It almost feels like spring, and there is certainly a lot of light and life in your iappANZ right now. Every day there is something happening in your Association. This week we are putting the final touches to our new website and Annual Privacy Summit line up. The Global Knowledge Networks for Sydney, Melbourne, Brisbane and Adelaide are shaping up with an event in Melbourne organised for this month. We are also going to send you a Survey soon to see what kinds of events you would find most valuable.

As a member organisation, our priority is to provide value to you. We think this journal does that with a wide range of topics and perspectives and of course updates from our regulators in Australia and New Zealand. But we are open to your suggestions. We would love to hear your views - perhaps counterpoints to pieces in this Journal? We would be delighted to publish these as Letters to the Editor, so don’t hesitate to email our Editors Veronica Scott and Carolyn Lidgerwood to have your say (see details on page 26).

I was in the UK recently and had the good fortune to meet with one of our Keynote Speakers, Stephen Deadman, the Global Chief Privacy officer from Vodafone. Just as you enjoyed Mikko Niva last year, I am sure you will find Stephen to be a thought provoking and sparkling presenter who will discuss the business of privacy and all of its challenges and opportunities in November. Take a look inside to find out more about this year’s Summit, which has been perfectly named by our Vice president Anna Kuperman, Privacy@Play.

Over the last few months we have been profiling our marvellous Board members. This month take a look at the profiles for two of the longest serving Directors, Melina and David. Every Director has put in a great deal of effort over the year, and the results are a much larger and more vibrant organisation. Our membership has doubled and of course we are very lucky to have retained and grown our sponsors who are all major players in the privacy game. We have put on over 12 events to date, with more on the way. As volunteers we clearly have to love the work to do it, but there is always room for more of you to join our Board. Whilst there is work to be done, you couldn’t meet a better bunch to roll up your sleeves with. Let me know if you are interested, or if you would like to dip your toe in the water and join one of our Sub Committees in the meantime. We would welcome you warmly.

Enjoy the last of winter with this July Edition of Privacy Unbound.

Warm regards
Emma Hossack, President
Vice President’s Foreword

By Anna Kuperman
Vice President
M: 0419 803 263

This month we have another series of thought provoking pieces from our expert contributors. We start with a perfectly titled article by our President, Emma Hossack (‘Lost in Translation, Privacy Perceptions and Software Development’) on the dynamics between technology and privacy principles. Many of us counselling our information security friends within organisations can role play the language divide in our sleep, both conceptually and practically. Emma has succinctly captured the ins and outs of getting to the right conversation. Board Director, Peter Leonard provides very useful insight on considering a values-based governance framework for big data analytics and maximising the value of data in a transparent and ethically compliant manner. Turning from governance principles to practical data handling, Peter then looks at the recent OAIC investigation into the data breach by Pound Medical Centre.

We are grateful to be able to publish a key note speech given by New Zealand Commissioner, Mr John Edwards at Nethui in Auckland on the right to be forgotten and the ongoing debates regarding freedom of the internet versus regulation. And turning to the regulatory front closer to home, our editor Carolyn Lidgerwood discusses the Privacy by Design approach adopted by Privacy Victoria, becoming the first Australian privacy office to explicitly do so. David Watts, Acting Victorian Privacy Commissioner, has explained that the approach provides a framework to address the ever-growing and systemic effects of information and technologies and large-scale networked data systems.

Many thanks to Samantha Yorke for agreeing to chair the NSW Global Knowledge Net. You will see the depth of expertise and industry know-how, Sam brings to iappANZ in this newly created role in her profile. Watch out for opportunities to network and engage with your privacy peers in your State! We have a Privacy After Hours networking opportunity in Victoria (look at the back of the events calendar for further details). Former iappANZ Board Director and Treasurer and now Deputy Victorian Privacy Commissioner, Helen Lewin will be attending! So take this opportunity to meet other iappANZ members in your State.

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

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

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

Our LinkedIn group is:
http://www.linkedin.com/groups?gid=1128247&trk=anetsrch_name&goback=.gdr_1281574752237_3

Follow us on Twitter at: https://twitter.com/iappANZ
Introducing your iappANZ Board for 2014

Each month during 2014, we have been introducing some of our iappANZ Board Directors. Here is the lucky last instalment – meet Melina Rohan and David Templeton!

Melina Rohan

Melina Rohan joined the iappANZ at its inaugural conference in 2008. Since then she has been on the IAPPANZ board for a number of years and attended every iappANZ Privacy Summit.

That's the definition of an iappANZ stalwart!

Melina’s privacy and policy career has spanned three different industries over a number of years including telecommunications, marketing and the digital arena.

Melina was invited to become the inaugural Director of Policy of the Australian Interactive Media Industry Association’s Digital Policy Group in 2012. The AIMIA Digital Policy Group is a special interest group of AIMIA that represents 460 digital players in the Australia digital industry. The Digital Policy Group represents large and small, local and global players that provide digital content services, applications and platforms. The Digital Policy Group’s policy interests include cyber-safety, cyber-security, national security, content standards, copyright, privacy, e-commerce and governance.

Prior to being appointed Director of Policy for the AIMIA Digital Policy Group, Melina was Director of Corporate and Regulatory Affairs for the Australian Direct Marketing Association (now known as the association for data driven marketing and advertising).

In this role Melina provided compliance and policy assistance for a broad range of firms including the over 500 member organisations including major financial institutions, telecommunications companies, energy providers, media, marketing agencies, travel service companies, major charities, statutory corporations, educational institutions and specialist suppliers of direct marketing services. Melina’s policy responsibilities included but were not limited to Australian Consumer Law, the Privacy Act, Do Not Call Register and Spam legislation. Melina also provided secretariat support to the long standing ADMA Code Authority that oversees the handling of consumer inquiries, information requests and complaints. This function included assisting consumers to understand how they can control the marketing they receive as well as general privacy and consumer rights education.

That's a lot of privacy experience – but wait … there’s more!

Before ADMA, Melina was a Senior Regulatory Analyst at Optus having responsibilities for the development of inter-operator codes of conduct that facilitated the de-regulation of the telecommunications industry including Pre-selection Code, Local Number Portability and Mobile Number Portability. This role also extended to policy and compliance responsibilities in relation to privacy, management of Optus’ telephone listings and the Integrated Public Number Database (a database of telecommunications customers on which emergency services and law enforcement professionals rely for responding to ‘000’ calls).

Melina is happily married, a proud mother of one lovely little girl as well as a keen gardener and swimmer!

Melina holds a Bachelor of Economics from Macquarie University and a Masters of Business Administration from the Australian Graduate School of Management.
David Templeton

David Templeton is iappANZ’s dedicated and modest Secretary of the Board. We say modest because unlike the rest of us on the Board, David hates talking about himself, and your journal editors have found the task of extracting personal information from David to be like drawing teeth.

So to quote Warren and Brandeis (in their seminal 1890 work, The Right to Privacy), we have not exactly granted David the ‘right to be let alone’ (incongruous behavior from a peak body for privacy professionals!)

David Templeton is a financial services lawyer by background commencing his career in 1989 with Middletons in Melbourne before joining the Commonwealth Bank’s in house legal department and later, ANZ’s Legal Group.

David joined ANZ Bank’s Group Regulatory Compliance team in January 2006, where he developed a specialist interest in privacy and offshoring. David advised ANZ in relation to the ALRC’s review of privacy regulation and represented ANZ at APEC’s workshops on Cross Border Privacy Rules during 2007.

