President’s Letter

By Anna Kuperman
President
M: 0419 803 263

Dear members,

This is my first letter as incoming President and the last issue of our Journal for the year ... so, being a case of firsts and lasts, I would like to extend my appreciation to the generous volunteers who kindly gave their time, expertise and energy during 2014 to enhance learning and connections among our members. So, in no particular order, thanks goes to the following!

- Emma Hossack, our immediate Past President who will remain on the Board as ANZ Chair of Strategy and continue to inspire and drive initiatives for our members.
- Board of 2014 and our General Manager, Emma Heath.
- Melina Rohan and Julie Inman-Grant, our retiring Board Directors for 2014.
- Veronica Scott and Carolyn Lidgerwood, our very talented editors of Privacy Unbound Journal.
- Timothy Pilgrim and the Office of the Australian Information Commissioner for contributing to our Journal, our training events, sessions and member communications.
- Dr Elizabeth Coombs, New South Wales Privacy Commissioner, Katrine Evans, Assistant Commissioner (NZ Office of Privacy Commissioner) and Russell Burnard, NZ Government Chief Privacy Officer for generously contributing to our Summit this year.
- All of our presenters and contributors to the Journal this year.
- All of our sponsors without whom we could not provide valuable member benefits.

Lastly, a big welcome to Olga Ganopolsky and Tom Bowden, our incoming 2015 Board Directors who I look forward to working with next year. On that note, I’d like to wish everyone a happy and safe end to the year.

All the best. Anna
Vice-President’s Foreword

By Melanie Marks
Vice-President
melanie.marks@cba.com.au

I'd also like to take this opportunity to acknowledge and thank Danny Weitzner and CBA for presenting a special Breakfast Briefing in November. Details of this event are covered by Kate Monckton.

For the last decade in the profession, I have been saying “the wave is coming”. Well it seems the wave has arrived or at least started to arrive. Privacy is now a dinner party conversation. It’s newsworthy and companies and organisations realise just how much is at stake both in terms of compliance with legal frameworks and ethical decision making to build trust with consumers. Perhaps the heightened awareness is what is driving iappANZ growth and why the last Summit was the biggest ever and our membership rates have more than doubled over the last year.

The year ahead is going to be big. If you’re reflecting on how you can get more out of your membership, form stronger professional connections and make a difference to our profession, now is the time to join an iappANZ Sub-Committee. More details about this on page 5.

If you’ve got other thoughts on how the iappANZ can serve you and your organisation, I would love to hear them.

Wishing you a happy, healthy and relaxing break and I look forward to seeing you next year.

Melanie
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
Overview of iappANZ's 2014 annual Summit and AGM

by Veronica Scott

This year our annual Summit was held at the Westin hotel in Sydney's CBD. We were very pleased to be able to welcome more than 160 delegates, a notable increase on last year's numbers. For our member who were able to attend, we hope you came away with some more privacy insights and tools to use in your won privacy practice. For those of you who couldn't make it, we hope you can join us next year and in the meantime, we are pleased to be able to report on the day's sessions in our last Journal for 2014. You can also access some of the slides and presentations from our website here. A big thank you to our Summit sponsors, in particular our Platinum sponsors Intel and Commonwealth Bank.

The day kicked off bright and early with speed dating (and yes, some dancing – congratulations Russell Burnard) at 8am followed by a welcome from our outgoing president Emma Hossack. The Summit was then formally launched by The Hon. Michael Kirby, AC MG who (after giving what he said was the shortest speech of his (remarkable) 44 years of office) announced the winner of the iappANZ Journal Writing Prize, Alex Webling, who we profile in this issue, and whose winning article is reproduced below. The rest of the days' proceedings were then smoothly and tirelessly officiated by veteran journalist and commentator Richard Ackland – thank you Richard.

We were fortunate to have three remarkable and very different key note international speakers - from the USA, Scotland and England - Larry Irving (CEO Irving Group), Dr Libby Morris (GP and Clinical Lead, eHealth NHS Scotland) and Stephen Deadman (formerly Group Privacy Officer of Vodafone Group, UK).

We saw the launch of regulatory policies by the Australian Privacy Commissioner Timothy Pilgrim and the NSW Privacy Commissioner Dr Elizabeth Coombs. Our panels hotly debated what was currently hot in privacy and the impact of the European right to be forgotten.

The afternoon kept us alert with an illustrious panel of international privacy commissioners and experts together for the first time in Australia with a bit of help from modern technology) and our two break out workshops on crisis management (focusing on data breaches and emerging cyber threats) and the thought provoking 'Internet of things'.

We closed the day's proceedings with our AGM and 2015 Board election followed by networking drinks. Your new Board for 2015 has some familiar faces but we are also pleased to have some new faces, Olga and Tom (who is based in New Zealand):

Officers and Executive Committee:

Anna Kuperman (President), Melanie Marks (Vice-President), David Templeton (Secretary) and James Kelaher (Treasurer).

Ordinary Directors

Carolyn Lidgerwood, Peter Leonard, Veronica Scott, Tom Bowden, Olga Ganopolsky, Kate Monckton, Emma Hossack and Malcolm Compton
Sub-committees

We have the following sub-committees which work on key activities and functions of iappANZ. These are open to any of our members to join or contribute to in ways big and small and we would love to hear from you if you would like to help out:

- Membership & Partnerships
- Training & Events
- Global Knowledge Networks
- Online Strategy (website and digital)
- New Zealand
- Privacy Summit
- IAPP Strategy
- Privacy Unbound Journal

Summit coverage and feedback

We were so pleased with your feedback about the Summit. Thank you for what you’ve shared with us, and remember that further feedback can be sent to our General Manager Emma Heath (emma.heath@iappanz.org).

