Hi all,

WOW! What a Privacy Awareness Week (and Month) it was this year. It was a great to see so many of you out and about during the week including at the breakfast launch of PAW in Sydney. In this edition of Privacy Unbound, Emma Pond has written a brilliant overview of by UN Special Rapporteur on the Right to Privacy, Professor Joseph Cannataci’s visit to New Zealand as part of PAW. I saw him speak in Sydney and had the pleasure of spending some time with him afterwards and it’s safe to say that the bar has been set for future events.

We also held our inaugural ‘Privacy at the Club’ informal networking event in Sydney a couple of weeks after PAW with the topic of ‘Privacy Awareness Week - How was it for you?’ where two of our Board Directors Olga Ganopolsky and Malcolm Crompton along with Richard O’Neill from the OAIC and Dr Elizabeth Coombs from the IPC shared their insights and thoughts on the week and month. We’ve had great feedback about the content as well as the more informal format and venue, so watch this space for similar events in other areas.

We’ve also been progressing plans for the annual Summit in November (more details are in the Journal) and we are looking at whether a second day consisting of practical workshops would be of interest to our members. Initial feedback suggests overwhelming support for the idea but we would love to hear your thoughts. A short survey will be going out in the next day or so and we would really appreciate your input.

And speaking of Malcolm Crompton, it was with great delight I learned this week that our long time Board Director and all-round great chap is a recipient of a Member in the General Division of the Order Australia for significant service to public administration, particularly to data protection, privacy, and identity management, and to the community in this year’s Queen’s Birthday Honours list. Absolutely brilliant achievement and very well deserved.

As always, if you have any suggestions, comments or ideas for us about ways we can support you in your privacy careers, please feel free to contact me at any time. Kate
Dear Members

We have a splendid privacy smorgasbord of articles in this edition traversing local, regional and international landscapes.

Marta Ganko, Manager of the Privacy Practice at Deloitte Australia presents the findings from Deloitte Australian Privacy Index 2016 with an analysis of consumer brands’ websites and, for the first time, how the data in their mobile applications are being treated. The key themes identified include:

- 94% of consumers believe trust is more important than convenience
- Communicating how information is used and shared builds trust
- Thinking globally and acting globally when responding to regulatory change is increasingly necessary.

Anna Johnston shares her thoughts on de-identification as the cure to the data management compliance conundrum. Can modern day de-identification techniques unlock the promise land of big data analytics without compromising privacy? All this talk of rocket science reminds me of the genius words of Albert Einstein, ‘Everything should be made as simple as possible, but not simpler’. Anna highlights that we need to better understand the language and the techniques involved in de-identification for ourselves, so that we can perform proper risk assessments, and know which privacy controls to apply when. We look forward to your next blog with the crib notes!

Emma Pond, Chair of iappANZ’s New Zealand subcommittee and Legal Counsel (Privacy) Southern Cross Health Society provides a snapshot of Privacy Awareness Week events in Auckland and Wellington with UN Special Rapporteur, Professor Cannataci. Having attended Professor Cannataci’s keynote speech at the OAIC PAW opening event, some home truths echo, namely that Australia and New Zealand each have an important role to play on the international stage to create a society where privacy is properly safeguarded as a fundamental human right. Emma Hossack, iappANZ Board Director reports on the key messages from the OAIC PAW Breakfast, including the focus on de-identification and big data ... this years’ trending words (#watchout).

Fiona Coleman, Principal Adviser and Privacy Officer, Privacy ACC shares how the strategies that the ACC implemented during PAW to raise privacy awareness in a more colourful and fun manner. A great insight into the power of marketing strategies to maximise the focus on compliance as an enabler to achieve positive customer experiences.

Dawn Swan, Privacy Officer at Inland Revenue NZ in Wellington and a member of iappANZ’s New Zealand subcommittee, reflects on a talk presented by Vikram Kumar at a Technology & Privacy Forum in Wellington during New Zealand’s Privacy Week. The so-called supercharging effects of big data seem to be exposing the undercharged privacy protections in new technologies. A case of privacy under-design?

Kyle Lees, an iappANZ member provides an interesting editorial in law reform in the context of protecting a deceased person’s privacy in our digital ecosystem. Should a person’s right to privacy survive death? Is the digital footprint of a deceased person as proprietary and worthy of safeguarding by family members as other assets? In the same week as Brazilian media sent family members of missing Australian backpacker Rye Hunt photos of an unidentified body, it is certainly not an academic issue. Perhaps if we view privacy as a fundamental human right, the underlying concepts of extending tort or contract laws to achieve legal protection become more meaningful.

That’s a half year Privacy Unbound wrap. Happy Reading!

Anna
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&qoback=qdr_1281574752237_1

Follow us on Twitter at: https://twitter.com/iappANZ
Trust without Borders

by Marta Ganko

Any organisation which shares data has become a data broker of some sort.

In Deloitte’s second annual assessment of the privacy practices of more than 100 leading consumer brands operating in the Australian market, a more sophisticated Australian consumer emerges, seeing privacy as a function of both data protection and transparency around how their data is being used.

One of the most telling findings in this year’s survey is that more than 90% of the 1,000 Australian consumers rating the brands value trust over convenience – whether that be using the website or the brand’s mobile app. Surprisingly, this finding is independent of the respondent’s age.

