Privacy Unbound iappANZ

March/April 2016

UNLOCKING THE TRUTH ABOUT PRIVACY

ISSUE 69

President's Letter

By Kate Monckton
President
M: 61 409 613 029

Dear Members

Last week I was lucky enough to attend the IAPP Global Privacy Summit in Washington D.C. which was just fantastic. I'm not sure if there's a collective noun for privacy professionals but with over three thousand of us under one roof, there probably needs to be!

While we were in D.C, myself and two of the iappANZ Board Directors, Malcolm Crompton from Australia, and Tom Bowden from New Zealand, had the opportunity to sit down with Trevor Hughes, the President and CEO of IAPP and some of his team to hear about some of the new and exciting initiatives coming members' way, including a new CIPP Asia.

It was also great to see some familiar faces from ANZ over there – check out the photo of myself with iappANZ member Chris Rogers from EY, who was proudly sporting his certification ribbons on his name badge. I have come back to Oz with lots of ideas for our local summit here in Sydney in November and can't wait to get stuck back into working with sub-committee on finalising plans.

Privacy Awareness Week is just around the corner – keep an eye out for more information about some of the events we are planning in Australia and New Zealand. We have a wonderful group of volunteers working very hard on some really interesting workshops so please join us where you can.

As always, we love to get your feedback on any ideas or suggestions you have for ways that iappANZ can help support privacy professionals so please don't hesitate to contact us at admin@iappanz.org at any time.

Kate

Kate Monckton
iappANZ President

Vice-President's Foreword

By Melanie Marks
(Joint) Vice-President
Melanie.Marks@cba.com.au

Dear Members

Welcome to the April edition of *Privacy Unbound*. This will be my last foreword for the year as I hand over the role of Vice President to Anna Kuperman for the duration of this term. Many of you will know Anna as the 2014-2015 President of iappANZ. I wish Anna, the Board and our members a fabulous year ahead.

Without further ado, the wrap up of this edition is as follows:

- We kick off with a review of SAP's recent *Australian Digital Experience Report* by **David Templeton,** iappANZ Secretary and a senior manager in ANZ Bank's Products and Marketing team. The report points to the high adoption of online services by Australian consumers and affirms the significance of privacy in establishing a successful digital offering. If we accept that customer experience and data analytics are cornerstones of effective digital platforms, then we as privacy professionals must be key business enablers in helping our organisations to extract maximum value and success from digital initiatives.

- Across the Tasman**, Katherine Gibson**, Director, Gibsons Law, Auckland reviews the clear guidance recently issued by New Zealand's Privacy Commissioner to those agencies relying on the maintenance of the law exception to disclose personal information. What does this mean in practice for the agency faced with a request?

- Do start-ups have to comply with the Australian *Privacy Act*? Whilst the question may be a simple "no" in law (based on turnover), Australian consumers increasingly expect that the organisations that hold their personal information will uphold their privacy. In this month's Q&A, Australian Privacy Commissioner and Acting Information Commissioner, **Timothy Pilgrim** outlines his advice for start-ups and tells us a bit about his plans for Privacy Awareness Week (15-21 May) as well as the establishment of a new network for privacy professionals in public and private sectors.

- **Katryna Dow,** founder and CEO of Meeco describes her gig as a "world leading data independence start-up in the emerging personal data economy". This is one start-up which places privacy at its core. Katryna writes about how technology is leading to a profound shift in power whereby a failure to engineer for individuals to generate value from their data will enable a new form of feudalism – a digital dark age. Imagine the power of a network built on trust and transparency, permission and consent. Turn to page 12 to find out more.

- This year I will be thinking very carefully about whether I am a Jedi Knight for the purposes of Australia's Census. In this article**, Anna Johnston,** Director, Salinger Privacy exposes a quiet shift in policy which will enable Australia's Bureau of Statistics (ABS) to keep the names and addresses of every person in Australia from the 2016 Census onwards. If you were not aware of this change, I'd encourage you to read up and speak out.

In signing out as Vice President, I also take this opportunity to invite your feedback or ideas on *Privacy Unbound* or any of our member services via our email address: admin@iappanz.org.

Wishing you a happy, healthy and successful year ahead.

Melanie

Editors' note – hold the presses! We've just received Malcolm Crompton's insightful report on the IAPP Global Privacy Summit in Washington DC – and you'll find it on page 15ff. It's an excellent report that will make you feel like you were there …

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 regulators 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.

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

Digital Hicks and Ketchup

by David Templeton

Customer experience and behavioral analytics are mature disciplines among global technology giants and are now being embraced locally. If you work in a business that has customers, and an analytics proposal hasn't landed on your desk already, you can be sure it will soon, especially in Australia as we play catch up with the rest of the world on digital experience.

"Ketchup?" you say? No, catch up, catch up! I say. It's a notorious truth that Australia's knowledge and services economy is ripe for disruption. Big business down under has underinvested in digital sales and service channels. This lack of investment has now been recognized and I can safely say that in some sectors, business is scrambling to upgrade and fend off potential digital usurpers.

Last year SAP published its *Australian Digital Experience Report*. The report is available here. Built from an online brand comparison customer survey of 34 online brands across six sectors, the report revealed that many of our local brands offer a **profoundly diminished digital experience** by comparison to what customers expect (presumably from dealing with global online brands). The big reveal is that Australian companies, particularly incumbents in established markets, are a long way behind expectations with a lot of work to do if they wish to retain customers online. Digital hicks is my interpretation.

For Privacy Professionals, the report offers valuable insights. In particular, the report:

- Confirms the popular wisdom that Australians are enthusiastic adopters of online, particularly mobile. In other words, the opportunity in online in Australia is enormous, and Australian tolerance for new models of interaction is high
- Affirms the old adage that 'good privacy is good business'. In structuring the survey, respondents rated brands across 13 attributes and separately rated the significance of each attribute. **The topic of privacy came in at number 5,** where SAP's survey participants placed the attribute "Relevant offers without infringing privacy" (behind "Cohesive, integrated and simple", "Available anytime on my terms", "Respectful and dedicated to my needs" and "Fits in with my life and effortless").
- Reveals that improving privacy is a key opportunity area. Across 5 of the 6 industries represented, privacy (ie, an online experience that manages to be both relevant to customer needs and privacy friendly) was found to be one of the priority areas for improvement.