You can read the report about the Summit from New Zealand’s Office of the Privacy Commissioner (‘Prospecting for privacy gold in Australia’ at https://www.privacy.org.nz/blog/iappanz-summit/)

There was also terrific coverage in CSO – see at http://www.cso.com.au/tag/iappanz-summit/

You can also read the review from Malcolm Crompton (Information Integrity Solutions and iappANZ board member) right here: http://www.openforum.com.au/content/good-privacy-good-business.

Further reports from each of the Summit sessions follow ....
Speed dating for privacy professionals

by David Templeton

I’ve never really consistently been an early riser. So why would I make the effort to be at a conference before 8:00am, more than an hour before the morning’s keynote speaker?

Because it’s iappANZ offering Speed Dating, that’s why.

The Privacy @ Play organisers arranged a rapid burst of visits to each table by a recognised privacy professional. Just a few minutes each, so time to start a conversation but for mere mortals like me, not nearly enough time to finish one! There were more tables than daters, but I was lucky enough to get conversing with:

- **Kate Monckton**, of NBN and the iappANZ Board who was keen both to tell us all about iappANZ and listen to suggestions;
- **Helen Lewin**, Deputy Commissioner at Privacy Victoria, who jumped straight into an informative account of Victoria’s public sector privacy laws and reminded us that Victoria has a bill of rights. For those of you following the common law of privacy and linking recent UK cases to the *UK Human Rights Act 1998*, this is significant as it places Victorian plaintiffs in a position very similar to that of plaintiffs in the United Kingdom;
- **Ben Carr**, Chief Privacy Officer at Telstra, who shared insights into Telstra’s internal thinking concerning privacy;
- **Olga Ganopolsky**, General Counsel Privacy and Data at Macquarie Bank, who completed a very warm and welcoming round of introductions – ensuring everyone at her tables got to speed date too;
- **Daad Soufi**, Director of Legal and Regulatory Affairs at ADMA, who spoke of the issues that direct marketing is grappling with;
- **Russell Burnard**, New Zealand’s Government Chief Privacy Officer, who explained how his role differs from, and complements that of John Edwards, New Zealand’s Privacy Commissioner;
- **Tom Bowden** (CEO of Healthlink, New Zealand), whose organisation deals with 65,000,000 health records; and
- **Charlie Offer**, Partner at Ernst & Young, who discussed some of the challenges facing Australian organisations.

[Editors’ note: Hosts Emma Hossack and Jonathan Dobinson also played a fabulous range of privacy-inspired music tracks to set the mood – both of them may have missed their calling on commercial radio! Russell Burnard took home the smooth moves dance prize. We look forward to more speed dating next year! Thanks to all the daters and to the hosts]
Key note speech: *Privacy in the era of mobility*

by Larry Irving (CEO Irving Group)

Review by Anna Kuperman

I was fascinated by the presentation from Larry Irving, previously a principal advisor to the Clinton administration on telecommunications and internet policy and now CEO of the Irving Group.

Almost two decades ago, Larry authored a report around privacy and the Internet – an unknown field at that time but one that would change communication on a global scale. Ironically, the same concerns noted then loom now – what is being collected, how is it being used and why?

Irving described the pervasive nature of mobile devices - handheld beacons that can be used to track individuals. The mobile adoption rate is unprecedented in our technological history, and the smartphone rate eclipses that of mobile devices generally.

This is not a case of science fiction. This is happening now, with tracking being used in commercial settings to see how a customer moves through a store and assess the best lay out for shopping spaces. Irving talked about his own personal shopping for a refrigerator and being presented with ‘smart’ options which enable the contents to be restocked in an automated fashion with the device talking to the food supplier. Convenience or in-house surveillance? Does it matter? Well, it might if it affected your medical insurance by tracking your dietary habits!

Aggregation of data from multiple sources is being used to promote marketing offers when the tracking data and shopping habits from loyalty programs are correlated. So what? Well, Larry points out that as consumers, we don’t really know what data is being held, how it is being used, how it will be used in future or what controls are in place to protect individuals. Does it matter? Well, for some reason, our privacy concerns become less important when we think we are getting something for free. Irving says the lack of cohesive regulation for mobile devices, from platforms to apps means we’re flying without a net.

You can follow Larry on [Twitter](#).
Key note speech

The success of the Scottish shared health record system implementation: balancing the privacy and clinical outcomes

by Dr Libby Morris

Review by Emma Hossack

Whenever I hear tales of ehealth implementations, I think of the quote by Nobel Prize winning Laureate in Economics, ‘You can see the computer age everywhere but in the productivity statistics.’ ehealth does not have a sterling record for being on budget and producing outcomes, as we have seen with the issues surrounding the Australian Personally Controlled Electronic Health Record and the English NPfIT. Consequently, the presentation by Dr Libby Morris was a pleasure.

Libby spoke about the Scottish Key Information Summary, which is a national shared records system operating in all GP practices in Scotland. The aim of the programme is to ensure that timely accurate information is available for all clinicians to improve patient safety. The first evaluation has been completed by Yorke University, and the presentation covered the findings, including the challenges of fulfilling the needs of patients and clinicians. Libby also discussed the tension between patient trust and the value to public health through the extraction of pseudonymised data, and plans to use this information safely for secondary uses and feedback to practices.

Scotland has 14 Health Boards which oversee primary and secondary care. The primary care sector has been using sophisticated records for 20 years, and has excellent databases, but none of them are connected. Whilst silos create a level of privacy on account of the cost and inconvenience of linking up information without indexes, the inability to share information is inimical to the provision of good healthcare. Particularly in the emergency department, when time can be critical.

