Privacy Unbound is the journal of the International Association of Privacy Professionals, Australia-New Zealand (iappANZ).

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.

CONTENTS

PRESIDENT’S LETTER

PRIVACY UNBOUND 2016 WRITERS PRIZE

PRIVACY HIGHLIGHTS FROM 2016

REPORT FROM THE iappANZ 2016 SUMMIT - TRUST IN PRIVACY

SOCIAL LICENSE AND PRAGMATIC TOOLS: HOW TO UNLOCK PUBLIC DATA

GDPR: A MIDDLE GROUND TO THE DE-IDENTIFICATION DEBATE?
Welcome to the last Privacy Unbound for 2017, whilst you are busily preparing for some much deserved time off over the festive period we hope you have an opportunity to flick through the edition and reflect on some of the key issues we are facing as privacy professionals and contemplate emerging trends for 2017.

The last edition for the year is also the Privacy Unbound editors opportunity to announce the winner of the 2016 writing prize. The competition was very strong in 2016 with the judging panel taking a number of weeks to decide on a winner, a testament to the quality and relevance of the content coming from the membership for inclusion. We are always looking for content so encourage members to touch base with our editorial team.

Planning for events and activities in Australia and New Zealand in 2017 has started, including a review of our sub committees, Privacy Awareness Week in May, the APPA conference in Sydney in July and the annual Summit later in the year.

On behalf of the iappANZ board I wish you all a safe and happy festive period and look forward to seeing you in 2017.

KATE MONCKTON
President, iappANZ
THE PRIVACY UNBOUND 2016 WRITERS PRIZE

The Privacy Unbound Editorial team has spent the last 4 weeks reading and re-reading every published article from the past 12 months to determine the 2016 Privacy Unbound writing prize winner. Each article was subject to a number of criteria including originality, relevance, insights given and enjoyability to read.

After much debate the editorial team are pleased to announce Kyle Lees, Privacy Advisor at NBN as the 2016 writing prize winner for his article “Pokémon GO: “The Delusion of Solitude”. Kyle has been a great contributor over the course of the year. His article “Intimitatem Post Mortem” Privacy After Death” from the May/June issue was topical, interesting, well written - and we’re all going to end up in his “Digital Necropolis” one day. His article from the July/August issue “The Reckoning: Census Fail” was a neat perspective of the issues.

A special mention to Anna Johnson of Salinger Privacy for her article “Why you might want to become a Jedi Knight for this year’s Census“ which came a close second and Peter Leonard for his Grubb article and also to Fiona Coleman for her piece about what the ACC did during PAW - practical and different.

All iappANZ members are encouraged to submit pieces for editorial consideration in 2017 and congratulations once again to Kyle, you can find his winning piece in the June/July Issue of Privacy Unbound in the members section of the iappANZ website.
Q&A WITH WRITING PRIZE WINNER KYLE LEES

Kyle Lees was born in the wake of a smelt flame in Maidstone, United Kingdom (UK) and thereafter soon moved to the Lucky Country. Here, he went school in Sydney before heading back to the UK in his late teens for matriculation in law at the University of Kent, Canterbury, later going on to study law at the Universiteit van Amsterdam (UvA), in the Netherlands. After settling back in Australia Kyle has worked in a range of technology, media, government, policy and legal roles for the last decade or so, including at the national broadcaster. He enjoys sailing and spending time with his family, where he lives on the New South Wales Central Coast.

He currently works as a Privacy Advisor at nbn, a challenging and dynamic role, which he enjoys.

Q: What first made you interested in privacy?
A: Kyle says this is a difficult question, and one which is going to result in a long and rambling answer!

Kyle has always found privacy fascinating from a human rights perspective. More recently, Kyle says the "ubiquitous trajectory and resulting fissures which cleave between new forms of media, law, technology, and humanism - have served to awaken in him the distant memory of a panopticon legal nightmare. The very kind envisaged by Kafka, and breathed into life by Camus".