ANZ recognised David as a subject matter expert in privacy and nominated David as its Privacy Compliance Manager in early 2008. In that role, David's mandate was to ensure that privacy obligations are effectively integrated into ANZ’s compliance framework though the development and administration of a global privacy policy.

In 2010, David assumed a senior managerial role in ANZ’s Australia Division with responsibilities that include management of retail customer information and business enablement. David has maintained his interest in Privacy.

David joined the iappANZ Board as a founding member in 2008 and was appointed Secretary in 2009. A Board could not ask for a better Secretary!

David lives in Melbourne with partner Adele and son Hugo.

David holds bachelor degrees in law and science from the University of Melbourne.
Lost in Translation:
Privacy Perceptions and Software Development

by Emma Hossack

Privacy is increasingly becoming a part of mainstream commentary and contemporary debate due in no small part to sensationalised press commentary by publications such as News of the World or breaches on the scale of the one by Target. However there are other reasons for business to sit up and take notice of privacy.

Technology is being used to enable greater efficiency in the digital economy. We are increasingly moving online to connect, deliver and access services meaning that the ‘digitally connected business world is virtually here’. A recent report from the CSIRO identifies a number of global trends, what it called ‘megatrends’. Megatrends, as defined by the CSIRO, are significant global shifts in environmental, economic and social conditions that will play out over the coming decades.

Underpinning these trends is the need for people to trust new ways of connecting and accessing services. Because privacy can get lost in translation between the various layers of an organisation, be they commercial, compliance, technical or marketing, it is often misunderstood. Consequently privacy is often relegated to compliance for the legal and IT departments. And this is where I believe organisations miss the point and the value of privacy. Unless there is confidence by the users that their privacy will be observed, business opportunities will be lost or their full potential never realised.

As President of the iappANZ over the last 18 months, I have had the privilege and stimulation of being immersed in privacy news feeds, becoming familiar with many privacy practitioners, iappANZ sponsors and engaging with privacy regulators in both Australia and New Zealand.

I have also been met with the shocking realisation that too many of my ‘non-privacy’ business colleagues consider privacy to be boring and simply about compliance. Privacy is a much maligned concept and under-rated practice. This needs to change and the challenge of expressing privacy as a business enabler and, importantly for the ‘C’ suite, as a revenue and profit generator with all its fascinating nuances is up to us as privacy professionals. Of course your association, iappANZ, would love to hear more of your ideas on this topic.

In the meantime, this article is intended to help that conversation.

Firstly it’s useful to look at some of the current approaches to privacy which are gaining global traction. With the explosion of data, it’s worth keeping up with where ‘privacy thinking’ is going. Having some of this up your sleeve is useful armoury when you are told ‘privacy is boring’.

Then I want to provide you with a practical example taken from my own software house, which illustrates how approaches to privacy can influence product development, corporate culture and possibly the bottom line.

Some current privacy thinking

The Privacy Act came into law the year after I left Law School, and I was told not to worry about it as it was a bunch of human rights issues, soft law which would never impact on my legal practice. At that time, 70% of the listed assets of Fortune 500 companies were tangible. Now companies like Facebook with market value over $190 billion, and worth more than Coca-Cola, have less than 10 percent of their listed assets in the tangible sphere. According to Kenneth Cukier and Viktor – Mayer Schoenberger, data is the new oil - and data controllers depend on trust of its providers to keep the data flowing.

Privacy isn’t defined in the Privacy Act for a very good reason. It is a contextual concept, something which eludes finite description and thus has resulted in the terminology throughout the Australian Privacy Principles of ‘reasonable steps’. Daniel Solove says most definitions fall short – privacy is elusive, the right to be let alone, a basic human right, the right to live free from interference, to act without surveillance or ‘dataveillance’. Or a combination of secrecy, anonymity and solitude according to Ruth Gavison. Whatever it is, it is near impossible to grasp the concept unless it is linked with a high regard for autonomy, without which its relevance disappears. Autonomy is essentially about the ability to control ourselves and personal information, so privacy in this sense is then, according to Professor Fred Cate, ‘not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves’.

At no time has this been more relevant than now, in a digital economy, where the Australian Privacy Principles and other regimes may try, but will not always cure, the practical difficulty of securing vast amounts of personal information securely.

Current debates about the collection and use of data, circling around consent have also reached the headlines. Google and Facebook have raised the profile of privacy, and phrases like ‘the right to be forgotten’, are now in the headlines and a part of public consciousness.

1. ‘Big Data - a Revolution that will transform how we live, work and play’
4. Fred Cate ‘Privacy’ (1968) 77 Yale LJ 475,482

---

2. Our Future World CSIRO Futures www.csiro.au/futures

---

---
On account of the imbalance of power between parties who hold the data, those who provide it and those who want it, as well as the complexity and length of consent notices, there are good arguments that there should be a shift of responsibility to the larger entities seeking the data. Another compelling view in my opinion, is the consideration of intellectual property as a means of privacy protection. Rio Tinto CEO Sam Walsh has called data, ‘the mine of the future’. So what about treating data as something with a value which can be used in transactions like other intangible property?

This theory was explored by Samuelson in the United States over 10 years ago on the basis that individuals have an unfounded sense of ownership over personal, health or financial data – unfounded because individuals do not have a legally recognised right of ownership. Consequently, if we were to create a right of privacy as ‘ownership over personal information’, then this would enable companies the freedom to negotiate with individuals for the use of their data which would result in more meaningful collection. On this basis, individuals would provide exactly what data they are happy to part with for consideration – even if it is simply the knowledge they are helping research into incurable diseases – and on that basis, the personal information provided may be more accurate and candid. There could also be less wholesale trawling for personal data on the Internet which could save businesses money. Personal information could be protected as a valuable commodity in the digital economy.

This idea has been picked up recently by research in UK by Ctrl+Shift which claims that the Personal Information Management Systems (PIMS) market is worth in excess of £6B per annum.

You can see the PIMS infographic (to the right) at: https://www.ctrl-shift.co.uk/news/2014/07/30/pims-infographic/.

---

6 Particularly in respect of Big Data – the imbalance of power is highlighted.
7 Microsoft Whitepaper on Notice and Consent 2012.
Another argument for the market-based approach to personal information disclosure rests in the costs saved on regulation, as the market would then regulate the protection of property rights. Perhaps a step too far towards the market based approach for Australia; but the transaction based model with additional protections could have merits.
9 Alessandro Acquits at the iappANZ 2012 Summit.
PIMS are essentially tools and services which enable individuals to use information to get ‘stuff done and manage their lives better’.

Ultimately the aim is to provide more useful real time information sharing between organisations and individuals. PIMS allow individuals control over their own data and make them the point of integration of data about themselves. PIMS make people specify their wants and needs and also make these preferences available in the marketplace. As a result of PIMS, there are richer insights into products, customer content is more efficient and risk and compliance costs can be reduced by enabling permissioned, trust-based data sharing.

With this proposed consumer empowerment or autonomy comes the debate. Every commercial arrangement is adversarial, buyers wanting it for less and sellers wanting to charge more. But sometimes a development transcends this. Like Henry Ford’s system of mass production which not only gave consumers better cheaper products, but also made Ford richer through volume of sales. Now with a personal information economy, PIMS offers a similar breakthrough with voluntary personal information sharing. Individuals can choose with whom they share, the costs are reduced and privacy incursions limited.