While I have no word on whether SAP are considering the same exercise in New Zealand, I can see that Australian business, at least in the financial sector where I live, has listened to SAP (or recognized the problem independently). Everywhere I look I see digital disruption recognized as an existential threat and moves to significantly upgrade and personalize customer experience using data and analytics.

CX is vital to online success and is emerging as a distinct commercial profession

Customer experience (CX, sometimes referred to as UX for 'user experience') refers to your customers' perspective on your sales/service engagement. The phrase is channel agnostic, but it's in digital interaction, where there's noone to paper over the cracks, that has brought the imperative of a well-designed CX into focus.

At its simplest, CX is about whether your customers liked dealing with you, whether they would come back again and say nice things about you, or whether your online offering was just annoying, perhaps taking too long, demanding too much personal information, or steering them into a one way labyrinth of screens from which browser closure and restart was the only return? Looked at more closely though, designing good CX is not just about addressing a few isolated pain points. As the SAP report reveals, sophisticated online customers require a holistic design that puts the customer first. Customers expect a journey that is at the very least cohesive, simple, accessible, fits in with them, predicts needs and responds relevantly while respecting privacy, is responsive, exciting and engaging... SAP's list goes on, across 13 core attributes that reflect consumer preferences.

Good CX is vital, particularly in markets where similar firms offer similar services at similar price points. In traditional sales and service, the tone of a firm's people defined the customer experience. If it went badly, it went badly in a particular instance. In digital, a site or

app's relative joy and "wow factor" decides who grows share in a contested market. In digital, if it goes badly for one, it will be going badly for many others. For firms looking to digital for future growth, CX design is a key priority.

It's not just business that needs to focus on CX. Public sector agencies with monopoly control on access to essential government services can get away with a more basic CX for a while, but agencies looking to build positive engagement with online stakeholders will need to offer a consistently satisfactory CX in order to do so and eventually, poor CX will tarnish any operator.

Good CX is impossible without good privacy. Disclosures, consents and security/credential management are core elements of online interaction where the CX, ie the convenience, simplicity and ease of these tasks is as vital as it is to any other element of the online interaction. Choices and privacy controls available to the customer must be clear and easy to make or use. Equally, the way a digital service predicts customer needs and preferences, and the manner in which it presents or reflects predictions back to the customer must be respectful of privacy. Good CX remains within the bounds of a permitted space defined by purpose, context and consent, the core ingredients of APP 6.

Analytics – determining the next best action

Alongside the CX team, developing a compelling and sales effective digital experience will involve the analytics folk and the marketers. Their focus will be designing and implementing an insight led next best action program to ensure that customers are engaged across all channels, including online, with suggestions and offers that are truly relevant, well timed and deftly positioned.

Next best actions are the optimal next step to take with a particular customer, identified by taking account of what you can fathom about that customer's likely needs and preferences from their past behavior. A next best action could be as overt as proposing a particular product at a particular price, as simple as leaving the customer alone, or anything in between. Next best action, customer centric marketing is emerging as the new dominant paradigm for direct marketing.

Like CX, the next best action program won't be effective without good privacy. The data that an organisation chooses to analyse, how it chooses to interpret that data and what suggestions it makes on the basis of those interpretations are all direct outputs of personal information, collected both directly and indirectly from customers (and subject to the privacy obligations). It will be very difficult to position a 'next best action' proposal deftly or relevantly if the proposal sits at odds with the customer's expectations.

Done well, analytics enables needs and propensities to be identified with sufficient accuracy to present a considered and appropriate cross sell. Done poorly, insight led offers can be deeply embarrassing and privacy invasive.

How this affects you - analytics, CX and privacy practice

Customer analytics, the prioritization of online as a sales and service channel and the need to optimize customer experience while doing more with data, are rapidly moving fields with a high privacy touch and significant security challenges. The chances are high that your organisation is or will be investing in insight led customer management and improved CX. You, the privacy professional, are a key enabler for this.

It will be vital to understand what's at stake for your business. Organisations can't avoid this challenge. Building simple and engaging online CX and effective analytics and insights are now core business disciplines.

If you are new to this, I encourage you to learn more about CX design. Customer experience is emerging as a distinct commercial discipline, using a well-developed range of techniques and recognized design principles to optimize online interaction. Courses and qualifications are now available.

There's a lot on the web about this, one quite deep and no-cost site is https://hackdesign.org/ . The better your understanding of the business and its environment, the more effective you will be as an enabler to, or even better, as a member of the development team.

Digital redesign brings both challenge and opportunity. You can expect to be confronted by novel business needs. CX design aims to meet people where possible on their own terms, and to meet real needs. You'll be thinking about managing identity and keeping information safe while people interact online at home, work or in between. Your organization may need to deal online safely with families and groups, recognizing that some services are purchased at a household level and any member of the household might need

to deal with you, across a range of age groups. As the online experience becomes deeper and the optionality extends, new paradigms for information collection, management and use will evolve and you will have the joy of dealing with this.

You'll need clear, simple and empowering privacy policies and tools. You will need to find a potentially narrow sweet spot between simplicity, specificity and sufficiency to support your analytics and marketing programs. Sometimes you'll need to force a judgment call, perhaps about not making a particular type of offer or using a particular field in the analytic, or perhaps to obtain a specific consent rather than rely on context and inference to support a particular use of data. You might have to vintage data according to the consents and context that applied at collection. When you do make a judgment call, you'll need clear, articulate thinking to shift business imperatives and the trust of your organization's development team.

If you are close enough to the development team, you can take advantage of the opportunity to poll real customer reactions to your privacy solutions.