Q: If there was a prize for the "epic privacy fail" of 2016 - who would you award it to?
A: Kyle thinks this year's winner is undoubtedly, the Census debacle, and congratulates the Australian Bureau of Statistics (ABS).

Q: On the other hand, who would you single out as a "privacy champion" in 2016?
A: Here, Kyle applauds Timothy Pilgrim and Ben Grubb for their battle to include metadata as 'personal information' in the context of Australia's Privacy Act data protection rules.

Q: Present shopping. How do you approach it? or What do you buy for the person who has too much already?
A: Kyle says he tries to stay in the present. He says his approach is one of mirth and that he generally tries to give the gift of laughter, or failing that, music.
iappANZ is the pre-eminent forum for privacy professionals in Australia and New Zealand. We are affiliated with the International Association of Privacy Professionals (IAPP), the largest and most comprehensive global information privacy community and resource with more than 23,000 members. We work with public and private entities across all industry sectors in Australia and New Zealand as well as the Privacy Commissioners in both countries.

iappANZ offers our members a wealth of opportunities to expand their privacy knowledge, compliance, interests and networks. Our members in Australia and New Zealand represent some of the best minds in the privacy field, from large public companies and the government sector to not for profit, SMEs and individuals.

www.iappanz.org | +61 2 9431 8684 | admin@iappanz.org
The Office of the Privacy Commissioner in New Zealand ended 2016 with a flurry of activity, with Privacy Research Week events in Auckland from 13th to 16th December. These began with the 3-day Privacy, Security & Trust conference, hosted by Unitec, for which Privacy Commissioner John Edwards was Honorary Chair. The week included the 2-day Asia Privacy Scholars Network 5th International Conference, the OPC’s Privacy Research Symposium, and ended with the Sexuality and Privacy in Aged Care Forum. More information about Privacy Research Week can be found here.


The Privacy Research Symposium was a first for our office and highlighted four research projects supported by our Privacy Good Research Fund. These included studies on the ethics of information sharing; high needs clients; electronic healthcare records, and cyber-safety for children


**Law reform**

A big focus this year has been providing advice and support to the Ministry of Justice and Parliamentary Counsel on reforming the Privacy Act. The main objective of the impending law change is to update the country’s 23 year-old privacy legislation and to ensure its consistency with the privacy laws of other OECD countries.

Some of the proposed changes we are likely to see in a law change include:

1. Mandatory breach notification (we received 148 voluntary notifications in 2015/16
2. Access determinations
3. Compliance notices
4. Penalty powers (creation of offences of destruction of documents and ‘pre-texting’)

We’re also discussing other additional matters that might be included in new privacy legislation to ensure it responds to the current environment.

The draft Bill is scheduled to be introduced to Parliament mid next year. However, we are highly conscious of the uncertainties of the Parliamentary timetable, especially with recent news of a change of Prime Minister and election year looming. We’re keeping our fingers crossed.
Information sharing

Government information sharing has been a dominant theme throughout 2016. We supported government agencies in information sharing in a variety of different ways, from informal consultations on the application of the Privacy Act to ongoing work to produce formal Approved Information Sharing Agreements. We gave advice on major “big data” projects including the Integrated Data Infrastructure, the Social Investment Unit and the Data Futures Partnership. We encouraged these projects to use privacy to increase the value of their data sets, particularly through the principles that deal with accuracy of information. We engaged in a new government process in which agencies were asked to find situations where current privacy law was preventing them from sharing information with one another. We worked with a number of agencies to identify those situations, and to find ways to appropriately share information in compliance with the Privacy Act. This helped agencies share information without compromising privacy, and without having to wait for a law change in order to get things done. The Office has a growing role in assisting agencies to undertake information sharing in responsible ways and have participated in a number of fora. As part of that effort, we also launched an Advisory Opinions policy, https://www.privacy.org.nz/news-and-publications/guidance-resources/advisory-opinions/ in order to provide clear guidance to agencies on specific situations.