What this means is that organisations have a real opportunity to reposition and proactively build trust with their customers. And there is also the imperative that they safeguard the data that is entrusted to them, no matter who it is delivered to or in which country they reside.

The combination of emerging privacy regulation and the common practice of sharing data highlight new types of borders. National borders are obvious; however in today’s porous world where data is shared across organisations and with subsidiaries and third parties, new borders have emerged.

The Deloitte Australian Privacy Index 2016 analysed the state of privacy of 116 of Australia’s leading consumer brands in 13 sectors – government, banking and finance, insurance, telecommunications, technology, media, retail, health and fitness, travel and transport, social media, energy, and for the first time, real estate and higher education.

The Index comprises a consumer survey of 1,000 Australian consumers, a website analysis, a mobile app analysis, and a confidential organisational survey.

Deloitte Australian Privacy Index 2016 rankings

There are three key areas that indicate good privacy practices, according to consumer expectations as well as Deloitte’s analysis of best practice website and mobile behaviour:

- Using information reliably and respectfully
- Implementing adequate security measures when information is submitted publicly
- Informing consumers how their information would be used.

Which industries performed the best?
Number one in the following list is the most trusted industry with the best perceived governance and the most up-to-date regulatory approach:

1. Banking and finance
2. Government
3. Energy
4. Insurance
5. Telecommunications (mobile/internet/home phone)
6. Higher education
7. Technology
8. Travel and transport (airlines/agencies/hotels/taxi)
9. Health and fitness
10. Retail
11. Social media
12. Media (news/television/radio/entertainment)
13. Real estate

What were the strengths of the organisations that did well?

Organisations that did well offer:

- Mobile apps that advised the user what they did with their collected data
- Security protocols on their website to protect personal information when capturing it
- Safeguards for data, being transparent and actively communicating with the consumer what they did with their data, and why, if and when they took action equals a trusted brand by consumers
- Cookies with a shorter expiry timeframe. The average time across all organisations surveyed was 657 days, the worst were persistent cookies stored for three or more years.

Key Themes

- Trust is more important than convenience for consumers
- Communicating how information is used and shared builds trust
- Think globally and act locally when responding to regulatory change
The top three most trusted industries as identified by consumers were:

- Banking & Finance
- Government
- Higher Education

The three least trusted industries as defined by customers were:

- Social Media
- Media
- Real Estate

Australian consumers are more concerned about sharing the following types of information due to their sensitivity:

- Credit Card Details: 71%
- ID Numbers: 65%
- Medical Records: 34%
- Fingerprint or Facial Image: 34%
- Financial & Credit History: 33%

After experiencing a privacy issue with an organisation:

- 22% of consumers decided to make a complaint
- 19% told their friends and family about it
- 22% stopped using the brand
- 16% stopped using the website
- 8% uninstalled a mobile app
- 7% took no action
- 3% wrote a negative review
- 3% chose ‘other’ as their response
Other key findings

- Australian consumers are most concerned about sharing credit card details (71%), identification numbers (65%) and medical records (34%)
- 18 to 25 year olds are more concerned about sharing mobile numbers or browsing history than medical records; 26-39 year olds are more concerned about sharing their address
- 71% of the 1,000+ consumers surveyed had never had a privacy issue with a brand
- 29% cited 851 privacy issues with organisations included in the survey over the last 18 months
- We complain more about privacy as we get older; more than 38% of 40-64 year olds have made a privacy complaint but less than 8% of 18-25 year olds have.
- 99% of brands implemented layered privacy policies in their apps
- 28% of apps did not have an accessible privacy policy before login. Of these, 45% did not have a privacy policy accessible from Google Play. Yet 96% of all apps assessed transferred user information in or out of the device without logging in
- 52% of brands provided a detailed list of countries to which they disclose privacy data. The banking and finance industry performed best with 76% of app brands tested providing a detailed list. This was closely followed by government and real estate.
- Before even logging into most of the 88 apps accessed, the app was reading information from our device, of which 94% was sent overseas. Depending on the app this data could include your contacts and/or your location however individuals were always informed in such cases.

Trends

- Consumers are becoming more discerning

Consumers are becoming increasingly aware of how organisations are using and handling their personal information, and the risks they face when sharing their personal information.

94% of consumers consider trust more important than ease of use of website, app or device

- Consumers want choice

It is important that organisations pay attention to consumer expectations to ensure they are:
  - Informing consumers exactly how their information will be used
  - Giving consumers the power to decide what they want their information used for

67% of respondents are concerned if their personal information is sent outside Australia
>21% want to be informed if organisations send information to third parties

- **Increased and active management of third parties**

As organisations focus on core business functions and outsource peripheral functions for operational efficiency, they are still responsible for protecting the personal information they pass on to 3rd parties.

>60% of organisations surveyed have a process to review 3rd party compliance with privacy requirements

- **Global approaches to privacy and data protection management**

Organisations are starting to adopt a global approach to managing privacy and data protection risk exposure

46% of organisations indicated that they have European citizens as customers

- **Balancing data commercialisation and consumer choice**

Organisations have an opportunity to build trust with customers by informing them of their commercial uses of customer information and offer a choice as how they want their personal information to be used

*The most common complaint was that information was being used inappropriately (17%)*

How does your organisation rate? See next page.....