All in all, whether you are with a disruptor, helping an incumbent to play catch up or dealing with the challenges of effective public service delivery, an economy in transition promises a world of opportunity to the privacy professional. **Good privacy people are key enablers to digital success.**

David Templeton is the Secretary of iappANZ and joint editor of Privacy Unbound. David is also a Senior Manager in ANZ Bank's Products and Marketing team.

Please provide me with your customer details – we need these to maintain the law

by Katherine Gibson

New Zealand's Privacy Commissioner recently gave clear guidance to those agencies relying on the maintenance of the law exception to disclose personal information – be prepared to defend your decision, and if a complaint is made, you must prove you were justified in your belief that the disclosure was necessary.[1] *But what does this mean in practice for the agency faced with a request?*

This does not necessarily signal a change in the application of IPP11(e)(i),[2] but it is a sharp reminder to those agencies that they simply cannot assume the Government agency has got it right (that the exception allows disclosure), or (where it is implied in the request) that the Government agency has the right to the information under the Privacy Act. For those agencies who do not have the luxury of a well-resourced legal or privacy team, this places a very real burden and additional cost on the agency to get it right. A responsibility that comes with using personal information in order to do your business.

OPC Transparency Report

In last month's Privacy Unbound, Privacy Commissioner John Edwards told us one of his focuses for 2016 is to encourage private sector agencies to publicly report the number of personal information requests they have received from government agencies, and how many of those requests they complied with. This followed the Commissioner's report on the trial undertaken by the Commissioner's Office where 10 companies provided information on the number of types of personal information requests they received over a three month period.[3] Most of these requests were made under a statutory power,[4] but according to the report around 18%[5] of the requests were made without any such power, and the disclosure was made relying on exceptions in Principle 11(e) and Principle 11(f).

One of the exceptions is for law enforcement purposes. The Act requires the agency to believe, on reasonable grounds that non-compliance (with the principle that personal information should not be disclosed) is *"necessary…. to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution and punishment of offences"*.[6]

The Commissioner has said that his Office will publish guidance on the Privacy Act disclosure exceptions to assist both the Government agencies requesting the information and those agencies receiving the requests. This will no doubt be welcomed.

A useful checklist for agencies

Pending release of the guidelines, a useful checklist may include:

1. It is the agency receiving the request who has the responsibility to make the decision on whether the exception applies. The requestor does not make the decision.

2. The agency should ensure it has enough information to make the decision. That should include information about why the requested disclosure is necessary to avoid prejudice to the maintenance of the law – this will be information that will probably need to be obtained from the requesting Government agency.

3. At the date of the disclosure, the agency must believe that the disclosure is necessary with reference to the particular IPP11 exception being relied upon. The information must be inspected and assessed on this basis before it is disclosed.[7]

---

[1] Privacy Commissioner "Transparency Reporting Trial Aug-Oct 2015 Full Report", at para 40.
[2] The "maintenance of the law" exception to the disclosure principle.
[3] "Transparency Reporting Trial Aug-Oct 2015", Ibid 1.
[4] Such as s17 Tax Administration Act 1994, s11 Social Security Act 1964 and s71 Search and Surveillance Act 2012.
[5] 2,073 requests – see page 14 of Report.
[6] IPP 11e(i).
[7] Geary v Accident Compensation Corporation [2013] NZHRRT 34 at paras 201 to 203.

4. Reliance on the exception by the agency cannot be an explanation *devised in hindsight".*[8]

5. The disclosure of the particular information must be necessary to avoid a particular prejudice to the maintenance of the law. A general assumption by the agency that the disclosure will result in a possible consequence is not enough.[9]

6. The agency should keep a record of the process it undertook to make the decision and the reasons relied on for disclosure.

7. If a decision is made that an exception applies, the agency should consider whether it should exercise its discretion to provide the information – the exception *permits* disclosure, it does not *require* it.

How has the exception been applied?

Many of the reported cases regarding the maintenance of the law exception involve disclosure by a Government agency and are fact specific. Care needs to be taken when applying them to different facts.

Circumstances that have fallen within the exception include:

1. The complainant was on a student permit (which can be revoked if a permit holder has been convicted of criminal offending). The Department of Corrections disclosed the complainant's criminal convictions to Immigration New Zealand ("INZ") as part of preparing a pre-sentence report regarding the complainant. The Commissioner held INZ has a maintenance of the law role and the disclosure was necessary for the maintenance of the law as INZ needed to confirm that the man was still eligible to hold a student permit.[10]

2. An investigator at the Ministry of Social Development ("MSD") disclosed to a journalist that the complainant was under investigation for benefit fraud. The journalist had previously written news reports that indicated the complainant was involved in benefit fraud. The Commissioner was satisfied that the investigator had approached the journalist to obtain information about possible offences and this was part of the MSD's statutory function to investigate potential offences involving public funds.[11]

3. The Police contacted a university to find out where a student was. The Police informed the university that they had serious concerns the student's mental health and needed to know where he was. The University revealed where and when the student would be sitting his exams (after the Police failed to find him at his home address).[12]

4. The complainant had been admitted to the No Asset Procedure ("NAP") by the Official Assignee ("OA"). The MSD was one of the man's creditors and provided personal information to the OA objecting to the entry into the NAP (there are certain circumstances under the Insolvency Act in which a person should not be admitted to the NAP). The Commissioner was satisfied that the MSD had provided the information to help the OA to establish whether the complainant should have been admitted to the NAP.[13]

Here are some of the circumstances that have fallen outside of the exception:

1. The complainant was a client of the ACC. The complainant had provided a reporter with information about her case claiming that the ACC had mishandled it. The ACC responded to questions by the reporter and also provided comments on the allegations. The ACC claimed that the exception applied as non-compliance was necessary due to the need to counter incorrect information and without doing so the ACC's ability to maintain the law (under the relevant statute) could be