Building knowledge

We also worked on sharing information of a different variety. One of our big projects in 2016 was the development of AskUs: www.privacy.org.nz/ask AskUs is an interactive knowledge base that aims to answer any of your privacy questions. We started with a core of several hundred questions and answers, and we’re actively working to expand these answers in response to the questions the public pose. Check it out for yourself, and see if you can throw us a curly question! We may not have the answer yet, but your question will spur us to write one.

Intelligence and security

We have worked throughout the year on intelligence and security developments and policy. The Independent Review of Intelligence and Security in New Zealand reported back (the Cullen Reddy report) early in the year and we were pleased to contribute to that process. Privacy Commissioner John Edwards attended the first International Intelligence Oversight Forum in Bucharest in October, and in the same month, we made a submission on the New Zealand Intelligence and Security Bill. Our submission supported applying all of the privacy principles to intelligence agencies, and strengthening the oversight role of the Privacy Commissioner, amongst other things.

Privacy Week

During Privacy Week in May, our Office hosted a visit from UN Special Rapporteur for the right to privacy, Professor Joe Cannataci, who gave thought-provoking presentations at our Privacy Forums in Wellington and Auckland.

We released our latest UMR survey results on public perceptions of privacy which demonstrated that 65 percent of New Zealanders continue to be concerned about privacy. We also asked respondents about information sharing. Significantly, respondents were more open to information sharing when safeguards were put in place. A majority were willing to share data as long as they could opt out if they chose (57 percent); there were strict controls on who can access the data and how it is used (59 percent), and data is anonymised and they couldn’t be identified (61 percent). New Zealand’s first ‘Right to Know Day’ - a day dedicated to raising awareness of people’s right to see their own personal information that agencies hold was also held in Privacy Week, and we launched our online request tool - AboutMe.

International Conference

Privacy Commissioner John Edwards continued in the role of Chair of the International Conference of Data Protection and Privacy Commissioners (ICDPPC) and our Office continued to act as the Secretariat: https://icdppc.org/

The conference in October in Marrakech, Morocco https://www.privacyconference2016.org/ discussed emerging privacy challenges, particularly including robotics, artificial intelligence, and encryption.

Trends for 2017

Other developing trends in data protection and privacy include:

Promoting and deploying Privacy-by-Design, Privacy Impact Assessment and privacy enhancing technologies

There is no trade-off to be made between innovation, enterprise and privacy. Good privacy and security practices, when designed in to new technologies, become a selling point and improve the whole network. Privacy is a fundamental human right. But like many other rights, it is not absolute but access to communications by law enforcement, security or intelligence agencies should be according to consistent legal standards, regardless of the jurisdiction.
Promoting transparency in relation to access to or use of personal data for purposes other than those for which the data subject has consented.

Edward Snowden’s allegations showed us how the online platforms that many of us use on a daily basis were allegedly freely available to agencies for intelligence purposes. Several of the most prominent online platforms responded with regular “transparency reports”, in which they revealed the nature and extent of official calls on their customer data. Last year, our Office undertook a project to get a better view of personal information requests by New Zealand law enforcement agencies. Over a three-month period, government agencies made nearly 12,000 requests for personal information from 10 New Zealand companies last year, and the companies complied with 11,349 of those requests. We are working to encourage more agencies to adopt this reporting practice.

Developing and promoting appropriate standards and safeguards for the de-identification of personal data, and for the prevention of re-identification of individuals from de-identified datasets

Industry and governments alike are clamouring to reap the benefits of so-called “big data”. The ability of data scientists to derive public benefits from analysing large datasets is undeniable. But to get the societal benefit of such data, it is not necessary to identify individual mobile phone users, and to do so would in many cases breach privacy principles. Researchers have proven the ease with which individuals could be extracted from a supposedly de-identified dataset.

Ensuring citizens and consumers continue to have transparency about the basis on which automated decisions affecting them have been made

At the recent International Conference of Data Protection and Privacy Commissioners in Morocco, attendees heard that even though it is still quite undeveloped and not widely understood, the concept of “algorithmic transparency” is facing considerable challenges in the light of artificial intelligence, machine learning, and “unpredictability by design”.