The programme spent one year just talking with and otherwise educating patients and community groups about the proposal. With a lot of investment in education, opt out was seen as a viable way forward. The team agreed to a very basic ‘vanilla’ data set, uncontroversial, with demographics, allergies, adverse reactions and medication history. A small data set made it easier to cope with at the start. It attracted no media interest. There was no ‘big bang.’

Within a year, the Scottish programme had 5 million records and 100% coverage. The system is not just empty registration numbers either, they have had 3.6 million accesses, and are now beginning a patient access pilot and are looking at Application software, for example mobile apps which are designed to run on smartphones and other mobile devices. One of the other reasons the system was able to work so well, was the fact that in Scotland each patient is registered to one General Practitioner, leading to a greater sense of trust and, by having a GP ‘home’, outcomes are easier to achieve.

In Scotland, access to the patient’s record is covered by a simple and transparent access log which is graphed and shows anomalies like weekend and after hours log ins. This enables breaches to be identified, such as when...
an emergency worker looked up all the health records of members of his football team and the Prime Minister. This was noticed by the Practice manager on the graphs and led to the dismissal of the emergency worker.

In the emergency care sector, only Key Information Summary (KIS) is retained, and not all people have all their information registered. For instance, palliative care patients do not. Scotland took a granular approach to who needs what information where, and not a top down one size fits all.

The Scottish primary care information system, SPIRE, also enabled the use of extraction of patient data and used pseudonymisation, which identified and separated data sets which could, with permission, be linked later in time. No information was allowed out without separation of the identifier at the source. They also had reference to the Caldicott Report and a Privacy Advisory Committee.

By starting small and creating a culture where providers were educated about the huge responsibility to look after patient information and ‘put themselves in the patient’s shoes’, the project engendered trust. Just as Professor Alessandro Acquisti told us at the iappANZ 2012 Privacy Summit, once you have people’s trust there is a likelihood that they will provide you with even more information. In the case of healthcare, this is invaluable for research and service deployment. For example the study showed that mental health issues were twice as prevalent in disadvantaged areas.

In summary, how did this group manage to shout across the chasm? By taking incremental steps, educating the patients and starting small and gently.
Keynote speech: *Personal Data disrupted*

by Stephen Deadman

Review by Melanie Marks

There are two kinds of privacy dialogues taking place in today’s world.

One is about how best to address legal and compliance obligations to manage privacy as a risk concern.

The other is about how to embrace change by driving new, customer centric information and business models.

Stephen Deadman, former Group Privacy Officer and Head of Legal – Privacy, Security & Content Standards at Vodafone Group champions the second dialogue, joining strategists, venture capitalists and analysts in recognising the tremendous business opportunity emerging from changing consumer expectations in privacy.

Here are the key themes from Stephen’s presentation at the Ssummit:

*Privacy is on the front page*

Privacy is now a dinner party conversation. The Snowden revelations have made individuals increasingly aware of and concerned about how organisations and governments are handling their personal information. Privacy infringements and violations are now front page news. Privacy has become a constant in the media and commentary on privacy regimes are now also playing out in the arts, meaning it is increasingly become part of a collective discussion.

*People as products and growing distrust*

Beyond mere awareness, there is a growing perception that organisations are benefiting from people’s personal information and with this comes the mounting suspicion that we are the ‘product’ and that are being exploited.

Individuals are recognising that their information has a value – whether it’s a set of information that forms a verified digital identity that organisations can trade, or a profile that makes them a marketable candidate - which again has economic value, consumers will increasingly distrust organisations that make the wrong decisions or act outside of their expectations. Consumers are beginning to recognise that service providers holding their data may face conflicts of interest in respect of it.

The asymmetric Internet is driving distrust amongst consumers. Here’s how the thinking goes: corporations hold huge data banks with sophisticated analytics tools which they use and exploit pursuant to non-negotiable sets of terms and conditions. The vendor controls all. By contrast, the little guy has scarce information, no access to analytics and no control over the contracts he enters into. Put simply, he (or she) is powerless.

*Old privacy frameworks don’t work as well anymore*

1980s frameworks for managing data viewed it as a waste product: valuable but to be treated in containment. These frameworks don’t work in today’s high pace, high volume, data driven world of interactions and transactions and whilst data previously was something controlled only by wealthy businesses it is now conceivable that individuals might be able to process their own data.
Big business is starting to recognise the inherent value in being the holder of data and of digital identity and to market this as a differentiator. Think Apple’s commitment to privacy:

‘A few years ago, users of Internet services began to realise that when an online service is free, you’re not the customer. You’re the product. But at Apple, we believe a great customer experience shouldn’t come at the expense of your privacy.

Our business model is very straightforward: we sell great products. We don’t build a profile based on your email content or web browsing habits to sell to advertisers. We don’t ‘monetise’ the information you store on your iPhone or in iCloud. And we don’t read your email or your messages to get information to market to you. Our software and services are designed to make our devices better. Plain and simple.’

*It’s all about control*

This tsunami of change is driving consumer interest in transparency and better yet, control. In an economy where technology and unlikely entrants to new markets are already shaking up business landscapes, a new disruptor is emerging and that is the consumer, actively seeking and *expecting* ways to personally manage their data, rather than leaving this business to organisations and governments with their own motivations and conflicts of interest. As a result, organisations will have to adapt or risk losing customers.