For more detailed information on the methodology and further findings from the Deloitte Australian Privacy Index download the report [www2.deloitte.com/au/privacy-index](http://www2.deloitte.com/au/privacy-index)

Marta Ganko manages the Privacy Practice within Cyber Risk Services at Deloitte Australia. Contact Marta on [mqanko@deloitte.com.au](mailto:mqanko@deloitte.com.au)
MOST TRUSTED
Our customers are better off after we use their information

TRUSTED MORE
We give our customers a choice as to how their information is used/shared. Where we don’t, we explain why

TRUSTED A LITTLE
We listen to our customers’ concerns and attempt to incorporate their feedback. We give our customers some choice as to how their information is used or shared. Some of our customers are better off

TRUSTED A LITTLE
We tell our customers what we do with their data, but we don’t give them a choice as to how it is used or with whom it is shared

LEAST TRUSTED
We are compliant, but we know we hide the real story regarding customer usage in our privacy policy

LEAST TRUSTED
We sometimes try to comply with the Australian privacy requirements

LEAST TRUSTED
Our organisation is not required to comply with privacy requirements so we don’t
Magic and rocket science: de-identification is the new black

by Anna Johnston

De-identification ... it’s the latest buzzword.

With all the press it’s been getting recently, you could be forgiven for thinking that de-identification is the magic solution to all the privacy problems facing open data and Big Data projects. But like other forms of magic, this may prove to be just an illusion. Resolving privacy risks is easier said than done.

Increasingly our clients want advice on how to do data-matching, or release datasets under Open Data initiatives, or conduct Big Data analytics, in a privacy-protective manner. Some are seeking to participate in cross-agency research projects; others are facing requests to hand over their data to the NSW Data Analytics Centre; while others are simply seeking to find policy or operational insights by leveraging their own data via business intelligence systems. All are worried about the privacy risks.

There is big picture advice available, like the OAIC’s new guide on how the APPs apply to Big Data, and our own guide to resolving the ethical issues raised by data analytics. But the one aspect of the discussion that I see causing the most angst is de-identification.

Is de-identification the answer? Is it the same thing as anonymisation? How do we even do it?

The Australian Privacy Commissioner Timothy Pilgrim recently described de-identification as “privacy’s rocket science – the technology that unlocks the potential of where we want to go, while protecting individual rights”. But he also warned that just like space flight, “the risks of getting it wrong can be substantial and very public”.

Thud. Ouch. That’s the sound of over-excited data analysts falling back to earth.

As a society, we want privacy protection because it is the oil that lubricates trust, and without trust we cannot function. The fear of being monitored and targeted for what we say or do has a chilling effect on our freedom of speech. Public health outcomes cannot be realised if people don’t trust the anonymity of their health information; think of the clients of sexual health, mental health and substance abuse services in particular. But we also want the full value of data to be realised. If big data analytics can help find a cure for cancer, or prevent child abuse, we’re all for it. Bring it on, we all say.

And for the organisation holding data, de-identification sounds like a magic solution, because if you can reach a state with your data where it is not possible for any individual to be identified or re-identified from the data, then it no longer meets the legal definition of “personal information”. And that means you don’t have to comply with the Privacy Act when you collect, store, use or disclose that data. Legal risks resolved, hooray, let’s all go home.

So de-identification seems to promise that we can have our cake and eat it too. It’s the holy grail of data management.

BUT ... and this is a big but ... can true de-identification ever be achieved, without the utility of the data also being lost?

I have written before about how easily an individual’s identity, pattern of behaviour, physical movements and other traits can be extrapolated from a supposedly ‘anonymous’ set of data, published with good intentions in the name of ‘open data’, public transparency or research. The examples are many: Netflix, AOL, the Thousand Genomes Project, the London bike-sharing scheme, Washington State health data, and my personal favourite, the NYC taxi data.

So should we throw in the towel, and give up on trying to pursue data analytics? (Or even worse, give up on privacy?) No, I don’t believe so. I think we just need to get better at de-identification, because there is more than one way to skin this particular cat.

But we’re not going to get better at de-identification unless we understand it. Privacy professionals should not be seduced by boffins who whisper techy sweet nothings in our ear like ‘SLK’ and ‘k-anonymity’, ‘differential privacy’ and ‘encryption’. Instead, we need to better understand the language and the techniques involved in de-identification for ourselves, so that we can perform proper risk assessments, and know which privacy controls to apply when.
(For what it’s worth: SLKs are keys used to link data about people with confidence, using a code generated from details like their name, gender and date of birth. The code works only as a pseudonym, so don’t even think about describing SLKs as offering true anonymity, or you’ll get a grumpy tweet from me.)

Privacy professionals need to better understand the relative merits and limitations of different de-identification techniques. Open data advocates and data analysts need to develop deeper understanding of the full spectrum of privacy threats that can impact on individuals. And we all need clearer guidance on how to balance data utility and data protection, within the scope of privacy law.

The UK’s Data Protection Commissioner has a really useful Anonymisation Code of Practice – but it’s not a light read at 108 pages. In the US, the National Institute of Standards and Technology has published a 54-page paper on de-identification which laments the absence of standards for testing the effectiveness of de-identification techniques, and just this month academics from the Berkman Center for Internet & Society at Harvard University have produced a 107-page tome proposing “a framework for a modern privacy analysis informed by recent advances in data privacy from disciplines such as computer science, statistics, and law”.