[8] Geary v ACC, Ibid above; Director of Human Rights Proceedings v David James Crampton [2015] NZHRRT 35 at para 84.
[9] K v Police Commissioner, Unreported, Complaints Review Tribunal, Decision No 33/99, CRT 17/99, 26 November 1999 at page 6.
[10] Case Note 94081 [2007] NZ PrivCmr 8.
[11] Case Note 93362 [2007] NZ PrivCmr 19.
[12] Case Note 97705 [2008] NZ PrivCmr 3.
[13] Case Note 211183 [2010] NZ PrivCmr 10.

prejudiced. The Commissioner held that the maintenance of the law exception did not extend to upholding the standing or credibility of a particular enactment or statutory body.[14]

2. A Police officer was seeking to find the complainant to serve a notice of disqualification of driving (following a conviction of driving while intoxicated). The complainant's mother asked why he was looking for her and the Police officer told her of the offence and the need to serve a notice of disqualification. The Police stated the disclosure was necessary as they rely on the assistance from the public to locate people and officers are more likely to receive assistance if they are able to answer such questions. The Tribunal did not accept this view (the opposite could be the case as the mother may well have assisted her daughter to evade service).[15]

3. A Police officer delivered a court summons for the complainant (charge of careless use of a motor vehicle after a car accident) to the complainant's mother's address. The complainant did not live there and therefore service at this address was not in accordance with the relevant statutory provision. The police and the mother discussed the complainant's involvement in the accident which was overhead by 2 children who were relatives of the complainant. The Commissioner noted that a summons could fit within the exception, but held that the non-compliance was not necessary as there was a prescribed statutory procedure in place regulating how the summons should be served.[16]

4. The complainant received a letter with "Community Probation Service, Department of Corrections" on the back. The Commissioner rejected the submission of the Department of Corrections that as this would encourage the mail not to be overlooked it was necessary to print those words to avoid prejudice to the maintenance of the law.[17]

Does the agency just say no?

When a request is made the easiest way to ensure compliance with the disclosure principle is to simply say no.[18] This strategy could also be a powerful message to consumers - "*Do business with us as we will not provide your information unless we have to by law.*"[19] But is this the outcome society wants – privacy trumping law enforcement? Should we expect businesses to assist Government agencies with maintaining the law? Yes we should and like many privacy issues, it's all about getting the balance right.

Katherine Gibson is Director, Gibsons Law Limited in Auckland (http://www.gibsonslaw.co.nz)

[14] Case Note 8649 [1997] NZ PrivCmr 3. Note this case was considering Rule 11(2)(i) Health Information Privacy Code.
[15] K v Police Commissioner, Ibid 9.
[16] Case Note 51765 [2003] NZ PrivCmr 13.
[17] Case Note 35455 [2003] NZPrivCmr 17.
[18] This of course does not apply where the request is pursuant to a statutory power, a search warrant or a Court order.
[19] A recent example where release of personal information by a bank to the Police has led to significant media coverage is the release by Westpac Bank of Nicky Hager's personal information. It has also been reported that other banks did not provide information to the Police.

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

with Melanie Marks

1. Does the OAIC have any advice for start-ups, who may not be governed by the Privacy Act, but whose business models rely heavily on customers trusting them with their personal information?

Start-ups are a challenge in Australian privacy regulation as they generally aren't covered by the Privacy Act by virtue of being small businesses. Yet many rely on personal information for their business models, and all of them intend to grow into larger businesses.

The OAIC has developed a short resource for start-ups to help them understand the importance and value of integrating privacy into their business from the outset, rather than trying to play catch-up when they suddenly find themselves having to comply with regulation.

Our technology policy team, led by Este Darin Cooper, is working closely with fellow regulators and with the start-up community to impress the benefits of 'privacy by design' to businesses using financial or other personal information to innovate for the future

.

2. We've heard that the OAIC has launched a new network for privacy professionals. Where can our members find out more?

The new Privacy Professionals Network (PPN) is an update to our previous Information Contact Officers and Privacy Connections networks, bringing together, for the first time, the public and private sector privacy professionals.

We think that this combined network — mirroring the unified nature of the APPs — will provide a valuable opportunity for privacy professionals across all sectors to compare and learn from experiences.

We will also be holding regular PPN meetings and seminars, where members will have an opportunity to hear from experts, listen to case studies, and network with other members. We're keen to ensure that meetings will take place in locations right around Australia, and so I'm pleased to say that the first PPN meeting being held in Perth in June.

We will be contacting the existing members of our ICON mailing list to let them know about this opportunity, but if you'd like to sign up you can contact ppn@oaic.gov.au or see further information at https://www.oaic.gov.au/engage-with-us/networks#ppn

3. Can you tell us what's planned for Privacy Awareness Week this year and about this year's theme "*Privacy in your hands*"?

This year the Office of the Australian Information Commissioner (OAIC) will be celebrating Privacy Awareness Week (PAW) from the 15–21 May.

A robust regulatory framework for privacy is now well established in Australia, as is a broad understanding of our privacy rights and responsibilities. This year's PAW theme, *Privacy in your hands*, reflects how this framework empowers individuals, organisations and businesses to make informed choices and maintain smart privacy practices.

This year's PAW will also take on an international perspective, with the first visit to Australia by the United Nations Special Rapporteur for Privacy, Professor Joe Cannataci. Professor Cannataci will be the key speaker at our annual Business Breakfast, which will be held on Monday 16 May in Sydney.

I'm also excited to announce that, for the first time, our PAW campaign will have a dedicated campaign site. This site will hold all the dates, information and resources you need for the week, including training resources, videos, and partner logos.

Keep your eye on www.oaic.gov.au/paw for all the news, updates and ticket information.

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

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

It's Not About Privacy – It's About Power

by Katryna Dow

The privacy debate is the shadow cast over the start to our 21st Century. We are surrounded by extreme views. Privacy is political; just ask Snowden. Privacy is over, declares Mark Zuckerberg. Privacy is joy, says the couple reunited.

.