*Bring on the PIMs*

Enter personal information management services (PIMs) which are – in Stephen’s words – accelerating and deepening existing digital disruption by filling key value gaps in today’s consumer markets. This is good not only for the consumer but for the organisation. Personally curated data has intrinsically higher value than other sources, displacing less ‘responsibly sourced’ data in the market. Personal control over personal data can help legitimately unlock Big Data opportunities. The market value of PIMs is substantial (think £16.5 bn or 1.2% of the UK economy, compared with the automotive industry (0.7%) and pharmaceuticals (0.97%)). Also, the current level of venture capital investment in PIMs illustrates we should all be taking notice! Examples of PIMs which are giving individuals tools for controlling their personal information right now include:

- https://www.allfiled.com/
- https://www.respectnetwork.com/
- http://ctrlio.com/
- http://www.miicard.com/
- http://www.socialsafe.net/
- https://mydex.org/

Stephen explained that Vodafone has embarked on a program of change in response to the new personal information disruption. It has reviewed its settings both in policy and technology and looked for ways to innovate and build upon its relationship with customers. It has developed the tools and capabilities to put the customer in control.
Even if your organisation is not yet ready to embrace the sorts of PIMs offerings already in the market, every organisation should be reflecting on what this growing demand tells us about consumer expectations and what this means for business strategy and opportunity.

Stephen concluded by noting that 2015 sees the 800th anniversary of Magna Carta – the great charter of human liberties. In an environment where individuals need to take control of their own data in order for the Internet to meet its full potential, perhaps it’s time we had a Magna Carta for the web? Food for thought.
Privacy, the state of play

by Australian Privacy Commissioner Timothy Pilgrim

Review by Carolyn Lidgerwood

‘... recent events such as the Target breach in the US, and the impact that had on their financial performance and the personal impact it had on their senior management should be sufficient warning about the importance of managing privacy risk. And if they’re not, then I hope you’ve read my recent decisions, listened very closely to what I have been saying about our regulatory approach, and that you’re planning to read our Regulatory Policy very closely, because not taking the right approach to managing privacy appropriately will not put you in good stead in the event I undertake an investigation of your organisation’. (Timothy Pilgrim, iappANZ Summit)

With this, the Australian Privacy Commissioner had everyone in the room sitting up straight!

The Commissioner provided a timely overview of the year that’s been and what to focus on in the year to come. Here is an overview of his messages at the iappANZ Summit

Setting the scene

At the outset, the Commissioner emphasised that privacy is far from being irrelevant in our modern, online age. To the contrary, it is becoming increasingly intertwined with everything we do, and people are becoming increasingly aware of the value of their personal information and the importance of protecting it.

This emphasises the importance of trust – and finding the balance between protecting our privacy and participating with others in the modern technological age.

This was a key theme of the day, and the Commissioner placed it ‘up front and centre ‘at the start of the Summit.

Developing this theme, the Commissioner referred to the recent International Conference of Data Protection and Privacy Commissioners and its focus on ‘ubiquitous connectivity’. Devices that we use to make our lives easier also generate a massive amount of data. While new technologies and big data pose privacy challenges, the technology neutral principles behind privacy (including transparency, accountability and responsiveness) themselves provide the tools we privacy professionals need to navigate those challenges.

Assessments are coming

The Commissioner characterised new Australian Privacy Principle 1 (APP1) in the Privacy Act as ‘the bedrock principle that sets up all of the other practices, procedures and systems organisations need to have in place to meet their obligations. If you get APP 1 right, you’ve got privacy governance right’.

In 2013, not long before the commencement of the new APPs and as part of an annual global sweep, the Office of the Australian Privacy Commissioner assessed whether the privacy policies of the top 50 Australian websites, public and private sector, were ready to comply with APP 1. Most were not.
Going forward, the Privacy Commissioner’s office will be conducting assessments of websites identified as part of that annual sweep, checking for compliance with APP 1. The Commissioner emphasised that while no specific sector will be singled out, the focus will be on organisations that are the high risk or high volume users of personal information. Don’t say you weren’t warned.

New resources

The Commissioner emphasised a number of times that his office works with APP entities, providing guidance to assist them to comply, and conciliating complaints. However sometimes, regulatory action is necessary.

In this context, the Commissioner announced that the launch of his office’s *Privacy Regulatory Action Policy*, which explains the powers available to the Commissioner and the approach his office will take in using those powers. While the Policy is not a radical shift in approach, it provides transparency. A *Guide to privacy regulatory action* is also under preparation. When read with the *Privacy Regulatory Action Policy* and the APP Guidelines, the Guide will help organisations to understand what the Privacy Commissioner expects – and that is the definition of essential reading!


The Commissioner explained that in addition to investigating and attempting to conciliate complaints, he has discretion about the use of other regulatory powers, and factors that will be taken into account include:

- the seriousness of the situation;
- whether the organisation in question has been the subject of prior compliance or enforcement action;
- whether the conduct relates to a systemic issue; and
- whether the entity has taken appropriate steps to remedy the situation, and what these steps are.

Where there has been a data breach, the Commissioner emphasised that attempts to conceal the breach will ‘not be looked well on by our office’.

The Commissioner also announced that revised security guidance will also be published soon, in the upcoming *Guide to Securing Personal Information*. This will contain examples of reasonable steps entities are required to take under the Privacy Act to protect the personal information they hold. The Commissioner also emphasised the importance of ‘designing and building-in security measures that factor in the human element’ – noting that human error happens and security measures need to recognise that.