As with all new trends there may well be a few false starts. We saw it at the start of the IT revolution in the 70s and 80s where we heard of the IT productivity paradox, as Nobel laureate Robert Solow said ‘You can see the computer age everywhere except in the productivity figures’. One of the reasons for this was that the productivity was being measured using old metrics. Conceptually productivity needs inputs and outputs. Convenience and access however, are less easy to measure. So for example the installation of ATMs was initially deemed a productivity failure by those who failed to measure the enhanced consumer convenience. Some large corporations have realised new metrics are required in respect of privacy, but most organisations have not. And you don’t get what you don’t measure.

**A Business case for the Privacy by Design of Edocx**

Disorganisation militates against privacy and people’s right to have any control over information about themselves.

The Ponemon Institute’s recent survey figures found that 59% of businesses are ineffective at managing access to personal information, 29% of employees accessed very sensitive information very frequently, which is 40% more likely to result in the loss or theft of confidential documents. Furthermore, 35% of employees attach and send confidential documents using personal email, which is 40% more likely to result in the loss or theft of confidential documents.

So, how to get organised? Listening to client concerns, my business decided to build an information logistics platform that would also provide modular storage so that clients could host their data in their own data centres or choose Amazon in Sydney or Polaris in Brisbane.

This project taught our team many things. One of those things was that it illustrated that Privacy by Design can mean different things to people from different disciplines.

**Tensions between the architects, the lawyers, the business heads and client requirements**

Everyone has a different perspective. And I think the tensions between the groups are valuable as they ensure we all stake our place and argue it out. The tensions between the groups at my company may well be every company in microcosm.

Our lawyers look at the risks and privacy principles, indemnities and breaches, what is reasonable and how we should protect our business.

The software architects don’t understand what they are saying. Not because they aren’t super intelligent - one of our University Medallists is called ‘the twins’ as it is said he thinks so fast he has to have 2 brains. These guys just think differently and use very literal language.

Then there are the business heads who can’t see the benefit of a deluxe software approach and are concerned with scope creep and the timelines of getting a product out to the market.

The management of expectations of all these groups is crucial. We must be privacy compliant and enhancing, whilst managing the cost and the functionality. And that is before you get to the user experience – what do they need to accomplish, how experienced are they, what interfaces are they familiar with? What attributes are needed if the data collected need special privacy rules? What does reasonable steps mean? Where is the ‘reasonable steps’ button on the keyboard? Everything must be able to be classified and put into a column in a database, so terms like ‘best endeavours’ and ‘reasonable’ are just not precise enough.

Building a software product over 5 platforms, and answering all of this up front is like asking the defence lawyer to guarantee up front how long and how much for the trial of Lindy Chamberlain – there are many twists and turns. It is not simply coding a policy – it is workflow, legal, ‘UX’ or user experience and innovations along the way to keep ahead of the competition. Falling foul of the expectations either side can be fatal.

Unlike Ian Oliver, the CPO for Here who I read in the iapp Dashboard, I don’t think we need a *lingua franca* for lawyers and developers. We think differently and we talk differently. I am never going to be able to code Java, and they are never going to be able to usefully interpret and apply laws. We don’t want to and it’s not our talent. We borrow from the mining industry and have adopted a habit of starting every meeting with ‘privacy moments’ (the IT industry’s version of a ‘safety share’).

So instead of them straining to teach me the multi layered complex interactions of hundreds of components that make up encryption, and me trying to explain the history and totally illogical direction that the law sometimes takes, we have made a pact to respect each other’s expertise, talk about what we need to achieve and make sure that if it’s within the bounds of possibility, we just do it.

---

11 iapp Daily Dashboard 30 June 2014
12 Originally dreaded, and now enjoyed.
There are many aspects to this design of a privacy compliant system, and if it is something you or your clients are doing, you should look at The Privacy Engineers Manifesto – getting from policy to code to QA to Value by Michelle Dennedy. And just to counter the argument that lawyers always stifle innovation, take a look at a paper called The risk based approach to privacy – improving effectiveness in practice which was recently released by Hunton Williams Lawyers though the Centre for information Policy Leadership.

It takes many good deeds to build a reputation and only one bad one to lose it. If data is the mine of the future, then privacy is the way to capitalise on and the value buried within the global megatrends. Confidence and trust are essential – whether looking at a business proposition (such as the information logistics platform I’ve just described), or whether you are looking at how you will share your own personal data (perhaps trading it for consideration, as in the examples given earlier).

You must treat data like the most valuable asset on your company’s balance sheet or in your own private bank account because if it isn’t now, you may be missing something.

Next month, Emma will provide further insights and practical examples about ‘privacy by design’ in software development, and the complex decisions that can involve.

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

www.extensia.com.au
www.edocx.com.au
www.iappanz.org

13 Download it free as an e-book
14 http://www.informationpolicycentre.com/Privacy_Risk_Framework/
15 Benjamin Franklin
Big News on Big Data

by Peter Leonard

A key role for privacy regulators is provision of guidance about how to apply privacy principles to design appropriate privacy settings and options into new business applications. Although national privacy laws differ greatly, regulatory guidance is frequently relevant and useful across multiple jurisdictions and different legislative schemes. For this reason many privacy professionals maintain a stash of copies of discussion papers and reports from privacy regulators around the globe. Privacy professionals advising as to big data applications are spoilt for choice: a flood of reports and analyses spills out from regulators and policy makers on different continents. Volume of available material always exceeds reading time, so selectivity is key.

One regulator that usually has interesting insights is the United Kingdom Information Commissioner’s Office. The UK ICO was an early voice of reason in the anonymisation debate, in particular with release of its November 2012 Anonymisation Code of Practice. The UK ICO recently returned to the topic, publishing in late July 2014 a discussion paper entitled ‘Big Data and data protection.’ The paper is a thoughtful and balanced analysis of good privacy practice applied to business applications of big data derived from personal information. Much of its length (50) is devoted to discussion of Eurocentric issues, including when an organisation is a ‘data processor’ under when processing is ‘fair’ under the EU Directive and its national implementation in the UK Data Protection Act 1998. But this should not obscure the relevance of most of the discussion in the paper in Australia, New Zealand and other APEC countries.

As the Information Commissioner notes in the paper, many applications of big data do not require use of personal data. However, a number of important applications may in some cases, including use of personally identifying data from monitoring devices on patients in clinical trials, mobile phone location data, data on purchases made with loyalty cards and biometric data from body-worn devices. There are also sometimes concerns expressed about what is sometimes called the ‘segment of one’ marketing: fine tuning the offer of products of services to an individual based on their characteristics such as age, preferences, lifestyle etc. Findings derived from big data analytics can be applied to marketing to individuals (e.g. ‘people with these characteristics tend to want these products or services at this time’).

Many big data applications are based upon anonymisation of personal information before analytics is conducted. The academic literature continues to grow around studies that demonstrate cases where anonymisation is not effective to prevent the risk of re-identification of individuals. Examples that have recently gained significant media interest include the uniqueness of our patterns of movements being used to re-identify individuals from anonymised individual level mobile phone data and the uniqueness of our gait being used to identify individuals from their ‘Fitbit’ data stream. The Information Commissioner engages with this literature and with the frequent assertion that privacy regulation can’t keep up with data analytics. As the Commissioner puts it, ‘We do not accept the argument that data protection principles are not fit for purpose in the context of big data. Big data is not a game that is played by different rules. There is some flexibility inherent in the data protection principles. They should not be seen as a barrier to progress, but as the framework to promote privacy rights and as a stimulus to developing innovative approaches to informing and engaging the public.’