Data portability

Just as number portability has proved crucial in promoting competition in the mobile phone sector, so is data portability an important concept in promoting consumers’ rights, and facilitating the ease of access to, and exit from, telecommunications, online, and other services. Data portability is part of the European General Data Protection Regulation; due to come into effect in 2018, and will need to be provided for beyond Europe.

There is much on the horizon to ensure 2017 will be an interesting and challenging year for privacy practitioners and regulators alike.
REPORT FROM THE iappANZ 2016 SUMMIT
BY HELEN LAUDER & VERONICA SCOTT

The annual iappANZ Privacy Summit was held on 14 November 2016 at Cockle Bay Wharf in Sydney. The theme was ‘Trust in Privacy’. We were treated to a packed day of keynote speeches, through leadership and the opportunity to catch up and network with fellow privacy professionals from across Australia and extend a particularly Nau mai, haere mai to our New Zealand members.

Some takeaways

If you are too busy to read the full report, as you go into 2017, take these thoughts with you from the Summit:

- GDPR: organisations are not ready, it is taking away flexibility and simplifying the conversation by making the approach to compliance all about avoiding penalties
- Organisations should be thinking about how we treat and value personal information in the context of a new world order of data driven technology
- As privacy professionals, we need to be proactive, engender trust, stay ahead.
- Privacy is about people, trust, ethics and transparency
- Its no longer simply a question of processing data - data has to be at the centre.

Views from our Privacy Commissioners

After a warm welcome from our fabulous iappANZ president Kate Monckton, the Summit kicked off with an update from the Australian Privacy Commissioner, Timothy Pilgrim PSM.

Mr Pilgrim welcomed the planned iappANZ Australian and New Zealand privacy certification and indicated that the OAIC will look for this accreditation when undertaking compliance audits. He emphasised the importance of governance and transparency, including in building trust with customers. Acknowledging the impact of social media on the privacy debate following the crash of the Census website and the privacy concerns at the announcement that the ABS was retaining personal information for longer than previously understood, Mr Pilgrim confirmed his investigation into the website incident and confirmed that no personal information had been compromised as a result of the DDOS attack.

We were also given an update on the re-identification offence Bill which will amend the Privacy Act 1988 and, which has now been referred to a Senate enquiry and Mr Pilgrim stressed the important and ongoing issue of de-identification, as well as providing an update on the activities of his Office throughout the year. He explained his role as both Privacy Commissioner and now Australian Information Commissioner and the intersection of the information laws noting the increase in people seeking access to Government information. Looking ahead Mr Pilgrim touched on the topics that his Office will be focussing on in 2017. He looked forward to the introduction of mandatory data breach notification (noting there were still many data breaches going unreported and some for long periods of time), he will be encouraging privacy by design, talking more about what the new GDPR means for Australia, developing further international cooperation in privacy governance and finally he confirmed that the Community Attitudes to Privacy Survey would be conducted. It will be launched in Privacy Awareness Week, so watch this space.
The New Zealand Privacy Commissioner, John Edwards, then spoke on the proposals to change New Zealand Privacy Act in the context of why we need privacy and to respect privacy, noting the growth in data, social media and online communications. These also include mandatory data breach notification as well as enhancements to the Commissioner's powers and new tools he would have, such as the ability to issue compliance notices and oversight of agencies. Currently his offices is limited to exerting influence with no power to impose penalties. He also discussed the Harmful Digital Communications Act 2015, which includes a range of measures designed to prevent and reduce the impact of harmful digital communications, such as cyberbullying. Finally he discussed the new 'AskUs' online knowledge base available at: https://www.privacy.org.nz/blog/ask-us-about-privacy/, which is designed to answer questions about privacy issues and how they might affect individuals, agencies and businesses.

KEYNOTE SPEAKERS

The seven habits of highly effective privacy professionals

Our first keynote speech was by the fascinating Simon McDougall who is the Managing Director of Promontory and has a wealth of experience in privacy. Simon discussed what we all want to develop – the seven habits of highly effective privacy professionals. He sees privacy is being about:
- Trust
- Innovation
- Digital
- Reputation

and explained how we can 'sell' privacy in our organisations by emphasising trust and reputation, then we will be ready for a crisis.