Wrapping up the year

The year that has passed has seen:

- much work to implement the new privacy laws, the most significant changes to the Privacy Act since its commencement;
- the ALRC’s report on a statutory cause of action;
- examination of mobile apps as part of a global privacy sweep;
- renewed focus on the data retention debate;
- the right to be forgotten gaining attention not only in Europe, but throughout the Asia Pacific region;
the largest growth in privacy complaints to the office since the Privacy Act commenced; and
a very successful Privacy Awareness Week.

The Commissioner also noted that since March 2014, he has made five section 52 determinations, including a recent award of $18,000 for non-economic loss. It has been a big year.

In that context, the Commissioner noted that the Government’s decision to abolish the Office of the Australian Information Commissioner was still being implemented, but it remains ‘business as usual for privacy’, in that there will continue to be a Privacy Act, a Privacy Commissioner supported by an Office, and business as usual in terms of privacy regulation.

In concluding, the Commissioner emphasised that this is where we must all get to with privacy compliance - privacy is about business as usual - and must be embedded in all of our processes.

The Commissioner’s speech is available in full at:
iappANZ Writing prize 2014

Winner profile – Alex Webling

by Carolyn Lidgerwood with Alex Webling

Alex Webling is this year’s winner of the iappANZ writing prize for his article ‘Can social login be privacy enhancing?’, which was announced at the Summit. This is the second year of the prize, which has had some terrific contributions warranting quite a few special mentions. Alex now keeps company with our now iappANZ Board member and Treasurer James Kelaher who won last year’s inaugural prize.

Here we profile Alex and reproduce his winning article.

1. Congratulations on winning the Privacy Unbound writing prize for 2014! Can you tell us how you came to be a privacy professional?

I’ve been working in the area of information security, management and privacy since 2002 when I started working in the Federal Attorney-General’s Department as the ‘Special Advisor – Electronic Security’.

Setting up the Australian Government’s Computer Emergency Response Team in 2007 and subsequent roles taught me the importance of personal information. In 2012 I developed the proposal to make the Document Verification Service (DVS) available to the private sector and led teams that worked on the government’s biometric interoperability framework and developing research which gave better data on the size of identity crime in Australia and the systemic flaws in the federated identity system. It was this experience which gave me a detailed understanding of Australia’s identity system and its myriad vulnerabilities.

I left the public service in 2012 and set up Resilience Outcomes, which focusses on strategic information security and management. www.resilienceoutcomes.com

2. What are the current issues in privacy and data protection that interest you most?

I think one of the biggest issues is related to secure identity in the online world. There needs to be a paradigm shift in Australia’s identity system to make identity safe and secure in the online environment and to reduce the costs of using identity for both the public and organisations.

This is as much the fault of government policy settings as much as the realities of corporations. The ‘federated identity system’ that we depend on is broken. Systems like the DVS provide some bandaging, but the move online is tearing at an already archaic system.

The other issue is a lack of information security strategy in organisations.
Organisations, both private and public, collect far more information than they need to. Often there is what I call a ‘Pokemon approach’ (Got to catch ‘em all) to customer information. Data storage has become extremely cheap, but the cost of data security is soaring. I know there are excellent exceptions, but I think that there is a failure to understand the risk equation at the board level.

I generally advise companies to think very carefully about whether they need to have private information. It may seem obvious to readers, but one of the cheapest breach mitigations is to not collect sensitive information in the first place because it creates a target for hackers and exposes companies to enormous reputational risk if it is exposed. Information management systems are currently built with the idea of keeping all information indefinitely – too few organisations think about the advantages of getting rid of information as soon as it is no longer valuable, or the risk equation changes.

In light of the breaches on major corporations such as Sony, this message needs to be shouted out from the rafters!

3. Despite being a privacy journal, we do love hearing people’s stories! Can you tell us some more about you?

My first language is German and I grew up in Adelaide. I’ve lived in Brisbane since the beginning of 2013 when we moved from Canberra. Apart from spending time with kids, family and our new dog, Cleaver Black the standard poodle. My other interests are: I try to walk or cycle during which time I listen to any number of podcasts ranging from Nature and BBC Click to the RN Media Report. Cooking outrageous dinners with my spouse (such as the pepper fried crabs we ate recently), - gaming (Xbox – Currently Destiny), usually in an online session with an eclectic group of Adelaide refugees and photography, mostly macro  
https://www.flickr.com/photos/kangaroo-pie/ or http://www.wordpress.com/awebling. Also for the last year I’ve been doing a bit of programming (thank you Codeacademy and Coursera) and I bought an Arduino kit to tinker with.
Can ‘social login’ be privacy enhancing?

(Originally published in the May 2014 issue of Privacy Unbound)

The likelihood that any Australian Government is going to create an online identity credential now seems distant with the National Trusted Identities Framework (NTIF) almost forgotten. How quickly the Internet forgets, but maybe that’s a good thing if you’re Mario Costeja González.

But the need that the NTIF sought to fill has not gone away. Governments are trying to work out how to service their citizens/customers/users at lower cost. The Internet offers one possibility, but in taking their services online, government agencies expose themselves and us to different threats and potentially higher risk. However, it seems inevitable that government agencies will follow financial institutions in offering higher value transactions online. In the end, the economic argument is likely to drive government agency migration online with more high trust services. Recent federal and state/territory budget announcements are only likely to spur this movement.

There are a number of threats that need to be mitigated before a government agency could potentially provide its services online. Probably the key issue is for the agency to be sure that a user requesting access to a site is who they say they are. Currently issuing the customer with a username and password mostly does this, but the model is beginning to fail. The problem is that most people don’t interact with government agencies on a regular basis and yet information sensitivity and computer capabilities require users to adopt increasingly complex and nonsensical passwords.