The Commissioner returns to the core thesis of the 2012 Anonymisation Code of Practice: namely, that although it may not be possible to establish with absolute certainty that an individual cannot be identified from a particular dataset in combination with other data that may exist elsewhere, ‘The issue is not about eliminating the risk of re-identification altogether, but whether it can be mitigated so it is no longer significant. Organisations should focus on mitigating the risks to the point where the chance of reidentification is extremely remote.’ In mitigation that risk, anonymisation will often be key. Anonymisation may be used when data is shared externally or within an organisation. ‘For example, an organisation may hold a dataset containing personal data in one data store, and produce an anonymised version of it to be used for analytics in a separate area. Whether it remains personal data will depend on whether the anonymisation ‘keys’ and other relevant data that enable identification are retained by the organisation.’

In this brave new world, organisational dynamics affecting data governance will increasingly be the determinant to whether big data may be ethically handled, as well as in compliance with laws. The Commissioner refers to a Boston Consulting Group paper that argues that the potential gains from using big data are so great that the management of personal data (including issues of how data is collected, consent, purposes and security) is a ‘c-suite’ issue: that is, an issue that should be addressed at chief officer level within an organisation. ‘This positioning of personal data issues means that there is a convergence between the data management agenda and the data protection and privacy agenda.’

So what should data analytics providers do?
First, put in place an appropriate values-based framework and rigorous governance arrangements to effectively identify and appropriately quarantine uses of personal information from any anonymisation-based data analytics.

Second, ensure transparency of practices and fairness of disclosures by educating people as citizens and as consumers. ‘This means explaining the benefits of the analytics, in terms of improved services, more relevant marketing or enhanced rewards, and looking to foster a value exchange, in which people are happy to provide data if they are informed and have trust in how it will be used.’ Providers should not place undue reliance upon formalistic or complex privacy statements or notices, which may not be read or understood by consumers and therefore don’t foster trust and may also be legally ineffective because they are insufficiently ‘transparent’.

Third, consider use of intermediaries, including trust certification third parties or others that can assist is demonstrating that anonymisation and other risk mitigation implemented by a corporation is embedded and systemic and demonstrably reliable.

Fourth, be particularly careful in any repurposing of personal information. If an organisation has collected personal data for one purpose and then decides to start analysing it for completely different purposes (or to make it available for others to do so) then it needs to make its users aware of this. As the Commissioner notes, ‘This is particularly important if the organisation is planning to use the data for a purpose that is not apparent to the individual because it is not obviously connected with their use of a service.

Fifth, don’t forgo minimisation of use of personal information. Although a key feature of big data is using ‘all’ the data, minimisation of use of personal information requires organisations to be clear from the outset as to what they expect to learn or be able to do by use of personal information, as well as satisfying themselves that the personal information is relevant its use not excessive, in relation to that aim.

The Commissioner’s paper is a good and timely read. From the reviewer’s experience, many early data analytics applications simply don’t effectively quarantine uses of personal information from uses of anonymised data. This was partly because many applications were developed in the United States of America for use in industry sectors that were not subject to significant privacy regulation and then then applied in jurisdictions such as Australia and New Zealand without appropriate localisation to accommodate economy wide privacy rules. Many alleged anonymisation practices fail through poor understanding of organisational dynamics and because legal form takes precedence over appropriate data governance. Many early applications of customer data analytics have been rudimentary in process design and frankly slipshod in project execution. From both better understanding of the issues and the ethical imperative, the position is now quickly changing. Good practitioners of big data analytics will increasingly be able to differentiate themselves from those sub-standard early movers.


See also the Commissioner’s blog, http://iconewsblog.wordpress.com/2014/07/28/seven-things-you-should-know-about-the-icos-big-data-report/

Peter Leonard is a partner at Gilbert + Tobin Lawyers working with data analytics applications and also a director of iappANZ.

Alasdair Wallace, You and all your friends, 2006
Exploring privacy over the next 25 years:
The right to be forgotten

by John Edwards, Privacy Commissioner of New Zealand*

This is an edited version of the keynote speech given by the Commissioner at Nethui in Auckland on 11 July 2014.

On May 13 of this year the European Court of Justice ruled that Google in Spain should break links to an old newspaper story about a debt of a plaintiff, Mr Gonzalez, because he’d paid the debt. The decision was based on European privacy law, and the principle behind it has been called ‘the right to be forgotten’.

I’m actually not a big fan of the term.

The decision was based on the Spanish legal requirement on the relevance of personal data; the right to be forgotten that has been under debate as part of the review of Europe’s 1995 Directive isn’t yet a part of EU law, though plans are afoot to make it so.

Also, a right to be forgotten means different things to different people. It can mean data portability, so that if you decide to leave (say) Facebook, you should be able to take your links and content with you, and have that deleted. Do we feel more comfortable with that formulation?

It could mean a right to anonymity, or to its cousin obscurity. And it can mean the removal of content from public search. In his typically prescient way Australia’s most famous jurist Sir Michael Kirby even proposed a right not to be indexed back in 1999.

The right to have people forget you.

But let’s take the phrase at face value for the moment. If we end up with this right, then who would it apply to? Well, everyone. If it’s a right then it doesn’t make sense if it only applies to a few people.

But that’s too passive. A right doesn’t mean much if you can’t enforce it; so, unless you can convince them you’re so boring you fade from their memory the moment you stop talking to them, what it actually means is:

The right to make people forget you

But again, we’re not talking about people with their fallible memories, are we? It’s the information systems, information machines that people have created, that are doing the heavy lifting, so:

The right to make machines forget you

Since the Spanish court case, Google in Europe have been receiving more than 10,000 requests a day that it forget about some kind of personal information, that it break links to information that is no longer relevant.
Why would you want the right to make machines forget you?

Privacy is all about helping people keep control over their own information in the face of technological innovations that lessen that control. And if every aspect of your life is being tracked by machines that never forget then more and more of your information is heading out of your control at every moment.

Security expert Bruce Schneier said, with reference to the internet-enabled world: ‘we are embarking on a great experiment of never forgetting.’

Eventually, nearly every aspect of our lives will be logged and searchable. Will we lose some of our ability to change as we grow, because we’ll be locked closer and closer to who we have been in the past? Some might say we’re already there with Facebook.

The conversation which has begun in Europe and which is gathering momentum around the world is a response to this increasingly ubiquitous hoarding and storing of personal information.

But it’s complicated because if you can make a machine forget about you, you can make it a lot harder for people to talk about you, which can be very attractive for the bad people of this world. The information you’d like to remove about yourself is sometimes the exact information that other people want to keep hold of and be able to access. Is this talk an affront to free speech? Surely free speech isn’t something we should give up without taking a very careful look at what the future might hold.

The Right to Be Forgotten – looking to the future

Harvard law professor Lawrence Lessig attempted to give us a tool to look into that future in his early 1990s book ‘Code (and other laws of cyberspace)’. Professor Lessig suggested there were four ways that people were regulated, four forces acting on the individual.

Market, mores, law, architecture

The example he used to explain these four terms was the bicycle. Imagine a meeting of serious people who want to accomplish the important goal of protecting bicycles. After an hour or two they settle on those four options: market, mores, law, and architecture.