Amidst these differing views it's evident is that the privacy norms of the past are fast eroding in the digital, Wi-Fi enabled, security camera tracked world we inhabit. I am not sure it is going to get better in the short term; in fact I think it is going to get a lot worse. In part, because we focussed on debating privacy, when the real issue is power.

Power is a difficult conversation to have. It implies opposition and the absence of parity. It's not polite, so it's the conversation we avoid. And yet, as our lives become increasingly digital, we are faced with the harsh reality of how our current economic models work. They are driven by data … data is information, and information is power.

Back in 2012, the first thing I did when founding Meeco was write our Manifesto. I wanted something I could hold myself to account to. I wanted a beacon for those days when decisions are hard to make. But most of all, I wanted to capture the essence of what I believe will be the challenge of this century.

"Up until now the power to capture, analyse and profit from personal data has resided with business, government and social networks. What if you and I had the same power?"- Meeco Manifesto

What would a world look like that empowered a child through holding their personal information in trust, as an asset for their future? Key data like their medical, educational and financial records. Imagine if they grew up in a world where they could decide who has access, for how long and for what purpose. How might that shift the balance of power in their favour?

This is the century of the digital native. Their entire lives will be captured in some digital form. They will learn through doing in a virtual reality world. They will have multiple careers relying on reputation and networks to enable their next gig. They will rely on mirco transactions to ensure and insure their experiences and outcomes.

They won't own things in the way we do now. Their fridge will order its own contents; their home thermostat will adjust based on the body it recognises. They will 3D print things in a day that used to take months to build. All the while data, habits, movements, sensors, feedback and decision enablement will pervade their lives.

Power is shifting around us, through the things we use to the networks we join. Just as the power of computing has moved from mainframes to wrist devices, so will the flow of information move from the enterprise to the individual. However, if we don't engineer the means for individuals to generate value through these activities then we are essentially enabling a new form of feudalism – a digital dark age. To counter this, trust must be established. The shift from products and services to experiences and outcomes will require participation for customisation, opt-in and acceptance. Therefore we must provide the means for inclusion and reward for the generation that will herald this change.

If indeed the information they provide, together with context and intent, removes friction, enables the flow of information, limits risk and helps reduce cost, then they must receive value in return for the value they shape. This positive upside could be a network effect enabled by the flow of information; a network built on trust and transparency, permission and consent.

Imagine if privacy wasn't a debate for this generation, but instead it became a design feature and differentiator. Imagine the power in that.

Katryna Dow is the founder and CEO of Meeco, a world leading data independence start-up in the emerging personal data economy. See more at Meeco https://meeco.me/ The Meeco **Manifesto is at: https://meeco.me/manifesto.html**

Why you might want to become a Jedi Knight for this year's Census

by Anna Johnston

In the week before Christmas last year, the Australian Bureau of Statistics quietly trashed your privacy. We have only a few months to claim it back.

In December 2015, the ABS announced its plans to collect and keep the name and address of every person in Australia, starting with the August 2016 census. And to then use your name and address, to link your census answers to other sets of data, like health and educational records, so that the ABS can develop "a richer and dynamic statistical picture of Australia through the combination of Census data with other survey and administrative data".

That's right – census data could be linked to health records too. So that the ABS can do things like "(understand) and support … people who require mental health services".

This proposal represents the most significant and intrusive collection of identifiable data about you, me, and every other Australian, that has ever been attempted. It will allow the ABS to build up, over time, a rich and deep picture of every Australian's life, in an identifiable form.

Up until now, the name and address portion of census forms was not retained by the ABS; just as soon as the rest of your census answers were transcribed, the paper forms were destroyed. But the new proposal is to keep name and address, as well as your answers to all the Census questions included this year, such as sex, age, marital status, indigenous status, religious affiliation, income, education level, ancestry, language spoken at home, occupation, work address, previous home address, vehicles garaged at your address, and the relationships between people living in the same home.

Statements from the ABS which trivialise the risks posed by stripping away census anonymity have missed the point. Seeking to justify the proposal by saying that the ABS will never release identifiable information ignores the point that they shouldn't have it in the first place. And, as my mother taught me – you shouldn't make promises you cannot keep.

The risks include leaks from corrupted ABS staff, or organised criminals who wish to perpetrate identity theft and fraud by hacking into the database. The ABS is not magically immune to the risk of data breaches. It was only last year that one of their staff was convicted of leaking data to a friend at the NAB as part of a multi-million dollar insider trading scam.

Blithe reassurances about the security of census information ring hollow as we have seen the slow but steady fallout from so many recent data security breaches, from the Ashley Maddison hack to the Department of Immigration's bungle which saw 9,250 asylum seekers' details published online. Whether from external hackers, deliberate misuse by ABS staff or negligent losses of data, the *only* way to prevent data breaches from occurring is to not hold the information in the first place.

Of even more concern is the temptation posed for the Government of a centralised population dataset, just within its reach. How simple it would be for the federal police or ASIO to require the ABS to hand over details of all Muslim men. Or for Centrelink to demand to know just who is living with whom on what income, while claiming welfare benefits. This is the greatest potential impact of the proposal – that the ABS becomes the unwitting tool of a Government intent on mass population surveillance.

The ABS's own privacy review noted that it faces the risk of what's known as function creep: that in the future, "name and address information from responses to the 2016 Census may be used for purposes beyond what is currently contemplated by the ABS". In what seems a fairly breath-taking degree of naivety, the ABS decided that the risk of this happening is "very low", but that if it did, its response would be to review internal protocols and "consult affected stakeholders".

The statisticians must be living in fantasy land if they think that once they hold identifiable data on all 24 million people in Australia, that not a single government department, Minister or police force will be interested in tapping into that data for their own, non-

research purposes. Just look at the agencies queueing up to get their hands on the metadata that telecommunications companies must now keep by law.

And in the event that a Trump-esque leader demands that the ABS hand over the names and addresses of all Muslims living in Australia (as US census data was used to round up and imprison Japanese-Americans in World War II), how is a review of internal protocols, or consultation with stakeholders, going to fix things?