This in turn makes the passwords more difficult to remember even as they are harder to crack. It also means that password resets are much demanded. Yet at the same time, customers are expected to change their passwords regularly, not to write them down or repeat them for other online services.

It seems clear that these password requirements largely force customers to break their user agreements and either, write their passwords down, or worse re-use them for other services/websites.
It also puts government agencies in a bind. They want to provide online access to their services because it could be cheaper to operate than bricks and mortar outlets (if they didn’t have to reset too many passwords), but they also do not want to be embarrassed by privacy and security breaches.

One option is the use of a social login to help secure online authentication. This could enhance user information security and minimise privacy breaches. Social login, also known as social sign-in, is a form of simple sign-on (to web resources) using existing membership of a social networking service such as Facebook, Yahoo, Twitter or Google+ to sign into a third party website in lieu of creating a new login account specifically for that website or service. Social login is designed to simplify logins for end users as well as provide more and more reliable demographic information to website owners. Social login can be used as a mechanism for both identity authentication and user authorisation.

Social login is being adopted by private sector organisations for a number of reasons including: rapid registration; verified email contacts; and customer ‘stickiness’. However social login also offers three major benefits for government agencies.

- Currency of contact data. Contact data such as email tend to be kept up to date by the user.
- Passwords are less easily forgotten because they are regularly used. At the same time, the social login passwords are not transmitted from the user to the agency website.
- Security. Agencies can leverage security technologies implemented by the social networks that they might never be able to replicate themselves. Because of their resources, social networks such as Google and Facebook are able to detect and patch ‘zero day exploits’ (ie which take advantage of a security vulnerability on the same day that the vulnerability becomes generally known) quickly.

So what are the privacy risks?

A user, when accepting the convenience of a social login, can share a significant amount of their information between a third party website (such as a government agency) and the social network. The social site is informed of every social login performed by the user. Often, it is worth considering whether users understand exactly what they are sharing and whether they are giving informed consent to share. However this risk can be mitigated with the creation of clear and detailed login screens, which explain what the users are sharing.
As an example, the following information is returned when a Facebook user agrees to share their ‘Basic Profile’. Other than the email, the information is not verified and may not be present. However, several organisations claim that the quality of the data returned is in general very good because social network users feel social pressure from their friends to be accurate:

<table>
<thead>
<tr>
<th>Address</th>
<th>Birthday</th>
<th>Verified Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>Family Name</td>
<td>Formatted Name</td>
</tr>
<tr>
<td>Gender</td>
<td>Given Name</td>
<td>Homepage</td>
</tr>
<tr>
<td>Preferred Username</td>
<td>Profile Photo</td>
<td>Time Zone</td>
</tr>
</tbody>
</table>

At the same time, it is not necessary for the third party website to collect all the information if it is not required.

Another issue surrounds current sensitivities with the USA NSA’s indiscriminate ‘hoovering’ of online data. It is important to note that because all the large social networking sites are based in the USA, they are subject to USA’s laws and customs related to security and privacy. Under that regime, Australians are given significantly fewer protections than USA citizens or residents. Effectively, the social networking site itself provides the main protection for reputational reasons. However, readers may be aware that there have been recent moves in the USA to change this approach for what the US charmingly calls ‘aliens’ like Australians and give the same protections for all users irrespective of citizenship.

Can we get the benefits of social login and have citizen privacy as well?

With careful design it seems possible that social login could enhance privacy for users at the same time as providing benefits to government agencies. Considering the social login as an adjunct to agency authentication rather than the whole process could be an answer. If customers nominate their social login at the same time as they were enrolled into a government service, they could later use their social login as the first stage of an authentication process. This would provide an outer layer of defence against hacking. The user could then login to the agency itself using a separate authentication process.

The advantages of this model (beyond defence in depth), are that the user logs into the agency with their authenticated social login username, but does not gain access to sensitive information without providing an agency specific authentication. The social network also does not receive any sensitive information beyond the fact that a user logged in at a website. The use of government portals can be used to obfuscate which government agency a user is accessing. At the same time, with consent, contact information from the social login site could be compared with that held by the agency and presented to users so that they can choose to update the information held on them by the agency.

At both the state and federal level, government agencies are starting to actively consider social login. Provided that governments are also prepared to carefully design the user interaction so that the social networks don't get any more personal information than the user/citizen is prepared to share - by turning off analytics and sharing social network authentication gateways across groups of government agencies, it can provide benefit to users and government alike.
In the longer term, government will be able to verify citizens online when they wish to enrol themselves for services. The possibility arises to use the Document Verification Service (DVS) combined with social history to connect an entity to an identity, but that may be a discussion for another time.

Alex Webling. BSc, BA (Hons), Gdip Comms, GdipEd, ZOP, is a registered security professional in the area of enterprise security management and has 20 years experience as a senior executive for the Australian Federal Government including in cyber-security, critical infrastructure protection, identity security and resilience. To tell Alex what you think, please email him on alex@resilienceoutcomes.com. He would love to hear from you.
Privacy Panel: *What's hot in privacy? Yes it can be sexy!*

**Review by Kate Monckton**

The first panel session of the Summit saw Ben Carr (Telstra), Dr Elizabeth Coombs (NSW Privacy Commissioner), Mia Garlick (Facebook) and Jon Lawrence (Electronic Frontiers Australia) take to the floor skilfully chaired by Jennifer Mulverny (Intel) to leave little doubt in our minds that privacy is anything but dull!

Jennifer opened with a humorous anecdote relating to her young son on the concept of trust that had a more serious message for the adults in attendance. Trust was a key theme across all of the panellists’ comments with Ben Carr noting that for Telstra to be successful as they expand their services, trust is pivotal to their success.