1: They could subsidise bikes and make them cheap – this would make it not worth the thieves while to steal them. This is targeting the market, how buying and selling things reflects human behaviours.

2: They could try and change public opinion and make bike theft unacceptable by mounting a big advertising campaign with a catchy slogan - maybe go to Facebook and post ‘steal bikes, lose likes’. This is hitting the mores, the way people think as a group, social acceptance.

3: They could introduce a statutory mandatory life sentence for bike theft. This is the law part of the story – a formal and codified set of rules for society, mediated through designated bodies like courts and Parliament.

4: They can attach padlocks to every wall, making it as easy as possible to lock your bike up. This is using architecture, the structure of the world, to accomplish your goal.

But also remember that each of these affects the other – the law has to deal with the world as it is, the existing market forces, the way people think. The market is similarly constrained by mores, architecture and laws. And so on.

The big thing that Lessig realised, is that in an electronic world, architecture is fluid. It’s made of code so it can be re-written silently and seamlessly. When Google, say, wants to change the way it stores its email or to how it ties together its users, it changes its code. Code is mutable.
So let’s break it down and apply these four views to the Right to be Forgotten – but don’t forget when we use that term, we are incorporating the right to have information deleted, and the right to force a search engine to not link to other sites hosting information ...

How is the Market likely to support or hinder the right to be forgotten on the Internet?

Market and Mores

The strongest tension is probably from the Mores. Companies operating in the Market need to respond to the Mores, because if they don’t they go out of business. Competition demands responsiveness.

The recent alarm over Facebook’s mood alteration research is a good indicator of how quickly public opinion can react to a perceived misuse of user information.

We’re already seeing services like Snapchat make a virtue of how much information they don’t collect, how it is not available for search, self destructs after a limited time, and therefore does not need to be ‘forgotten’. If people can price their privacy in a way that makes sense, then the market will respond.

But also, don’t underestimate the capacity of those with the greatest to lose in the unregulated marketplace to attempt to influence the mores to better support their business model. ‘Privacy is over’ declared Zuckerberg in January 2010.

Market and Law

Market entities need to be legally compliant otherwise they get in trouble. There’s a long history of the law stepping in when one player becomes monopolistic and in those cases, the law usually wins.

However, there are lots of loopholes to discover along the way, as we have seen in the copyright area, where the market has been fighting the law for a couple of decades.

As the regulator in New Zealand, I have some options to address market issues, but hasty law is often bad law.

Market and Architecture

Architecture is in this context the least restrictive of the three forces because as Professor Lessig pointed out, code is architecture. So market entities that are working with code get to create their own architecture. And even when market entities try to lock down their code, it doesn’t last long; jailbreak apps are an architectural innovation, responding to a lack of individual control.

So it seems possible that if the idea of the right to be forgotten takes root then we may see a vigorous corporate defence of their right to have machines never ever forget about you by use of their architectural control of code as we’ve seen in the area of digital rights management.

However, I think, on balance, I’m optimistic about the market’s role in this.
Mores

It’s been a busy couple of years in privacy. WikiLeaks, the Edward Snowden revelations about the NSA, and a range of well-publicised data breaches have made privacy a household word. People are becoming more aware and concerned.

But there is also the chance that everyone will assume everything is known about them and give up, the ‘privacy is dead: get over it’ approach.

There’s no lack of concern at the growing power of big companies, Facebook, Google, Amazon, the rest. You could argue we are seeing the rise of multinational information aristocracies. But importantly there is no intermediary between us and them. We all use these services and we give our information to them of our own free will.

A key issue is people mostly don’t value their personal information very highly. On one hand, it makes sense because each individual data point is not much use to anyone. But if you flip it around, the multinational information aristocracies are nothing without the information of their users.

And another possibility is that we’ll all stop caring as much about whether someone might have smoked a spliff, recorded an embarrassing video or said some risqué things in a chatroom. The social expectations about acceptable behaviour can change fast; look at smoking and drunk driving, both of which were much more mainstream behaviours just a couple of decades ago.

As Giles Fraser, a South London priest and Guardian columnist, put it in a thoughtful opinion piece after the ECJ decision came out:

(I predict) the internet generation is going to end up being a lot better at what we used to be comfortable calling forgiveness. For if we are going to find it more and more difficult to forget, then we are surely going to find it more and more important to forgive.

This change is happening right now, and will continue to happen. But even if we end up in a more open, mature and forgiving world, where no-one cares about their permanent record because everything is awesome, is it enough for us rely on right now?

Law

The right to be forgotten as seen in the decision about the Spanish gentleman I mentioned at the beginning comes from existing law about relevance. A broader right to be forgotten is before the European Parliament. It recognises, to quote: ‘the desire of an individual to ‘determine the development of his life in an autonomous way, without being perpetually or periodically stigmatized as a consequence of a specific action performed in the past.’

The NZ Privacy Act actually already allows people to correct their personal information. You can do it right now – call up someone who’s holding information about you that’s wrong, or out of date, or inaccurate, or irrelevant, and tell them to correct it.

Agencies holding information have to either make the correction, or, if they don’t want to for whatever reason, they have to attach a statement setting out why you disagree with that information.

Could a New Zealand citizen assert a right to have links removed from a Google search on their name? The New Zealand law differs in some key respects from the Europeans’, but we have a similar obligation to keep information relevant.

The Law Commission finished its four-year long review of the Privacy Act in 2008 and, although they didn’t suggest there should be a right to be forgotten, they did propose a right to anonymity or pseudonymity in its report.
Following on from the Law Commission review is going to be a new Privacy Act, over the next year or two. Ending up with a right to be forgotten along the lines of the EU directive is one possibility, though admittedly a distant one, if there’s a good enough argument for it, if it becomes important enough to people, to the mores.

Architecture

Architecture is not just the web – it includes human architecture. We are human beings with fallible memory and limited storage space. We need memory because the world at any instant does not provide us with enough information to make the best decision about what to do next.

And as humans, we’ve supplemented our fallible memory with ever better prostheses, like books, libraries and computers. In the process, we’ve sanctified that notion of memory. The destruction of the Library of Alexandria is a historical crime that still has the power to make antiquarians shudder, because losing all that knowledge seems criminal.

However, while memory is anything in the past, if you make it fast enough the past becomes the present. A record of where you were five minutes ago is a record of where you are right now.

Conclusion and questions

Technical predictions are a quick route to embarrassment, but it’s safe to say that computers will keep getting better, and they will keep getting better at a faster and faster rate. Over time, retention will become more frictionless, and storage capacity and Moore’s Law follow the logarithmic curve relentlessly upward. We are either going to find some way to reintroduce friction and loss into the system or get used to living in a golden cage of information tweeting happily at our own reflection.

So some questions for you:

What do you think of a world where we have the right to more explicitly control how our information is stored and referenced, to make machines forget about us, would look like?

Is there a real demand for it, and is that demand strong enough to pull the architecture and the market with it?

And if we’re going to tweak the market, the mores, the law or the architecture to bring about that right, which version do we want to follow - a right to anonymity, a right not to be indexed or a right to obscurity?

Or should we merely forgive, rather than forget?

John Edwards is the Privacy Commissioner of New Zealand

The Commissioner’s speech can be read in full at: http://www.privacy.org.nz/news-and-publications/speeches-and-presentations/
Samantha Yorke is the new iappANZ Global Knowledge Net Chair for New South Wales, and is based in Sydney. This month we profile Sam, outlining her experience and musings on being a privacy professional in today’s interconnected world.