The *only* way to prevent function creep is to not hold the information in the first place.

A further privacy risk is re-identification from joined-up data. Even if names and addresses are used only for linking purposes – that is, to link your census answers with information about you from another dataset (such as health or education records), and then stripped out again – the added richness of combined datasets makes it easier to re-identify individuals. Disturbingly, the ABS's privacy review did not even consider this risk of re-identification, also known as "statistical disclosure risk". Nor did the concept of Big Data even rate a mention. If our chief statisticians are not calculating the statistical disclosure risk of their own proposal, we are all in trouble.

The only way to prevent re-identification from joined-up datasets is to not link them in the first place.

This proposal represents a massive breach of public trust, and shifts all of the privacy risks onto us, the people of Australia.

But it also carries enormous operational risks for governments, businesses, non-profits and community groups, which each rely on census data for evidence-based decision-making. Research tells us that when people do not trust a data collection, significant numbers of people will simply provide misinformation. Surveys conducted periodically by the Office of the Australian Privacy Commissioner found that around three in ten people stated that they had falsified their name or other details in order to protect their privacy when using websites in 2013; this figure was a jump from 25% in 2007.

In 2001, the ABS were worried enough about the impact on the integrity of census data to try and avoid a joke doing the rounds that people should list their religion on the census form as 'Jedi knight'. Their response was eminently sensible, pointing out that the accuracy of census data is important for all Australians, as it impacts on decision-making across all aspects of our lives: from where to draw electoral boundaries, to the building of schools and hospitals, and the routing of local buses. Further, the question about religion is the only optional question on the census; so if you object to being asked about religion, you can simply not answer it, without risking criminal penalties.

Nonetheless, in the 2001 census results, just over 73,000 people described themselves as Jedi, which is more people than identified as Salvation Army or Seventh Day Adventists, and only slightly fewer than those who listed their religion as Judaism.

If census data can be so easily skewed by a bunch of Star Wars fans, the potential impact of enough people being sufficiently concerned about safeguarding their privacy to contemplate providing inaccurate responses, or not responding at all, should surely make the ABS think twice about this proposal.

And what happens to other nationally-important data collections that don't have the force of law behind them? The ABS's review did not consider how a loss of public trust in the census might impact on some people's willingness to accept or embrace *other* government projects, such as the new My Health Record, if they fear the linking of that data with their census records.

I am surprised that the many stakeholders who seek to use census data, or indeed the agencies which run any other major government programs, are apparently willing to risk the integrity of the data on which they rely. Or perhaps, like the rest of us, they were too busy in the week before Christmas to notice that our privacy protections were being wrenched away.

The ABS's privacy review noted that it faces the risk that this proposal "may cause public concern which results in a reduction of participation levels in ABS collections, and/or a public backlash". Its suggestions for mitigating that risk are mostly focused on PR efforts to calm us all down, but it also says that the ABS will "reconsider the privacy design for the proposal, if required".

Which means that there is still hope, that with enough public pressure, the ABS itself – or at least the governments, businesses and charities which care about the reliability of census data – will see this proposal for the folly it is, and return to a census format designed to ensure both the integrity of our data, and the protection of our privacy.

Anna Johnston is Director, Salinger Privacy. *Find Salinger Privacy at www.salingerprivacy.com.au*

The Hottest Issues at the IAPP Global Privacy Summit Washington DC, April 2016

by Malcolm Crompton

I have been attending the IAPP Global Privacy Summit nearly every year since I first attended in 2003. Yet again, it was the biggest privacy conference ever held in history. The range of topics and parallel sessions was unparalleled: just look at https://iapp.org/conference/global-privacy-summit-2016/sessions-s16 to see for yourself. It's not physically possible to attend all sessions, but here are some of the most important themes that came through.

Privacy is becoming a top line issue in the US (even if how they treat privacy is different…)

A uniform theme at the Summit was the extent to which dealing with personal information in an appropriate way is now a top line issue at the board level. The handling of personal information is no longer seen as 'just a compliance issue'. Customer expectations of privacy often go well beyond the law and failure to meet those expectations will damage the business. The regulators (the Federal Trade Commission and State Attorneys-General as well as the 'new kid on the block' in privacy regulation, the Federal Communications Commission), are also all having increased impact.

This is also obvious by a number of measures:

The actual membership of IAPP is now 25,000; it passed 10,000 only a couple of years ago.

- Over 3,500 attended the Summit this year. The first I attended in 2003 only had about 300 in the room.
- IAPP now targets 'privacy for professionals', a wider reach than 'privacy professionals', so they are reaching out and understanding that most people need to know a bit about privacy but are not privacy professionals per se.
- On the other hand, of course, the Americans are always much more adventurous in their use of personal information, in the first place. So what is seen as appropriate privacy in the US may not match expectations in Australia.

Certification – more variants of the CIPP!

IAPP is responding to this increased focus on privacy in a number of ways. Of most interest to members of iappANZ and in our region is the announcement at the Summit that IAPP is now developing a CIPP credential (Certified Information Privacy Professional) for Asia for release later this year and a CIPP ANZ is anticipated for next year.

Watch this space!

Which leads me to a cheap advertisement, if you join iappANZ you are also automatically a member of IAPP and the rate for joining iappANZ is cheaper than joining IAPP direct. So you get two memberships and you get it cheaper. And there are various corporate memberships available for iappANZ as well.

Global developments

Unsurprisingly, trans-border data flows were a major focus. The cloud and the way individuals can interact internationally with friends and business all accelerate this trend.

Trans-Atlantic focus

However, there was an almost paranoid focus on the movement of personal information between Europe and the USA. Some of that has to do with volume: the huge interchange of personal information across the Atlantic. For a lot of the biggest growing businesses in the USA, Europe is their second big market area, for example the social networks such as Facebook and Twitter.