But in the meantime I think we need a brief, lay person’s guide to de-identification. A non-boffin’s set of crib notes, if you like.

Perhaps that will be my blog for another day. Just as soon as I’ve mastered pulling a rabbit out of a hat.

Anna Johnston is a Director of Salinger Privacy
ANZ PRIVACY AWARENESS WEEK – IT'S A WRAP

After a hectic few weeks during Privacy Week in New Zealand and Privacy Awareness Week in Australia we bring you a selection of reports on what went down, one of the highlights being Professor Joseph Cannataci.

Professor Joseph Cannataci in New Zealand for PAW

by Emma Pond

The centrepiece of the NZ Office of the Privacy Commissioner's Privacy week programme was a visit by UN Special Rapporteur on the Right to Privacy, Professor Joseph Cannataci who spoke at the OPC's forums in Wellington and Auckland.

He provided a fascinating and thought provoking insight into what it must be like to think about privacy from such a unique position.

At the Auckland forum Professor Cannataci spoke about the development of the use of 'big data' and the impact on privacy, and questioned the common description of big data as 'the new oil' that was necessary to make the world go round. He asked us to consider in whose interests such a view was - who stood to benefit from the view that the ubiquitous use of big data was the best way forward for the world and its citizens, and what the potential cost of that view was in terms of those citizens' individual privacy in the future.

Professor Cannataci introduced the concept of 'informational self determination', where an individual's quality of life is defined by certain values including the right to privacy and the right to freedom of expression. He provided a fascinating and thought provoking insight into what it must be like to think about privacy from such a unique position.

Drawing on philosophy and literature (including an incredibly prescient quote from Alexander Solzhenitsyn, replicated below) we were also asked to consider what the risks might be for humanity in being constantly under surveillance and subject to manipulation by algorithmic overlords, and the impact this might have on the necessary conditions we as individuals need to be able to develop our personalities (hint: these conditions don't involve being constantly surveilled).

At the Auckland forum Professor Cannataci spoke about the development of the use of 'big data' and the impact on privacy, and questioned the common description of big data as 'the new oil' that was necessary to make the world go round. He asked us to consider in whose interests such a view was - who stood to benefit from the view that the ubiquitous use of big data was the best way forward for the world and its citizens, and what the potential cost of that view was in terms of those citizens' individual privacy in the future.

In summary, Professor Cannataci was an engaging, thoughtful and entertaining speaker, who provided the audience of privacy professionals with an overview of an important current issue in terms of privacy.

"As every man goes through life he fills in a number of forms for the record, each containing a number of questions . .. There are thus hundreds of little threads radiating from every man, millions of threads in all. If these threads were suddenly to become visible, the whole sky would look like a spider's web, and if they materialized as rubber bands, buses; trams and even people would all lose the ability to move, and the wind would be unable to carry torn-up newspapers or autumn leaves along the streets of the city. They are not visible, they are not material, but every man is constantly aware of their existence.... Each man, permanently aware of his own invisible threads, naturally develops a respect for the people who manipulate the threads." Alexander Solzhenitsyn, Cancer Ward, 1968

Emma Pond is Legal Counsel (Privacy) Southern Cross Health Society
ACC Privacy Week

By Fiona Coleman, Principal Adviser and Privacy Officer, Privacy ACC

Privacy Week at the Accident Compensation Corporation (ACC) has become a time of year when we like to take more of an engaging approach to privacy. For most of the year, ACC staff are told to be vigilant in our privacy practices and strictly follow processes to prevent privacy breaches. In Privacy Week, the processes are still there, but we like to pat ourselves on the back for a job well done and have a little fun.

ACC’s campaign last year involved a staff member known as Captain Privacy. We ran a video and poster campaign where the captain caught people doing the wrong thing (eg talking about job interviews in a public lift, leaving documents at the bus station, or not checking that visitors to the building were authorised). The message was ‘Don’t be that guy, do the right thing by privacy’.

This year, we turned that message around and instead people were praised for doing the right thing. Following a gruelling round of staff auditions we appointed some new privacy heroes called the Mission Zero Agents. They roamed ACC catching people doing the right thing to protect personal information and would then recruit them to become agents themselves. A 1980s cop show theme was employed where the agents wear leather jackets and aviator sunglasses to add a sense of fun to the message. Mission Zero is the mission to achieve zero privacy breaches by doing the right thing at the right time in the right way. The messaging closely aligns to our wider organisational programme focused on improving customer experience.

Every day, a new video featuring the agents and their recruits was launched on ACC’s staff intranet. Each new theme highlighted privacy challenges in the organisation that needed to be addressed and prizes were awarded for answering simple questions related to the video.

All staff received a letter explaining the challenges and a Mission Zero Agent badge of their own (a selfie competition encouraged staff to send in pictures of themselves with the badge). And just to make sure some serious privacy learning occurred, ACC’s mandatory privacy learning module was relaunched with a fresh new look.

We’re proud of the campaign and the positive messages that will continue for the rest of the year. We know staff enjoy this approach, it gives them the opportunity to see privacy as more than a compliance exercise and is essential to delivering good customer service.

Fiona Coleman is Principal Adviser and Privacy Officer, Privacy ACC
Is there hope for privacy in an Internet of things world?