Samantha’s Profile

I recently took a leap of faith and embarked upon small business ownership after spending most of my career working for global technology companies. I now operate a legal and public policy consultancy business called New Mediation where I bring over 15 years of experience working in the consumer digital media and technology industry to my clients, who range from small Australian retail businesses to large blue chip multinational technology companies.

I’m also thrilled to serve as an advisor to the NSW Information and Privacy Commissioner’s office, All Together Now (Australia’s only national anti-racism charity) and a couple of Internet based start-ups founded by old colleagues, Quixo Facto (http://quixomatic.com/) and Taste Maven (www.tastemaven.com.au).

My European experience

I fell into the technology sector after arriving in London in the late 90s, with no job or network to speak of. Microsoft was looking for a lawyer to join a cross company team formed to help prepare their business and customers for the roll over into the year 2000. Remember we all thought that the world was going to end at midnight on 31 December 1999? I look back on this opportunity as a truly once in a lifetime experience which of course went by without incident and I soon found myself with a bit of spare time on my hands.

I was very excited to then join one other lawyer in supporting Microsoft’s fledgling consumer business across Europe, the Middle East and Africa. In 2000, this business consisted of 6 MSN websites but we could see the potential for growth in the online sector and we’d also been told in a conspiratorial whisper that there was a top secret new consumer product being worked on code named ‘Xbox’ that would need a lot of legal and regulatory hand holding in the coming years. Thus began nine years of supporting the expansion of the MSN business (33 sites by the time I left in 2008) and the launch of Xbox version 1 and the Xbox360 gaming consoles. It was a fascinating time to be working in the online space; I saw the birth of Google, Facebook and Twitter and the demise of AOL, MySpace and Friendster (which has now relaunched as a social gaming platform). I think of the Internet sector as being analogous to dog years – 1 year feels like 7 with the fast pace of change and innovation.

Interestingly, as the Internet grew, Governments and the media started to become more and more aware of the public policy issues emerging from this new publishing and communications platform. They began asking questions of the industry such as how do you try to keep kids safe online and what are you doing to protect people’s privacy? As I had been working so closely with the MSN and Xbox businesses I was asked to respond to these questions and represent Microsoft at Government meetings and within industry associations who were trying to present a unified voice.

On the regulatory front, the European Commission was quick to enshrine the fundamental right to privacy into the Data Protection Directive in 1995 and it was a fascinating and sometimes challenging effort to interpret these rights and obligations in the context of the ephemeral and borderless Internet. The other striking difference in Europe was the high level of awareness that the average
European citizen has around their right to privacy. Public discourse on privacy was much more prevalent than I could remember it ever being in Australia growing up in the 80s and 90s (I’m showing my age here!).

**Back in Australia**

Returning to Australia in 2008, 10 years after the Commonwealth Privacy Act was adopted, was an interesting point of comparison. Many of the public policy concerns that I had worked on in Europe were also being aired in Australia and whilst there was a lot of public debate about online safety issues, privacy rarely rated a mention. I joined Yahoo!’s Australian business soon after returning and enjoyed learning more about the Asia Pacific approach to privacy regulation and shaping Yahoo!’s privacy policies and practices in this region.

Fast forward to more recent times and privacy is a significant priority for many Australians. Privacy is regularly reported on by the media and concerns around unfettered surveillance and other privacy incursions are widespread. After leaving Yahoo!, I established the regulatory function within the Australian chapter of the Interactive Advertising Bureau, representing the digital advertising industry on issues such as online behavioural advertising, the reform of the Privacy Act and identifying best practice for moderating user comments on social media sites.

The legal and regulatory environment continues to struggle keeping up and remaining relevant when it comes to placing parameters around emerging technologies. There are fundamental challenges in trying to control a medium which knows no bounds and thus we are increasingly seeing efforts to harmonise principles based regulatory frameworks for privacy. I strongly believe that international cooperation and consistency is critical if we want to make a meaningful impact in maintaining and enforcing human rights and standards in the digital space.

Having worked with and alongside so many businesses who are actively charting a digital course for us all, I know that the industry takes these issues seriously and frequently goes above and beyond what their legal obligations are to ensure that their customers feel safe and empowered to make meaningful choices in shaping their digital experiences. It’s been a privilege to practice law and engage in policy formation in such a transformative time where our lives have literally been changed through the adoption of digital products and services and the evolution of ecommerce.

I became involved in the iapp when I returned to Australia, first as a run of the mill member, then as a board member, and now as what I call an actively engaged member. I am thrilled to assist in rolling out the new Global Knowledge Net program in New South Wales and am currently planning the first event for Sydney based members. Please be in touch if you have any suggestions or thoughts about how we can better share information and enable members to grow and succeed in their privacy related functions. I look forward to seeing many of you at the first event!

_Samantha Yorke is Managing Director of New Mediation and iappANZ Global Knowledge Net Chair for New South Wales_
Privacy by Design adopted by Privacy Victoria

By Carolyn Lidgerwood

On 1 July 2014, Privacy Victoria formally adopted Privacy by Design, becoming the first Australian privacy office to explicitly do so. Here is how it was explained by Acting Victorian Privacy Commissioner, David Watts, during Privacy Awareness Week (PAW) in May:

Privacy by Design ... is a series of internationally endorsed policies, approaches and benchmarks designed to integrate privacy with new technology to ensure that perceptions that privacy and the use of new technologies are tradeoffs, otherwise known as a zero-sum game, are overcome...

At a high level what Privacy by Design mandates is ‘embedding privacy into information technologies, business practices and networked infrastructures, as a core functionality, right from the outset...

Privacy by Design may be defined as an engineering and strategic management approach that commits to selectively and sustainably minimise information systems’ privacy risks through technical and governance controls. At the same time, however, the Privacy by Design approach provides a framework to address the ever-growing and systemic effects of information and communications technologies and large-scale networked data systems’.

The Acting Commissioner also observed that:

Ultimately Privacy by Design is the technique that is best adapted to support the joint objectives of respecting privacy and supporting efficient service delivery through the better use of information and communications technologies.

As summarised by Privacy Victoria during PAW, Privacy by Design is a framework that was developed by the (former) Information and Privacy Commissioner of Ontario (Canada), Dr Ann Cavoukian. Dr Cavoukian has emphasised that privacy assurance should become an organisation’s default mode of operation.

Privacy by Design should be very ‘front of mind’ in Australia right now. In addition to the practical initiatives in Victoria, Privacy by Design is also the focus of new Australian Privacy Principle 1 in the federal Privacy Act. That requires ‘APP entities’ (ie entities regulated under the federal legislation) to take reasonable steps to implement practices, procedures and systems to ensure privacy compliance. In this context, many Australian entities (in both the public and private sectors) are focussing on what Privacy by Design actually means in practice.