The particular focus was twofold:

- First, the new European General Data Protection Regulation (GDPR) that was not yet law at the time of the Summit; and.
- Second, the so-called Privacy Shield that is intended to provide for the safe transfer of data out of Europe into the USA in a way that's considered legal in EU law in light of the Schrems decision by the Court of Justice of the European Union.

Seen from some distance away from the North Atlantic, the single-mindedness of this focus was just a bit myopic. That said, a few companies in the USA were realizing that probably their next big growth delta is now Asia.

China – tempting but challenging

In any discussion (such as there was) that took account of the world beyond the North Atlantic, China was seen by the speakers as tempting but challenging. In a lot of ways, China is marked out as not available for Western digital business because China continues to develop its own digital equivalents, whether it is WeChat or any of the others. This protectionism is part of but goes beyond 'The great firewall of China' that seeks to ensure sure that Chinese people are not able to be in open and unconstrained political conversation with outsiders or even with themselves. It is also about building Chinese businesses for China and its market base of over a billion people. So some of the biggest companies in the world are actually digital companies in China: we just don't know about them.

CBPRs – a step towards a global solution?

While there was a lot in regard to cross border movement of personal information that the Summit didn't cover in much depth, there was some discussion of more relevance to our region.

APEC and its Cross Border Privacy Rules (CBPR) system was part of the conversation, especially as it compares with the EU's own but more limited Binding Corporate Rules (BCR) System, a topic on which IIS has written a few papers that are online at www.iispartners.com/Publications/index.html#data and www.iispartners.com/Publications/index.html#apec.

Very slowly, the EU and APEC are exploring the extent to which these two systems ask the same questions and solve the same problem and hence might be the beginnings of a global interoperability.

There was a very interesting session on the Trans-Pacific Partnership and how privacy is going to be dealt with in terms of the free flow of personal information. The US Department of Commerce has a very clear view that the APEC CBPR System is the solution to the issues being raised by the TPP.

Big Data

Big Data has become another of the 'bandwagon issues' but I did not hear much at the Summit that was new.

The exception was the pre-conference workshop run by Marty Abrahams who heads the Information Accountability Foundation. His thinking is always a few years ahead of everybody else's.

This was the way he described Big Data, for the purposes of getting people to see it through a new lens: *'Big Data is the use of personal information in ways not expected by individuals*'.

Think about it!

Tapping the social stream

There was another session that considered the limits to tapping into social media data stream flows, for example tapping into the twitter-sphere to follow trending concepts such as the performance of a particular brand or product. Most people would probably agree that participants in social media such as Twitter have willingly chosen to make a public statement unless they have limitations on their commentary. However, at what stage can a company reach out directly with a personal response? That is a live issue which I think is soluble but we are not there yet.

The ethical overlay

Another concept that is rapidly gaining currency in Big Data discussions is the idea of laying an ethical framework over any legal framework when deciding what data the organisation should collect, how it will analyse it and use it. The word 'ethics' was not on the agenda for this conference tenfold more than it would have been two or three years ago. And I think quite usefully.

Very importantly, this discussion goes beyond nailing an ethical framework up on the wall to looking at what mechanism the organisation will use to apply it and demonstrate this to the outside world. Companies are beginning to draw upon the example that has been around in the use of health information in health research for some time: of an ethics board of some sort. In Australia these are call Health Research Ethics Committees; in the USA they are called IRBs – Institutional Review Boards. Depending on the kind of information that the company is collecting and using, going to the full HREC model may be excessive but there are insights in the model that were discussed that quite explicitly at the Summit. IIS has been advising along these lines to some global companies for some time.

Privacy Programs continue to mature

Only four or five years ago did any sort of structured discussion about a concept called the privacy program commence.

For many years, a company might have had a privacy officer or might have had its compliance people including privacy in its remit.

In more recent times, a well-structured privacy program will have an intelligent area in the entity that thinks about privacy, possibly led by a chief privacy officer, some instructions or rules or framework that it requires the wider business to follow and some supporting training and mechanism for picking up the pieces where things do not quite go right. Better practice also takes account of the company's IT development, building in privacy by design, and privacy impact assessment.

Tips from the best in the business

Now we are seeing developments in best practice go beyond that again and this year's IAPP Vanguard Award recognised a leader in the privacy profession who had pioneered it. The IAPP has two coveted leadership awards that it hands out annually: the Privacy Leadership Award and the Vanguard award.

This year the Vanguard Award went to Scott Taylor who until very recently was the privacy officer at HP. He was appointed HP's privacy officer two weeks before the highly controversial board leaks at HP board when essentially board members were having all of their voice and data streams monitored without their knowledge. It blew up hugely on HP. It caused board resignations and CEOs to change and much more. The way Scott used the situation to advantage to build out one of the best privacy programmes going is really quite a remarkable story.

Most importantly, he was able to obtain and exploit the support of the top leadership. He was able to be in the CEO's office and have conversations that went beyond the kind of discussion many privacy professional have experienced: *'thanks very much, I've given you an hour of my time now just go out and solve it*'. Instead he was given a much more thorough endorsement so that he could engage every part of HP with authority. I'm now seeing it again in other companies but it's again an illustration of the maturing of the privacy programme.

Scott's message loud and clear is to engage the company's leadership and be strategic with the endorsement it gives.

And a must-read!

Also contributing to the Summit discussion of maturing Privacy Programs was a book written by Deirdre Mulligan and Kenneth Bamberger called *Privacy on the Ground*. Privacy on the Ground is based on a huge number of interviews in the USA, Germany and other countries, of actual privacy officers. It distils out of the interviews what people learned and what was effective in running a privacy program.

The book really illustrates how wide the privacy officer has to be in the US and in parts of Europe in terms of what they think about, who they engage, how they make it effective and just how dynamic it is. This is one area where I suspect many companies in Australia and New Zealand have a long way to go. *Privacy on the Ground* is a book worth getting hold of.

Data breach is inevitable, so plan for it!

This is the last theme I want to highlight as coming through in the Summit.