Jon Lawrence shared some fascinating statistics which showed the level of trust Australians have about government agencies’ handling of meta-data, with Telcos and ISPs not faring particularly well. He suggested that the majority of people are confused about data privacy and this is leading to a lot of anxiety about how their personal information is used by government and other organisations.

Mia Garlick gave us all a very enlightening insight into how Facebook is building privacy into its product features by encouraging users to determine what information they share with whom.

Dr Elizabeth Coombs spent some time talking about a new tool for the public sector that she launched at the Summit. The [Privacy Governance Framework](#) is an online privacy tool designed to encourage organisational engagement with the management of personal information. Explaining more about what makes a governance framework successful, Dr Coombs emphasised the need to have ‘CEO and down’ support.

There were a number of questions and comments from the floor, many of which returned to the role trust has to play in privacy with regards to government and the private sector.
Media Panel: *Delete-the right to be forgotten*

Review by Veronica Scott

The response to the European Court of Justice's decision earlier this year in Mario Gonzales' privacy complaint against Google, giving EU member citizens the right to request search engines to remove links containing their personal information has been strong on all sides of the debate. This was reflected in the media panel and it was no surprise that we were treated to a very lively and robust debate (which is just how we like it). It was a challenge trying to capture and do justice to all the arguments, but here goes …

**An unwelcome decision**

Panel chair Ann Flahvin (Media & Communications Counsel, Policy Australia and Special Counsel Baker & McKenzie) kicked off proceedings with the news of the UK government's plan to 'do what it can' to get rid of the right, having not intervened on the assumption that the ECJ decision would go the other way. It has described the decision as 'impractical, impossible [and] undeliverable'.

**Re-writing history**

Peter Bartlett (Partner, Minter Ellison) agrees. He thinks that this is a very bad decision and. Even though no one was saying their data is inaccurate or untrue, they can effectively re-write history. He gave the example of a report that someone had been charged with an offence as a true and relevant part of history. While accepting that it would be a legitimate requirement to report that at trial, the individual was found not guilty, he did not agree that references to the charges against the accused should be deleted altogether.

**How to enforce?**

Peter also expressed concerns about how Google will deal with the hundreds of thousands of requests it has received to take down links and queried what kind of training its employees will have to enable them to make decisions on such a difficult and subjective issue. Even more worrying is what the decision would mean for other search engines who don't have Google's deep pockets. Without the necessary expertise or resources, it could mean that search engines will err on the side of censorship. Therefore, he was of the view if you are going to have a system, it should be well thought out first and preferably applied world wide.

Closer to home, Peter cited a number of recent Court of Appeal decisions in Victoria and New South Wales, which he said showed that Australian courts were declining to make orders that would be futile and could not be enforced. By comparison, he said that the ECJ has made a decision that cannot be enforced against other publishers and therefore is largely ineffective while being a significant attack on freedom of the internet. He noted that the Australian Law Reform Commission had suggested, in its discussion paper earlier this year on its enquiry into a statutory tort of privacy, that there should be a right to be forgotten in Australia in relation to what people put online about themselves. However, this was not proposed in its final report.

**Impact on the public interest**

Richard Ackland (our MC and experienced journalist) thought the decision peculiarly European. He reminded us that it is only Google that has to take the link to the original source down, which should not affect free speech because you can still find the material itself on the original website. On the other hand, as the whole world is
now conducted through online search functions, a report that is very much in the public interest could be undermined. He used the example of former judge Marcus Einfeld, who, having been caught speeding in Sydney a few years ago, denied he was the driver and named Theresa Brennan as the driver. After a Daily Telegraph reporter filed a story on the court proceedings, a sub-editor did some research on the woman in order to find a photo of her. What he in fact found was that she was dead at the time she was allegedly driving the car - which meant that a judge had lied to the court. This case he said was an example of the many problems that the new right has thrown up.

Richard also thinks that the decision could lead to the ‘balkanisation’ of the Internet, rather than allowing it to be enjoyed at a global level.

A question of truth

At the heart of the decision for Richard is the question - what is truth? In the case of Mr Gonzales’ complaint against Google, the information online was true but with time passing, it became partially true. Richard is also concerned that the decision could become a mechanism for a defamation claim through the back door whereby plaintiffs could get a privacy injunction to stop a defamatory publication that was true.

A win for the interests of data subjects

In response, David Vaile (Co-convenor, Cyberspace Law and Policy, Faculty of Law UNSW) said that while the media and Google made much of the decision, nothing has been heard from the data subjects. This is, he said, a decision which channels their interests. Anyway, he believes the decision is really nothing new and has nothing really to do with the media. We already have legislation of this kind for example for spent convictions. The Australian Privacy Principles in the Privacy Act require personal information to be accurate, relevant, up to date and complete.

He said that the hazard for data subjects is the permanent global publication of every minor detail of their lives, that they post, their friends post and that the government collects. This leaves what he called ‘an exhaustive data trail’ from which global profits are being made with Google, as a product of the marketing and software industry, sitting at the top of the pile as the gateway. He said that what Google was really asking for was forgiveness, but it is not forgetting.

While our European friends balance free speech and privacy and in the USA free speech trumps everything, David reminded us that in Australia ... we have neither. Now, for the first time, it is the individual who gets to have a say. He thinks it is a small price to give individuals the right to ask in relation to something that affects their life. It is a balance between data sovereignty and digital protectionism. There is no magic law in cyberspace in relation to what Google can publish - the law of each particular country will apply.