By Dawn Swan

The Internet of Things (IoT) is setting off a wave of change but raises privacy concerns, according to Vikram Kumar who spoke at a Technology & Privacy Forum in Wellington organised by the Office of the Privacy Commissioner during New Zealand’s Privacy Week.

Vikram, a technologist and founder of an IoT company, KotahiNet, says IoT is a web of devices, not just one device, which are always connected.

They are in your home and elsewhere and have millions of sensors that collect and monitor everything we do. ‘Smart’ products in our homes send vast amounts of information to unknown destinations; the aggregation of real-time and historical data gives ‘big data’ a whole new dimension; and security can be compromised by suppliers who neither care about nor provide safe products and services.

“There is extensive monitoring, little we do is not tracked and analysed by the industry. This results in ubiquitous data collection where the data is invisible and re-use unclear."

He provided a simple example of an electric toothbrush: this could be connected via Bluetooth to an app which motivated and rewarded the user to brush their teeth. It was then sold to developers who converted the toothbrush and app into a game for children to get points. Later it was sold to a dental health insurance company which fundamentally changed things and how the information collected on the device would be used.

Vikram says the web of devices will get bigger in the long-term and noted it has already affected how communication, entertainment and media industries work. He predicts it will next set off a wave for physical industries (agriculture, infrastructure, and cities) and the potential is understated.

Vikram observed that new services are being driven by the use of data analytics – this means more data, extensive re-use of that data and combining it with other datasets. He referred to this as “supercharged big data”.

There are low or no access barriers to IoT and it is always on and listening. Features that cause concern are: no digital or screen interface which makes accepting terms and conditions more complicated, what the data is being re-used for and what happens to the data if the company goes out of business. He believes many devices have poor security due to a lack of incentives and skills.

A fundamental change with IoT is also that you can upgrade software by connecting to internet so ‘things’ can have long lives (10-20 years)

“Instead of having a normal washing machine, we now have computers that wash clothes and collect intelligence across all washing machines. There is also a difference between personal and device data."

Vikram predicts IoT will have a bigger impact than most expect and while it brings new challenges such as a lack of digital interface and big opportunities and benefits he warns that there are insufficient privacy protections.

You can view the presentation can be viewed on YouTube https://www.youtube.com/watch?v=jm7ur-I5tdg

Dawn Swan is Privacy Officer at Inland Revenue NZ in Wellington and a member of iappANZ’s New Zealand subcommittee
Launch of Australian PAW 2016:
Breakfast with the Privacy Commissioner and the Professor

by Emma Hossack

A full house at The Westin in Sydney this year, and in my view the best ever. Really. Our Privacy Commissioner Timothy Pilgrim definitely had a spring in his step, now that his office has been recognised in the recent Budget and given some well-earned funding and security. Pilgrim spoke of how privacy affects everyone and every organisation, with the Deloitte Privacy Index showing that 94% of Australians prefer trust over convenience. As an aside I saw the iappANZ Board look very pleased about this as they have chosen “Trust in Privacy” as the theme for this year’s 14 November 2016 Summit.

Other points which our Privacy Commissioner impressed upon us were:

- The critical Privacy by Design concept that privacy is not a bolt on from the Regulator’s viewpoint;
- The OAIC will have a privacy professionals network, with the first meeting being held in West Australia and which of course will work closely with iappANZ;
- A draft guide on Big Data key principles being released;
- The Australian Privacy Principles are technology agnostic for a good reason;
- The quote by our PM that “Government information is a national resource” and that de-identification will be an important area for the OAIC;
- That the OAIC is looking at a Consumer Privacy Network being established for education and consultation;
- The OAIC had 117 voluntary data breach notifications, 19 assessment over 101 entities across government and business and a whopping 12,241 privacy enquiries, and
- The key definition of ‘personal information” is being reviewed by the Full Bench Federal Court in August in an appeal of the Commissioner’s determination in Grubb v Telstra.

And if you want to read it all verbatim from the Privacy Commissioner see here.

The next speaker, was the wonderfully titled “United Nations Special Rapporteur for Privacy”, Professor Joseph Cannataci. I mis-heard and thought he was the ‘raconteur’ and well may he have been called.

Professor Cannataci caught our attention first up with his declaration that he sought his daughter’s consent to mention her lifestyle in his Blog. And he didn’t hold back with his frank appraisal of where he thought Australia should be going with regards to privacy. “Every risk is worth taking as long as it's for a good cause and contributes to a good life”, according to Richard Branson, and the Professor went on to challenge Australia to get moving and be true to our claim to be the land of “the fair go.”

Australia has, he said, had loads of reports and shows an awareness of privacy, but says the Professor, we must do something! Europe isn’t perfect, but it does recognise privacy as a fundamental human right – which Australia does not. Some of the audience clearly felt a bit uncomfortable - it sounded a little like one of our former Prime Minister’s comments about one of his successors, “...he won't get out of bed unless a focus group tells him to choose left or right.”

However you view it, it was certainly stimulating. “Australia needs to show the world that it is as good at privacy as it is at cricket!” declared Professor Cannataci who provoked discussion and praised our early foray with the extraordinary leadership of Michael Kirby, the Chair of the OECD Guidelines. Terrific questions, and a decisive responses - Cannataci made it clear the choice between security and privacy is not binary – “I want both!” A newly empowered Commissioner, a discursive speaker and an engaged audience. Great start to a super week and new beginning for privacy discourse in Australia.