To that end, Privacy Victoria has highlighted the 7 ‘Foundational Principles’ developed by Dr Cavoukian to promote the objectives of Privacy by Design. In summary, the Foundational Principles are:

1. **Proactive not Reactive; Preventative not Remedial** (ie this anticipates and prevents privacy invasive events before they happen);
2. **Privacy as the Default Setting** (ie privacy is built into the system as an automatic protection)
3. **Privacy Embedded into Design** (ie privacy is embedded into design of systems and practices, it is not an ‘add on after the fact’);
4. **Full Functionality – Positive-Sum, not Zero-Sum** (ie a ‘win win’ through accommodating all legitimate interests and objectives)
5. **End-to-End Security – Full Lifecycle Protection** (ie ‘cradle to grave’ management of information)
6. **Visibility and Transparency – Keep it Open** (ie enabling independent verification)
7. **Respect for User Privacy – Keep it User-Centric** (ie privacy defaults, notices and user friendly systems)

As part of its implementation of Privacy by Design, Privacy Victoria is developing materials which will be released shortly.

These materials will be of interest not only to the primary audience (ie Victorian public sector agencies and local councils), but also to other entities who are focussed on how to best meet their privacy obligations.
Watch Privacy Victoria’s website for more details – http://www.privacy.vic.gov.au

For further information about the Privacy by Design ‘Foundational Principles’, see http://www.privacybydesign.ca/

Carolyn Lidgerwood is Rio Tinto’s Global Privacy Counsel. Carolyn is also a Board Director of iappANZ

Sherry Karver, The Edge of Memory, 2014
Getting bitten by what’s in the garden shed

By Peter Leonard

The Australian Privacy Commissioner’s July 2014 own motion investigation report into the Pound Road Medical Centre\(^6\) is a timely reminder of how privacy breaches often occur through sheer inadvertence.

Inadvertence errors more readily occur in times of disruptive change. Two such disruptions are when an organisation moves premises and when an organisation shifts from paper based to electronic records and then fails to implement proper cycles of review for destruction of physical records or purging of electronic records.

The Pound Road Medical Centre (PRMC) was on the move, both from PRMC’s old premises at Amberley Park Drive (in Narre Warren South, Victoria) and from paper based records onto electronic records, using software called ‘Medical Director’. PRMC ceased operating its medical practice at Amberley Park Drive in April 2011 and then operated from new premises. Some paper based records were kept at the old site. In about October 2012, boxes of paper records which it turned out included PRMC patient health records – consultation reports, results of medical investigations, etc. - for approximately 960 patients were moved from a locked room in the building at the old site, into a ‘garden shed’ at the back of the site. This was so that renovations for sale of the site could occur. PRMC later advised the Australian Privacy Commissioner that at that time it did not recognise that the moved documents ‘included some health records’.

The garden shed door was locked with three padlocks. Initially, a representative from PRMC visited the site two to three times a week and later once a week (for maintenance, repairs and renovations to prepare for the sale of the site). In November 2013, the shed was broken into. As a result, the boxes of medical records were compromised.

The Privacy Commissioner applied the obligation to take reasonable security steps to protect personal information formerly imposed under NPP 4.1 and now continued under APP 11.1. Was storage in a locked shed the implementation of ‘reasonable security steps’? Not surprisingly, the Privacy Commissioner concluded that it was not.

The Commissioner’s reasoning is interesting. Although physical security is an important part of ensuring that personal information is not inappropriately accessed, in order to have complied with the ‘reasonable steps’ obligation, organisations needed to have considered what other steps might be reasonable to ensure physical copies of personal information were kept secure. Such other steps included monitoring the movement of physical files; regularly auditing (or stocktaking) the content of files (including when they are moved) to ensure knowledge of the contents and that any information that is no longer required can be securely disposed of or de-identified. It also includes implementing physical access controls such as issuing a limited number of keys or passes to areas in which the information is stored; monitoring and guarding the location in which the information is stored and using a secure means of storage, such as a safe, or a secure or locked room in monitored, guarded or staffed premises.

The Commissioner stated that he ‘did not consider there to be any circumstances in which it would be reasonable to store health records, or any sensitive information, in a temporary structure such as a garden shed. As an exacerbating factor, the shed was not located at PRMC’s premises, which means that PRMC was not in a position to effectively monitor access to the shed. PRMC’s failure to take reasonable security steps was also exacerbated by the fact that it did not identify or deal with health records stored at the site for a period of more than 2 years following the relocation.’

The Commissioner then went on to consider whether PRMC had complied with its obligation to take reasonable steps to destroy or permanently de-identify personal information not being used or disclosed for a permitted purpose (in other words, where the personal information is no longer required).

To comply with this obligation, an organisation must have had systems or procedures in place to identify information the organisation no longer needed, and a process for how the destruction or de-identification of the information would occur.

PRMC advised the Commissioner that prior to the data breach, PRMC reviewed paper-based patient health records every two years to identify whether the complete paper record had been scanned into the patient’s computer record (and if not, any remaining documents were then scanned to the computer record and the paper-based file then destroyed by secure shredding), and also to identify records which are eligible to be destroyed in accordance with the Health Records Act 2001 (Vic). PRMC confirmed that the last review of paper based records prior to the data breach occurred in early 2011.

The Commissioner noted that in order to satisfy the ‘reasonable steps’ requirements, consideration was required as to both procedures and adherence to those procedures. PRMC did not demonstrate in this instance that it had systems in place to identify all personal information that was not being used or disclosed for a permitted purpose. While the Commissioner accepted that PRMC had implemented such procedures at its current premises, these procedures did not appear to have been applied to documents at the previous site or when PRMC moved to its current premises. Although PRMC advised that when relocating its practice and moving documents to the garden shed, it believed that the relevant documents comprised only information other than patient health records, PRMC knew that the records included records such as payments to medical practitioners, paid invoices and accounts to third parties (which were also stored in the garden shed). These other records also contained personal information. Accordingly, PRMC’s obligation to securely destroy or de-identify personal information that was no longer required would still have applied to the records it actually knew were in the shed. In any event, the majority of the records identified in the shed following the data breach related to patients who ceased to be active patients prior to 2004 – at least eleven years old - which the Commissioner concluded also indicated a failure by PRMC to identify and securely destroy or de-identify personal information about patients that was no longer being used or required, regardless of whether such records were in the garden shed or not.

However, the Commissioner decided to close the investigation following his finding that PRMC was acting appropriately in response to the data breach. Responsive actions included reviewing its privacy policy, developing a data breach response plan, conducting training with all personnel (including partners, doctors and other health professionals working at PRMC) to ensure their understanding of privacy and security policies of the practice, and their obligations under the Privacy Act, undertaking a risk assessment regarding its management of personal information including patient clinical records, and implementing measures to review paper-based patient health records annually to identify whether they may be de-identified or securely destroyed. PRMC also advised that it intended to engage a specialist privacy consultant to undertake a further risk assessment, to help ensure adherence to privacy policies and procedures, and to undertake periodic reviews of data security processes.

As noted at the outset, privacy breaches often arise through inadvertence. Inadvertence errors more readily occur in times of change including when an organisation shifts from paper based to electronic records and then fails to implement proper cycles of review for destruction of physical records or purging of electronic records. The garden shed case reminds us that not only funnel web spiders can sting when you don’t know what’s in the garden shed.

Peter Leonard is a partner at Gilbert + Tobin Lawyers working with data analytics applications and also a Board Director of iappANZ.
We are delighted to announce some of our key speakers for Privacy@Play, the annual iappANZ Summit for 2014.

Privacy@Play will feature international and national speakers who address global privacy issues. There are streams include the Internet of things, Crisis Management and Delete: the right to be forgotten. We are also introducing our inaugural Asia Pacific Thought Leadership panel session with voices from Japan, Hong Kong, New Zealand, Malaysia and Australia.