He suggested we be more like the InfoSec sector and get ourselves up the curve. We should have a vision, sell privacy, sell ourselves, be proactive, think win-win, never let a good crisis go to waste, but own it, make friends and engage with others, think about what we have in common with them and evolve, keep up to date and be the bridge between the various risk functions. Because after all data is not "oil" its about people...

As a way of finding a commonality between the various areas privacy professionals have to work with, he suggested that data classification was a common activity to support.

PI-Exit – it's about people, people

Malcolm Crompton, Managing Director of Information Integrity Solutions, was up next with an energetic and challenging presentation on how we should treating personal information as an asset, and deal with the new world order of data driven technology with big data on a big scale and AI as the new buzzword.

His theme was that privacy should be more than just compliance. He suggested that the regulatory approach of imposing penalties (which underlies the GDPR) will take us backwards making us lazy and just simplifies the conversation. Organisations should be including personal information on the balance sheets and treating it accordingly, finding ways to value it. He identified areas for improvement including consent based collection which he said is grossly overused, plus limitation of collection and purposing (use), suggesting we should adopt an ethical framework and develop trustworthy permission structures.

Effective de-identification

Dr Khaled El Emam, Founder of Privacy Analytics was our afternoon presenter. He talked about thinking about re-identification risk through a risk management framework and considering the interaction between data risk and context risk.

Data risk can be managed through removing identifiers (but decreasing the utility of the data set) and context risk can be adjusted through mechanisms such as contractual controls and security controls. If context risk can be addressed, then there is less need to address data risk. He also discussed an ethics framework for managing 'creepy' analytics (analytics that lead to creepy inferences regardless of whether an individual can be re-identified). Measuring risk can be done by commissioning motivated intruder tests

Finally he made it clear that pseudonymous data is not de-identified.

GDPR readiness (RAT)

Polly Ralph, Senior Manager, Cyber Security & Data Protection at PwC, then gave what was a somewhat alarming insight into organisations’ readiness for the EU GDPR. She discussed the results of PwC’s GDPR ‘RAT’ (readiness assessment tool). The RAT revealed that many organisations are not ready for GDPR (although they still have until 2018 to be ready). Polly expressed an interesting view that, with consumers' increased ability to bring class actions, GDPR may be more of a litigation problem than a regulatory enforcement problem for organisations. This is because regulators look for what an organisation is doing positively for compliance, whilst the search for gaps in compliance becomes the focus is litigation is commenced. Organisations need to be ready for both types of problem.
JOINT SESSION: GLOBAL PRIVACY PROGRAMS IN AUSTRALIA & NEW ZEALAND

Two impressive and leading female privacy professionals, Jacqueline Peace, Lead of Global Privacy Function at Air New Zealand, and Greer Harris, Digital Trust and Privacy Lead at SAP Australia & New Zealand, treated us to a joint session on global privacy programs. They discussed their perspectives and insights on running a global privacy program from Australia and New Zealand. In particular, they discussed how to get ‘buy-in’ of the C-Suite for privacy on a global scale. This focused on the value proposition of trust and marrying privacy to the core values of the business, rather than looking at privacy as a pure compliance issue.

Keynote speaker Q&A The final session was the keynote speakers (Simon, Malcolm, Polly and Khaled) in a Q&A debate and discussion.

Wrap up and AGM

The Summit was closed by the iappANZ Co-Vice Presidents, Melanie Marks and Anna Kuperman after which a good crowd stayed on for the cocktail reception and the AGM was very well attended and supported. The Summit was a great way to wrap up 2016 and the Summit Committee should be congratulated for putting together such a great line up of speakers and topics.