Emma Hossack is a Board Director of iappANZ and CEO of Extensia
A report from the OAIC

May was an eventful month for the Office of the Australian Information Commissioner, and one that we think will have positive effects in Australian privacy awareness and governance for some time to come.

Budget announcement

The month started with the 2016 Budget, which confirmed that previous proposals to disband the OAIC were abandoned. The Budget included allocations to fund, ongoing, the OAIC’s privacy and FOI regulatory functions — recognising the important rights and protections that are provided to Australian communities through the FOI and Privacy Acts. This formally ended a period of uncertainty for OAIC, and allowed the OAIC team to approach Privacy Awareness Week 2016 with a renewed outlook and confidence.

Breakfast to launch PAW with special guest

This year Australian Privacy Awareness Week (or PAW) took on an international flavour, with a visit by the first United Nations Special Rapporteur for Privacy, Joseph Cannataci. Prof Cannataci was the key speaker at OAIC’s Privacy Business Breakfast on May 16, which was the most well-attended PAW Breakfast OAIC has staged. Over 200 attendees from nearly 100 different businesses and organisations enjoyed the Rapporteur’s thought-provoking challenge for Australia to take a regional lead in contemporary privacy law, and addressing the complexities it now attracts. The Rapporteur also delivered a well packed lecture at Australian National University, enjoyed chatting with IAPPANZ members at their PAW week drinks in Sydney, and attracted significant new attention to privacy issues though media events. His interview with ABC Lateline is one example.

Out and about

Meanwhile, the Privacy Commissioner and Assistant Commissioners spoke at business events in Sydney and Melbourne, with a combined audience of just over 1000 people, which was a great endorsement of how privacy awareness and privacy governance have matured in Australian business. The OAIC released new resources, including new privacy tips for parents and carers, and new access and correction guides, all of which are still available from our PAW 2016 website. We also worked with Facebook Australia to deliver a series of pro-privacy videos, providing fantastic new reach to youth audiences.

As the sun set on PAW week, it was time to follow it west, as the Commissioner visited Perth to lead a series of training and stakeholder engagement activities that made a substantial and positive impact on privacy awareness in the WA capital. The visit included a lecture at Edith Cowan University on privacy as a human right — which was well attended by many leaders of Perth’s academic and science community, including WA’s Chief Scientist — and a business breakfast attended by over 100 leaders of Perth’s business and corporate communities, kindly hosted by Gilbert + Tobin lawyers. The Commissioner also visited ABC’s Perth studios for an interview and to answer privacy questions sent by listeners.

Privacy Professional Network

The Perth visit also included the first face-to-face meeting of the OAIC’s new Privacy Professionals Network (PPN), in which local privacy practitioners could hear updates from the OAIC directly, and pose questions and concerns about best privacy practice and current issues. This was a very positive session and the Commissioner noted the importance of having the first meeting in WA, symbolising “that the national privacy regular will engage with stakeholders on a national basis.”

So all in all, a very big and very eventful Privacy Awareness month. The OAIC wants to thank iappANZ for all its support of PAW2016 events, and for helping to promote the first PPN meeting to WA practitioners. We look forward to working with iappANZ on many future PPN events as we develop the calendar for this new consultation network. Other meetings of the PPN will be announced shortly, so please join our PPN mailing list to receive updates on future events, which will be held both online and in various Australian city locations.

Richard O’Neill is the Director, Strategic Communications and Coordination at the OAIC
“Intimitatem Post Mortem” Privacy After Death

by Kyle Lees

In the absence of black letter edification, what this gap has created for the spectre themselves (alongside the bereaved) is a jerry-rigged collage of piecemeal rights protections provided by a range of broadly 'analogous' legal mechanisms made up of Freedom of Information (FOI), various State protections, medical ethics and legal duties of confidentiality.

Being in such liminality is haunting.

Decisions from the NSW Civil and Administrative Tribunal (Tribunal) have shown that broad privacy concerns of surviving family members also weigh on the decision to release information through FOI mechanisms. When such cases come before the Tribunal decisions can be made against FOI requests in cases where the release of death-scene or autopsy photos or coroner's reports would cause anguish, social and even cultural harm to the deceased person's family.

Nevertheless, whilst it remains a public interest test, it is worth noting that a disclosure to an FOI applicant is disclosure to the world. In contrast, French laws and subsequent judicial decisions en droit appear to define privacy rights of individuals in France as encompassing all aspects of an individual's spiritual and physical being - giving in principle each person the power to define the boundaries of their own private life and the circumstances in which private personal information may be publicly released. This right to privacy survives death, giving family members the ability to make privacy claims on behalf of the deceased.

The Digital Necropolis

In an age which has enshrined the online, and with Facebook arguably the genesis of the social media tsunami - more than three Facebook users die every minute. Moreover, nearly 30 million Facebook users died in the first eight years of its existence - leaving accounts and privacy controls in digital limbo because the majority of those users hadn't prepared for their digital, metaphorical, or literal death. What this serves to create is a digital graveyard replant with a minefield of potential privacy pitfalls. How will Facebook and any non-tech savvy families of these people manage this amount of digital content without relying on firm and consistent legal direction? The scope here continues to grow. Some writers have noted that by
2065, the amount of deceased users on the platform will have eclipsed the living.

