8133  
Quote: iappANZ Member to redeem your discount  
*7 CPD units in Substantive Law*  
<table>
<thead>
<tr>
<th>Session</th>
<th>Description</th>
<th>Presenter(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy and SPAM</td>
<td>Presented by Jodie Sangster, CEO, ADMA</td>
<td></td>
</tr>
<tr>
<td>Session 2: Understanding the Regulatory Environment</td>
<td></td>
<td>Peter Leonard, Partner, Gilbert + Tobin</td>
</tr>
<tr>
<td>Key Regulations When Advertising in Different Sectors</td>
<td>Presented by Georgina Hey, Senior Associate, Norton Rose Fulbright</td>
<td></td>
</tr>
<tr>
<td>Developments in Origin Claims and ACCC Investigative and Prosecutorial Powers/Remedies</td>
<td>Presented by Ayman Guirguis, Partner, Corrs Chambers Westgarth</td>
<td></td>
</tr>
<tr>
<td>Regulatory Issues in Online Behavioural Advertising: IAB’s Perspective</td>
<td>Presented by Daad Soufi, Director – Legal and Regulatory Affairs, Interactive Advertising Bureau</td>
<td></td>
</tr>
</tbody>
</table>
iappANZ Member: $687.50 incl. GST
Non-member: $907.50 incl. GST

Contact Emma Heath for further information – emma.heath@iapanz.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.

Our global body, the International Association of Privacy Professionals (iapp) says:

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

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

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

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

What about testing?

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

Our contact details

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