Presentation material and audio is available for download in the members area of the iappANZ website.
SOCIAL LICENSE AND PRAGMATIC TOOLS: HOW TO UNLOCK PUBLIC DATA
BY ANNA JOHNSTON

So November has been quite the month for discussing big ideas about Big Data. Between the iappANZ ‘Trust in Privacy’ Summit, the Privacy Commissioner’s De-identification Workshop, and the Productivity Commission’s draft report into Data Availability and Use, much has been said about public trust or ‘social licence’ as a pre-condition to effective data use.

(And that was before we even got to the two damming reports into #Censusfail released last week, from the Senate Economics References Committee and Cybersecurity Special Advisor to the PM Alastair MacGibbon.)

But how do you create the right conditions for better data-sharing?

I believe that if you want to facilitate data-sharing for the public good, you need two conditions:

- First, you need data custodians to feel they are on solid legal ground when they decide to release data; and
- Second, you need public trust.

I was asked to appear before the Productivity Commission earlier this week, to discuss some of their draft recommendations on this topic. With the objective of releasing the public value in datasets held by both government and the private sector, the Productivity Commission has recommended creating a new regulated category of data, to be known as ‘customer data’. Although I disagree with that particular recommendation – as outlined in the Salinger Privacy submission I believe the scope of the definition of ‘personal information’ is already sufficient – I nonetheless enjoyed a spirited debate on the issue with Chairman Peter Harris AO.

Mr. Harris said that the reason he wanted to move away from the definition of ‘personal information’ and instead talk about ‘customer data’ is because he wants businesses to treat their data as an asset, instead of as a ‘privacy compliance issue’. (There followed a brief period of furious agreement between us that privacy policies are generally well-crafted yawn-fests which consumers ignore.)

Mr. Harris also believes that consumers should be able to realise the value of their own data.

Personally, I think discussions on assets and the valuing of data tends to spill over into debate about who ‘owns’ data, which just muddles the waters. Privacy laws are deliberately drafted to be agnostic on the question of the ownership of data.

However coincidentally at the iappANZ Summit just a few days earlier, Malcolm Crompton had also raised the concept of data being classed an asset – although he was coming from quite a different angle. Malcolm’s point was that assets not on the balance sheet are usually ignored by company directors, so that by bringing personal information onto the balance sheet (for example through a change in accounting standards), you could potentially have more of an impact on ensuring privacy protection than strengthening our existing principles-based privacy laws.

In a similar vein, the brilliant information security blogger Bruce Schneier had this to say earlier this year, after yet another damaging data breach revelation: “data is a toxic asset and saving it is dangerous”.

So I came away unconvincing that we need a new, regulated class of ‘customer data’. If a business doesn’t yet understand that the information they hold about their customers is potentially both an asset and a liability, and it is therefore in their best interests to get their privacy practices right, calling it something new is not going to help.

But on the subject of language, I admit to being a fan of the term ‘data custodian’. The Productivity Commission’s draft recommendation 5.4 is to impose annual reporting obligations on data custodians, to make them justify their decisions about data access requests. Hmm, I’m not convince don that one. I made a submission that if the objective is, as the Productivity Commission says, to “streamline approval processes for data access”, then what data custodians need instead is pragmatic assistance.
My view is that the ideal privacy law sets tough standards that are nonetheless easy to comply with.

My experience over many years working with clients trying to comply with privacy laws is that the wording or ‘toughness’ of the rules themselves is almost irrelevant to the individual who needs to apply them. What matters to that decision-maker is how quickly and easily the standards can be found, understood, and followed.

For example, put yourself in the shoes of Phil the physiotherapist, or Sue the Centrelink manager, or Shari who is rostered on the front counter at a business. An insurance company investigating a personal injury claim has asked to see their file on Joe Bloggs. Phil and Sue and Shari don’t know whether they’re allowed to hand it over.

Their first thought is:

“Am I allowed to disclose this information?”

And likewise, the custodian of datasets of public value wants to know: “Can I lawfully disclose this information, in this format, in these circumstances, to this person or body requesting it?”

To answer any one of these questions can often involve a painstaking task of navigating through privacy principles, and exemptions, and applying the case law. It’s a lot easier to just say “no”, and “because of the Privacy Act”. Privacy gets a bad name. Research projects get bogged down. People start demanding exemptions from privacy law.