Despite the Privacy Act not applying to the deceased, the Office of the Australian Information Commissioner (OAIC) has offered guidance to government agencies "to respect the sensitivities of family members when using or disclosing information about deceased individuals". Parallel to this convention is the duty of patient confidentiality envisaged by Hippocrates and ethical protections around genetic information of the dead extended through the belaboured and fraught implementation of the draft National Health Privacy Code.

Alternate Models

Outside of pure legislative overhaul, two models could be offered as a means for protecting a deceased person’s privacy, especially given the advent of the increasingly encroaching online ecosystem. The first is rooted in contract law, while the second is rooted in proprietary law. The contract theory relies on looking at terms of service agreements that users accept to determine the scope of their posthumous privacy rights. Meanwhile, the property theory evaluates whether a deceased user’s digital assets may be treated similarly to real property after death. Yet even these measures do not sufficiently protect a deceased person’s right to privacy. As technology’s ubiquitous role in everyday life continues to develop, legislative reform should consider the realities of modern technology and its impact on the survival and perpetuity of personal information beyond death. As is currently being contemplated in South Australian Parliament, extending existing tort law to include Privacy could also serve to include mindfulness of a deceased person’s digital assets in order to redesign a key ideological oversight: that a person’s right to privacy survives death. This recognition that a deceased person ought to have an enforceable right to privacy is the best way to protect the right to privacy post mortem. Extending this sentiment posthumously is reasonable: the law already recognises the survival of a person’s dignitary interests past death. This is coupled with the risk that a mausoleum of digital assets can serve to convey much more information – damaging or otherwise – about a person, than the lost echoes of a material world.

If Privacy is indeed dead as some argue, it appears the debate into the privacy rights of the deceased in Australia remains alive and well.

Kyle Lees writes in a personal capacity and as an iappANZ member.


Productivity Commission: Privacy 3.0?

by David Templeton

We’ve mentioned the Productivity Commission’s inquiry into Data Availability and Use a couple of times in by-lines, but this review really requires deep consideration.

This review offers a fresh look at a three highly topical policy issues:

- Data sharing;
- Data Access; and
- Trust.

Judging from the tone of the Issues Paper, Data Availability and Use, this is a ‘take it from the top’, ‘white sheet of paper’, ‘suspension of disbelief’ type Inquiry that has the potential to throw open established privacy norms going back over matters considered by the ALRC and subsequent consultations.

The Inquiry tackles very good questions about democratisation of data and how technology can augment the rights of individuals, approaching the topic from the perspective of the economic and societal benefits that could flow from opening up otherwise closed datasets to broader uses and additional users. At the same time the Inquiry explores how a changed and arguably more open system of data regulation can retain and build the trust required to maintain participation.

For many of our organisations, this Inquiry will look like a godsend, an opportunity to revisit what some might regard as sacred cows. To others, the Inquiry might look like an exercise in ill-fated good intentions, paving that fabled road.

Either way, the Inquiry demands our full attention. Submissions on the Issues Paper close on 29 July and a draft report can be expected in early November for further consultation.

Data Sharing (and use!)

The Inquiry invites an open ended discussion on data sharing, inviting submissions on opportunities that could arise from sharing or pooling datasets, within and across both Federal and State governments, within the private sector and between Government and private sector. Consideration of the current barriers and whether they are unnecessary or excessive, and consideration of the competition issues that might arise is also invited.

The Issues Paper argues that data is a key economic resource. In a public context, the Commission cites a number of its past Inquiries in which access (and by implication, use) limitations on government datasets limit the availability of data as a resource, leading to issues such as:

- Duplication and repeated collection;
- Lack of transparency and lack of utility to individuals, which can result in a lack of accountability by obfuscating policy outcomes; and
- Limitations on access for research and missed potential for evidence based policy.

In a private sector context, the Commission anticipates that wider access to data (and again by implication broader usage) might have benefits in efficiency, consumer empowerment, competition and innovation.

Data Access

At the same time, the Inquiry addresses ways to unlock the utility of Big Data for individuals, asking whether individuals accessing their data should be offered access in meaningful ways, responsive to the context of an individual’s enquiry and beneficial to the individual by offering useful information. The Commission has the UK Mydata initiative and New Zealand’s Integrated Data Infrastructure initiative in mind as examples of open data access delivering real value to individuals. The Government’s reference to the Commission was in part driven by the Harper Review’s recommendation that Government should, in giving access to individuals, ‘present information and choices in ways that allow consumers to access, assess and act on them’.

Consideration of the both the opportunities, and the costs of providing value add-analysis to individuals is invited.

Trust

Lastly, the Inquiry invites submissions on how trust can be maintained by all stakeholders in the integrity of data use and disclosure, and invites a broad discussion (revisititation) of privacy regulation and data security. To illustrate, these are among the questions raised on this topic:

“What weight should be given to privacy protection relative to the benefits of greater data availability and use, particularly given the rate of change in the capabilities of technology?”

1 Competition Policy Review, Final Report, page 305
“Are further changes to the privacy-related policy framework needed?”

“How should the risks and consequences of public sector and private sector data breaches be assessed and managed? Is data breach notification an appropriate and sufficient response?”

So in conclusion, if you aren’t already working on this, please take a look and consider the opportunities and threats it might raise for your organisations or clients.