Any company that's now surprised by a data breach and hasn't got a data breach response plan deserves to die. Just as importantly, it would seem that Australia is about to catch up with much of the rest of the world and introduce a data breach notification law (at the third attempt?). New Zealand has the concept on the cards too.

Data breach management includes both having a plan and ensuring it is well practised, just like the fire evacuation drill.

Also, like a number of aspects of good privacy management in a company, data breach management is being handled as part of the company's overall crisis management capability rather than a something special on the side.

Overall …

The IAPP Global Privacy Summit is quite an experience! You must get to it at least once – it is a stimulating complement to the iappANZ Summit by being broader in scope while not always as relevant for those of us in this part of the world.

The Summit yet again suggested to me that in terms of data governance, and personal information in particular, Australia is still many years behind some other countries, with New Zealand somewhat better but still with some way to go. I think we probably already knew that.

We have much to learn from the rest of the world.

CIPP Certification that is relevant to our part of the world is coming. Keep an eye out for it.

In the meantime, a vast resource is available to members of IAPP and you can access it all at best price by being a member of iappANZ.

Malcolm Crompton is Managing Director at Information Integrity Solutions, and is a board member (and founding President) of iappANZ.
Malcolm can be contacted at mcrompton@iispartners.com

Privacy on holidays?

By Carolyn Lidgerwood

A light anecdote to complete this issue of Privacy Unbound. When on holidays recently, I attended a cocktail party at a very nice hotel in Colombo. Just as we were all settling in to listen to the speeches, there was a loud buzzing sound – just like a very large blow fly! A noisy drone proceeded to swoop in and out taking pictures – disruptive, invasive, and a curse for those who hate having their photo taken! I was on holidays … and I think privacy was on holidays too! It has to be seen to be believed … so here are the photos!

Privacy Events

Where and when	Event details	Price
MELBOURNE **Thursday 21 April** **3.30pm for 4.00pm start** **5.30pm finish incl. Q&A and networking until 6.30pm** **Minter Ellison** **Rialto Towers** **525 Collins Street** **Melbourne 3000**	**iappANZ Training Workshop** **MANDATORY DATA BREACH NOTIFICATION** The Australian Government has been consulting on what the proposed Bill to amend the Privacy Act 1988 to introduce mandatory notification reporting for serious data breaches should look like. The Bill would require regulated Commonwealth government agencies and businesses, unless exempted, to notify the national privacy regulator and affected individuals following a serious data breach involving personal information, credit reporting, credit eligibility and tax file numbers. The devil is always in the detail. So, what is currently being proposed? How does it compare to previous Bills and to the current voluntary guide? What are the key challenges? What is a serious data breach? When do you need to notify? These and more questions will be discussed by our panel of specialised professionals along with Q&A from the audience. Panelists: **Eugene Foo**, Deputy General Counsel, Legal Department Latitude Financial Services, **David Watts**, Commissioner for Privacy and Data Protection, Victoria, **Vanessa Swannie,** Chief Privacy Officer and Deputy Chief Risk Officer, Telstra, **Veronica Scott**, Special Counsel, Minter Ellison and iappANZ Board Director and **Mark Gallagher,** Policy Officer, Information Law, Civil Law Unit, Attorney-General's Department.	Free for iappANZ members $99 for non-members Costs deductible from joining fee
BRISBANE **Tuesday 17 May** **12.30 – 2.00pm** Corrs Chambers Westgarth L42, 111 Eagle Street Brisbane 4000	**iappANZ Training Workshop** **PRIVACY AWARENESS WEEK** **DATA SECURITY BEST PRACTICE - THREAT ASSESSMENT, PROTECTION AND RESPONSE** Topics to be addressed will include: • Best practice to protect against and respond to cyber attacks / data breaches • Legal obligations in respect of cyber attacks / data breaches e.g. under APPs, commercial law, directors duties, continuous disclosure, APRA standards and the proposed Mandatory Data Breach Notification legislation.	Free for iappANZ members $99 for non-members Costs deductible from joining fee Register here

	• Cyber Insurance business Panelists: **Helen Clarke,** Partner, Corrs Chambers Westgarth, **Martin Holzworth,** Director, Advisory, Ernst & Young, **Susan Elias,** National Manager FINPRO, Cyber, Marsh, **Van Karas,** Director, Shred-X Document Destruction. Chair - **Emma Hossack,** CEO Extensia and former iappANZ President and current Board Director.	
WELLINGTON and AUCKLAND **Wednesday 11 May,** **8.30am – 12.40pm** **Intercontinental Hotel** **2 Grey Street** **WELLINGTON** **Thursday 12 May** **8.30am – 12.40pm** **Crowne Plaza** **128 Albert Street** **AUCKLAND**	**Privacy Commission – Te Mana Matapono Matatapu** **Privacy Week 2016 (9-14 May)** **"Privacy in your hands"** **UN Special Rapporteur for the Right to Privacy.** **Professor Joseph Cannataci,** will be visiting New Zealand during **Privacy Week** this year and will give keynote presentations at the New Zealand Privacy Commission's Privacy **Forums** in Wellington and Auckland. The Privacy Forums are at the Intercontinental Hotel in Wellington on 11 May and at the Crowne Plaza Hotel in Auckland on 12 May. Our Privacy Forums are always oversubscribed. This year, we have an especially strong line-up of speakers and topics. Book your ticket now to avoid disappointment. Wellington program details Auckland program details	Cost: $150 NZD Earlybird (ends 17 April) $175 NZD Wellington Register Here Auckland register Here

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?

Currently, 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.

It has recently been announced that a new CIPP Asia certification is coming in 2016, and a CIPP ANZ certification is anticipated for next year – watch this space!

What about testing?

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

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

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 current listings

Our contact details

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

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

Veronica Scott (veronica.scott@minterellison.com)
Carolyn Lidgerwood (carolyn.lidgerwood@riotinto.com)
David Templeton (David.Templeton@anz.com)

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