Instead, I would like to see the process of navigation made much simpler. The rules can be tough, so long as they are easy to find, understand and apply.

Earlier this year we developed a tool for organisations regulated under NSW privacy laws, which includes not only State and local government agencies, but also private sector organisations operating in NSW if they hold ‘health information’. We mapped out the Disclosure rules under the two NSW privacy statutes into a flowchart based, question-and-answer format, to guide decision-making. Because of all the different exemptions and special rules for different types of personal information, the flowcharts in our Untangling Privacy guide run over seven pages – but the user can move through them quickly.

Untangling Privacy works together with our annotated guide to the NSW privacy laws, PIPPA in Practice, which explains the interpretation on offer from both the Privacy Commissioner and case law (updated quarterly) about what each part of each test of each rule means in practice.

But although they come as downloadable eBooks, our guides are effectively still in analogue form. We would love to have the time and funding to turn our two guides into a properly automated and digital tool: an ‘app’ so that all types of data custodians, both big and small, could very quickly navigate through to the correct rule for their situation, and could also click through to see up-to-date interpretation of that rule. This type of pragmatic tool would enable data custodians to really quickly figure out their answer, each time they are approached with a request to share or disclose the data that they hold.

In an ideal world, the app would also be made available to the public for free. There would be no more hiding behind “because of the Privacy Act”. I suggested to the Productivity Commission that this type of app would also help consumers exercise control over their data, because they could more easily understand what the privacy laws actually allow for.

So instead of creating yet more legal and reporting obligations on data custodians, let’s build them pragmatic tools. (Venture capitalists / Treasury officials / Philanthropists / Google : you know where to find me!)

But how about the second half of the equation needed to facilitate greater data-sharing?

I suggest that to gain the kind of public or consumer trust necessary to allow for more data-sharing, you have to make every effort to ensure that every possible step is taken to prevent things going wrong ... but also that people will be protected in the event that something does go wrong.

Prevention of data breaches requires better education of both data custodians and policy-makers. Alastair MacGibbon, in his recent review of the Census, recommended that there should be a ‘Cyber Bootcamp’ for Ministers and senior public servants. What a brilliant idea! I would love to see a ‘Privacy Bootcamp’ as well. (Mr Harris raised only a bemused eyebrow at this suggestion of mine.)

But while prevention is better than the cure, we need to ensure there are cures as well. Our system of statutory privacy principles is not enough. There are many privacy breaches which cause individuals harm, for which they currently cannot seek a remedy.

So I argued that if you want to promote greater data-sharing, you will need to convince the public that their privacy is going to be protected – or that if all else fails, they will be compensated for any significant harm that they suffer. In my view, that means that the Government should take greater steps to offer remedies for people who suffer serious privacy harm, in parallel with any steps to increase the level of risk posed to individuals from greater data-sharing.

The Australian Government currently has two privacy-related Bills before Parliament, one of which is the data breach notification bill, and the other is a proposal to criminalise the re-identification of ‘de-identified’ government datasets. However neither of those Bills will actually provide remedies for victims of privacy invasions.

I suggest that if the Government is serious about unlocking the public value in data, it should not proceed with legislation or projects to increase the amount of data-sharing without first engendering public trust, or gaining a ‘social licence’. At the least, we need legislation to create a statutory tort of privacy, as already recommended by the Australian Law Reform Commission and other inquiries.
I don’t think we need new names for personal information, or new accounting standards for data. But if we want to promote data-sharing in the public interest, while at the same time protecting privacy, we need to offer pragmatic assistance to data custodians, and better legal protections to consumers.