David Templeton is the Secretary of iappANZ and works at ANZ as Senior Manager in Product, Strategy and Marketing.
IappANZ 2016 Summit – 14 November 2016, Sydney

2016 iappANZ TRUST IN PRIVACY Annual Summit

MONDAY 14 NOVEMBER, 2016

Dockside, Darling Harbour, SYDNEY

“Excellent sessions, challenging and thought provoking, thanks iappANZ”, Sandra Kelman, Senior Privacy Adviser, Ministry of Justice, New Zealand.

Are you up to date with the latest privacy trends, developments and issues?
Are you interested in hearing from some of the world’s leading privacy thought leaders?
Do you want to network with like-minded people?

Come and join us for a day of insightful information and discussion on the key issues regarding privacy now and into the future.

Earlybird and registration information

Register here
### Events

__Note: the Adelaide Data Breach seminar has been postponed. A new date will be announced.\

<table>
<thead>
<tr>
<th>Where and when</th>
<th>Event details</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WEBINAR</strong></td>
<td><strong>ARCA Credit Reporting Corrections Webinar</strong>&lt;br&gt;Ensure your teams are complaint with the obligations under the Privacy Act. Under section 21U of the Privacy Act, credit providers should ensure the credit information they hold for individuals is accurate, up-to-date, complete, relevant and not misleading.&lt;br&gt;In practice, correcting an individual’s information can be tricky, particularly within the 30 day correction timeframe placed on credit providers.&lt;br&gt;The webinar will cover: The legal processes and obligations around dealing with requests for correction of an individual’s information – a number of scenarios to help attendees put their learning into practice.&lt;br&gt;Who should attend this webinar? The webinar is open to all industry participants, and is aimed at staff members and managers who handle or oversee requests for data correction, undertake corrections or make correction assessments.&lt;br&gt;Who will run the webinar? ARCA has organised this webinar as part of our ongoing Learning Solutions series. Legal Credit Reporting expert, Debra Kruse, will deliver the webinar.</td>
<td><strong>Cost:</strong>&lt;br&gt;Members $250 incl. GST&lt;br&gt;Non-members $300 incl. GST&lt;br&gt;How to sign up: Click <a href="#">here</a> and follow the instructions to register. Once you have registered, you will be emailed a link to the webinar.&lt;br&gt;Further questions: if you need more information, or you would like to organise a Corrections Webinar in-house, please contact:&lt;br&gt;Julianne Henry&lt;br&gt;Education Development Manager&lt;br&gt;Phone: 0438 353 472 or +61 3 9863 7855&lt;br&gt;Email: <a href="mailto:jhenry@arca.asn.au">jhenry@arca.asn.au</a></td>
</tr>
<tr>
<td><strong>AUCKLAND</strong></td>
<td><strong>Privacy After Dark</strong>&lt;br&gt;Come and join us for a casual get together of like-minded people with an interest in privacy</td>
<td>Free to members and non-members.&lt;br&gt;More information &amp; RSVP: <a href="mailto:emma.heath@iappanz.org">emma.heath@iappanz.org</a>&lt;br&gt;RSVP essential for catering purposes.</td>
</tr>
<tr>
<td><strong>AUCKLAND &amp; WELLINGTON</strong></td>
<td><strong>An Electronic Health Record For Every New Zealander by 2020. What Does This Really Mean?</strong>&lt;br&gt;The recent strategy announced by the Ministry of Health to</td>
<td>Free for members&lt;br&gt;Non-members $99NZD (deductible from iappANZ joining fee if you become a</td>
</tr>
</tbody>
</table>
establish a national electronic health record for individuals will affect every New Zealander. The strategy will impact how and where medical records are stored and used by medical practitioners (and potentially others) and how patients will be able to access their medical information. It is intended that electronic medical records will be accessible across the country. The Ministry of Health has stated that “Privacy is Assured”.

This event is for leaders and senior managers in health, health technology service providers, privacy professionals and leaders in patient advocacy to help understand the strategy implications and be part of the discussion.

The event will be held in Wellington and via video link in Auckland.

You will:

1. Hear from Jill Bond, Executive Director, Office of the Director General of Ministry of Health, about the details of a national eHealth Record and the rationale for adopting the strategy.
2. Learn about the privacy impacts of an eHealth Record system from Sebastian Morgan-Lynch, an expert on the topic from the Office of the Privacy Commissioner.
3. Understand how this will affect the efficacy of medical practitioners and patients.
4. Gain insight into the lessons learnt internationally in implementing similar systems from Dr Bernard Robertson-Dunn, an IT expert who is currently Chair of the Health Committee of the Australian Privacy Foundation.

**SAVE THE DATE**

iappANZ TRUST IN PRIVACY Summit

Are you up to date with the latest privacy trends, developments and issues? Are you interested in hearing from some of the world’s leading privacy thought leaders? Do you want to network with like-minded privacy people?

Come and join us for a day of insightful information and discussion on the key issues regarding privacy now and into the future.

Speakers and program agenda to be announced shortly.
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 iapp ANZ 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 iapp ANZ 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.

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/](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](mailto:veronica.scott@minterellison.com))
**Carolyn Lidgerwood** ([carolyn.lidgerwood@riotinto.com](mailto:carolyn.lidgerwood@riotinto.com))
**David Templeton** ([David.Templeton@anz.com](mailto: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.*