This year’s theme revolves around the evolution of privacy from a ‘bolt on’ compliance issue into an integral part of business. We will be taking a deep dive into how earning the trust of consumers unlocks information that is the lifeblood of business.

Confirmed key speakers:

- Timothy Pilgrim, Australian Privacy Commissioner
- Stephen Deadman, Global Chief Privacy Officer, Vodafone, UK
- Katrine Evans, Assistant Commissioner, Office of the Privacy, Commissioner, New Zealand
- Hiroshi Miyashita, Associate Professor of Law, Chuo University, Tokyo
- Mr Allan Chiang, Privacy Commissioner for Personal Data, Hong Kong
- Dr Libby Morris, Primary Care, eHealth Lead, NHS Scotland
- Dr Zainel Abidin Sait, Deputy Director General, Personal Data Protection, Malaysia
- Malcolm Crompton, former Australian Privacy Commissioner and holder of the iapp 2012 Global Privacy Award

We also have terrific group of panelists and guest speakers including from:

- ACMA - Commissioner, Australian Communications and Media Authority
- ADMA - Association for Data-driven Marketing & Advertising representative
- AGL - Head of Metering Operations, AGL Energy
- ARCA - CEO, Australian Retail Credit Association
- Johnson & Johnson Chief Privacy Officer, Asia Pacific
- Macquarie Group - General Counsel, Privacy & Data Legal and Governance
- Telstra, Chief Privacy Officer
- Victorian Privacy Commission’s Deputy Commissioner

Registrations are open:

Full Price: iappANZ Member - $595 plus GST, Non-member - $756 plus GST
Special Early Bird rate : iappANZ Member - $545 plus GST, Non-member - $706 plus GST
Non-members – iappANZ membership fee is deductible from the iappANZ Privacy Summit fee!

For registration information, please contact Emma Heath, GM iappANZ, emma.heath@iappanz.org
Win a Cash Prize: iappANZ’s writing prize 2014

iappANZ is very excited to announce the launch of its [$250 cash] writing prize for a second year running for an article that is published in our monthly Bulletin between December 2013 and October 2014. Anyone can enter (you don't have to be an iappANZ member), simply by writing and submitting an article between 500-1500 words that tells us something interesting, new and relevant about privacy.

All articles must be submitted by email, preferably in Word, to [veronica.scott@minterellison.com or an iappANZ email] by 20 October 2014. We will need the author's email address and contact number. You can submit as many articles as you like. Click here for more details.

The winner will be announced at our Privacy Summit on 25 November 2013 and their name and details will be published on our website. We also hope to profile the winner in our Bulletin.

So alert your network and get writing!

More details about the writing prize if you are interested:

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

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

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

Portfolio Manager - Customer Privacy & Awareness
Digital Protection Group, Commonwealth Bank

What will I be doing?

Reporting to the Executive Manager – Digital Trust & Privacy, this is a 6 month contract position delivering Privacy Impact Assessments and assurance services to the Bank. Responsibilities include:

- Managing the delivery of Privacy Impact Assessments and other privacy advisory services to internal customers;
- Managing two Privacy Advisors;
- Drafting, reviewing and quality assuring Privacy Impact Assessments and other privacy assurance services to the Bank;
- Building and implementing strategies to support provision of services to the broader Group, locally and internationally;
- Supporting the EM – Digital Trust & Privacy with strategic research and planning documentation to drive the digital trust agenda;
- Enhancing relationships with key stakeholders, internal and external; and
- Maintaining awareness of new privacy and network security laws and regulations as well as industry best practices and integrating these into technology and business processes.

What are we looking for?

- Strong knowledge and understanding of current industry practices, laws and regulations as they apply to privacy and data protection within Financial Services (both domestic and international);
- 8-10 years’ experience within Financial Services or another large corporate or leading technology provider, with recent and extensive experience in privacy and data security;
- Demonstrated thought leadership capability and ability to communicate to all levels;
- Strong customer focus;
- Practical experience in managing stakeholders to effect change, including strong influencing skills;
- Demonstrated commercial acumen and experience in service delivery and meeting budgetary KPIs.

To apply or for more information, please contact Christine Dunn at dunnch@cba.com.au before Friday 15 August 2014.
## Privacy Events

<table>
<thead>
<tr>
<th>Time, Date &amp; Location</th>
<th>Information</th>
<th>Price</th>
</tr>
</thead>
</table>
| **Monday 18 August**  | Privacy After Hours – in Melbourne!  
Join local privacy professionals for a drink and a bite and some networking.  
*Privacy After Hours are hosted by a local IAPPanz member. Anyone can attend. You don’t have to be an IAPPanz member, just interested in or involved with the use and protection of personal information.*  
[www.thedeanery.com.au](http://www.thedeanery.com.au) | Attendees are responsible for their own expenses. Drinks and bar food is available please see The Deanery’s website for details |
| **Thursday 28 August 2014**  | PRIVACY LAW MASTERCLASS  
Understanding privacy reforms and managing operational and compliance challenges from Australia’s new privacy laws.  
10% discount for iappANZ members · quote VIP Code: MP-IAPP when registering to receive the discount. | Fee $1195.00 before 31 July, 2014  
http://www.aventedge.com |
| **Friday 29 August 2014**  | PRIVACY LAW MASTERCLASS  
Understanding privacy reforms and managing operational and compliance challenges from Australia’s new privacy laws.  
10% discount for iappANZ members · quote VIP Code: MP-IAPP when registering to receive the discount. | Fee $1195.00 before 31 July, 2014  
http://www.aventedge.com |
| **Wednesday 24 September**  | WELCOMING A NEW PRIVACY REGIME IN NEW ZEALAND  
iappANZ and KPMG Wellington are hosting a privacy lunchtime presentation with guest speakers:  
John Edwards – Privacy Commissioner, New Zealand  
Russell Burnard – Government Chief Privacy Officer, NZ  
Paul Holmes - Strategic Privacy Manager, ACC, NZ | Booking and price information to come  
Check iappANZ website [http://www.iappanz.org](http://www.iappanz.org) for more information |
### Thursday 25 September
**12.30 – 2.00pm**
**Deloitte**
**Deloitte Centre, 80 Queen Street**
**Auckland**

**WELCOMING A NEW PRIVACY REGIME IN NEW ZEALAND**
iappANZ and Deloitte are hosting a privacy lunchtime presentation with guest speakers:
- John Edwards – Privacy Commissioner, New Zealand
- Russell Burnard – Government Chief Privacy Officer, NZ
- Paul Holmes - Strategic Privacy Manager, ACC, NZ

**Booking and price information to come**

Check iappANZ website [http://www.iappanz.org](http://www.iappanz.org) for more information

### Monday 17 November 2014
**All day event**
**The Westin Hotel, Sydney**

**iappANZ Privacy Summit**
Join us for another great set of privacy sessions and international keynote speakers
See details of speakers earlier in this edition of Privacy Unbound

**Full price:** iappANZ Member $595 plus GST, Non-member $756 plus GST

**Early Bird rate:** iappANZ Member - $545 plus GST, Non-member $706 plus GST
Non-member: the membership fee is deductible from the Privacy Summit fee

For registration information, contact: emma.heath@iappanz.org
IAPP Certification

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

The International Association of Privacy Professionals (IAPP) says:

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

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

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

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

CIPP/IT assesses understanding of privacy and data protection practices in the development, engineering, deployment and auditing of IT products and services.

What about testing?

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

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

Our contact details

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

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

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