Anna Johnston
Director, Salinger Privacy

Salinger Privacy provides specialist privacy consulting and training services, and publishes eBooks on privacy law. Find us, read our blog or sign up for our newsletter at www.salingerprivacy.com.au
GDPR: A MIDDLE GROUND TO THE
DE-IDENTIFICATION DEBATE?
BY HELEN LAUDER

The last edition of Privacy Unbound highlighted that de-identification has been a ‘hot topic’ for privacy in 2016. This theme continued at the iappANZ Privacy Summit in November where Dr Khaled El Emam presented a better way to think about re-identification risk through a risk management framework considering the interaction between data risk and context risk.

What are the issues?

Issues associated with de-identification include:

- what it means to properly de-identify information (if this is even possible);
- what is an acceptable level of risk when determining whether information can be re-identified; and
- how do we balance the value to society of data analytics against the protections of individual's privacy, there is a corresponding loss in the utility of the dataset (and vice versa). The importance of data sets (and their underutilisation in Australia) was recently highlighted in the Productivity's Commission's Draft Report on Data Availability and Use.

**GDPR - a new approach through pseudonymisation**

The EU General Data Protection Regulation (which comes into force in May 2018) (GDPR) includes a new approach that could be considered as a middle ground in the de-identification debate between protection of individuals and retention of useful datasets. It does this through expressly encouraging pseudonymisation. This development is relevant to Australian entities, not only as a potential way to rethink our approach to privacy law in the future, but also because of the extended extra-territorial operation of the GDPR. In particular, the GDPR will capture the processing of personal data of individuals in the EU by entities not established in the EU where the processing activities are related to:

1. The offering of goods or services to such individuals in the EU (irrespective of whether payment is required); or
2. The monitoring of their behaviour as far as their behaviour takes place within the EU.

The GDPR will apply to 'personal data', which is any information relating to an identified or identifiable (directly or indirectly) natural person. It does not apply to personal data rendered anonymous in such a manner that the data subject is no longer identifiable. The new middle ground is personal data which has undergone 'pseudonymisation', which means:

'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person'.

A reasonableness test is introduced through the recitals which provide that, in determining whether a person is identifiable, account should be taken of all the means reasonably likely to be used.

Personal data that has gone through the process of pseudonymisation is still 'personal data' regulated by the GDPR (assuming the individual is still reasonably identifiable, such as through additional information). This is similar to the position in Australia, where pseudonymous data is treated as personal information if the individual is reasonably identifiable. However, the GDPR appears to acknowledge that, provided the additional information that enables the attribution of the personal data to a specific individual is kept separate and secure, the risks associated with the pseudonymous data are likely to be lower and the legislative protections for this data can be relaxed.
The incentives to undertake pseudonymisation appear in the GDPR as follows:

1. It is a factor that can be used to justify processing for secondary purposes. Pseudonymisation is listed as an example of an 'appropriate safeguard'; the existence of which can be taken into account in determining whether processing for a new purpose is compatible with the purpose for which personal data was initially collected (and therefore a permitted new purpose).

2. It is a measure that can be used to satisfy the 'privacy by design' obligations. Pseudonymisation is provided as an example of 'appropriate technical and organisational measures ... designed to implement data-protection principles'. Such measures must be implemented both at the time of the determination of the means of processing and at the time of the processing itself.

3. It can be used as a measure to comply with security obligations. Pseudonymisation is included in the list of 'appropriate technical and organisational' measures that an organisation must implement (as appropriate) to ensure a level of security appropriate to the level risk associated with processing.

Whilst certainly not the solution that will end the de-identification debate, this legislative acknowledgment may provide at least a useful starting point at finding a middle ground. It encourages a mechanism that reduces the risk to individuals associated with data processing, whilst also allowing organisations to retain a data's utility.

In contrast, pseudonymisation is only considered in the Privacy Act 1988 (Cth) in APP 2 which requires that individuals have the option of using a pseudonym (subject to exceptions). This requires the individual to make a conscious decision to use a pseudonym. Experience shows that requiring action to be taken by individuals is not necessarily the most effective way to reduce privacy risk. Tying this specific privacy enhancing measure to express compliance incentives as in the GDPR may be a more effective approach. Time will tell whether this approach leads to an effective balance between protecting individuals and the benefits of data analytics, or merely add to compliance confusion.