In any event, he says, we already have Internet filtering via untransparent mechanisms and the likes of Facebook and Google get to decide what we are told. Why then shouldn’t Google have the responsibility to manage privacy in relation to its secret algorithms, which is in the end a marketing driven service?
Whaleoil.co.nz

The panel was asked how to deal with the kind of pernicious and very nasty things that a right wing New Zealand blogger had published about many people and made available via Google search results. Peter Bartlett pointed out that you can ask Google to take down defamatory material.

No sign, but the same repository

We were all made to stop and reflect by a comment from the floor that Google was merely a signpost to a repository of information which may or may not be correct. In a historical context, it was like one response to the Nazi invasion of Europe – people took down the street signs to try. The problem was still in the repository.

The decision it was said, raises a number of competing rights, including the right to regret....
Asia Pacific panel: Thought Leadership

Review by Carolyn Lidgerwood and Malcolm Compton

The Asia-Pacific panel at the summit featured a unique line-up of privacy regulators and thinkers, and provided excellent insights into the state of play in our region – appropriate for the Privacy@Play theme!

Panel Chair, iappANZ board member and former Australian Privacy Commissioner Malcolm Crompton asked each panel member to comment on the latest developments and also to discuss how accountability expectations have changed in the region. Here are some points from each country -

**Australia** – Timothy Pilgrim (Privacy Commissioner) challenged organisations to think about what they can do to improve privacy practices and ‘value add’ to their organisations. The Commissioner particularly focussed on organisations being accountable. That means an organisation has to be aware of what personal information it holds, what’s being done with it, who it’s being shared with and where it is.

The Commissioner emphasised that accountability procedures will come alive when privacy is a ‘front of mind’ issue for the board – ask whether your organisation’s privacy governance structure goes up to the board, and does the board understand its privacy obligations? Significantly, the Commissioner commented that recent investigations were demonstrating that some organisations do not have the procedures in place that are now needed under APP1, and that must be addressed.

**New Zealand** - Katrine Evans (Assistant Commissioner at Office of the Privacy Commissioner) introduced the New Zealand law reform process, including stronger enforcement powers for the Commissioner and mandatory data breach notification obligations. The Assistant Commissioner discussed the data analysis environment and the challenge of preserving privacy values, including protecting against misuses of re-identified data.

When discussing accountability, the Assistant Commissioner noted there had been a lot of change in the New Zealand public sector since the ACC breach, with a new Government Chief Privacy Officer and increased emphasis on risk management. While overnight change is not possible, incremental change is (with the quote of the summit – ‘How do you eat an elephant? One bite at a time’). The private sector is also looking to the public sector learnings from the ACC report – and that’s a shift from the past, when the private sector was well ahead of the public sector on privacy implementation. Now the line is less clear.

**Malaysia** - Dr Zainel Abidin Sait (Deputy Director General for Personal Data Protection) highlighted that in Malaysia, the focus is not so much on the fact that there is new legislation (which has been enforceable for just one year), but on creating a new compliance culture, with privacy becoming part of business processes. The message in Malaysia is that protecting personal data is everyone’s responsibility. Changes are happening, with significant numbers of privacy policies being published, a high number of registration applications, and codes of practice now developed for every main industry that handles personal data.

Accountability concepts are not centre stage yet, with the Deputy Director General commenting that Malaysia is still in the start-up phase. Lawyers have been targeted as a way of getting the privacy message through to business. Not only would lawyers influence industry, but they would see a business opportunity for themselves!
Singapore - David Alfred (Chief Counsel for Personal Data Protection Commission) explained that the Commission was established just last year, with the privacy provisions of Singapore’s legislation coming into force in July 2014. The Commission is focussed not only on enforcement but also on education and developing a new privacy compliance culture – with outreach to organisations being emphasised. The education message is about how personal data can be used while also being protected, and educating individuals to protect their own personal data.

In discussing accountability, the Chief Counsel commented on the role of the DPO or data protection officer in Singapore; and that as a compliance baseline, organisations needed a DPO and a policy explaining their data processing practices. The more senior in the company, the better the compliance perspective, and that is why in Singapore the DPO should be someone with appropriate seniority.

Japan - Hiroshi Miyashita (Associate Professor of Law from Chuo University in Tokyo) observed that while we are now all part of a global village with global information flows, privacy is still a local issue. He explained how privacy is often considered to be a form of individualism, which is not a big feature of Japanese culture (with its community focus). In this context, the Associate Professor explained the current law reform process in Japan and the challenges of big data - questioning whether personal data can ever really be de-identified, and in practice, the real issue should be whether the data is ‘less identifiable’. He noted that matters under discussion in Japan include a new supervisory authority, trans-border transfer regulation and exemptions for medium size businesses.

Accountability is not a Japanese concept, but the Associate Professor explained that in Japan the focus is on trust mark certificates (with 13,000 companies having these at the last count); and also on data breach notifications (with notifications to data subjects being common place). Issues about the right to be forgotten are also being vigourously debated in Japan, with conflicting court decisions, and more work needed on developing objective criteria for data deletion. The Associate Professor provided this memorable quote (almost as good as the earlier quote from New Zealand): ‘the Americans want to be famous; the French want to be forgotten’.

Hong Kong - Allan Chiang (Privacy Commissioner for Personal Data) joined the panel on a live link and discussed how ‘accountability’ was being promoted in Hong Kong through his Privacy Management Plan initiative. He observed that when he commenced as Commissioner, the emphasis in Hong Kong was on technical legal compliance but that was no longer sufficient. Today, organisations need to go beyond that and ensure that privacy becomes part of corporate governance, with the attention of senior management. The Commissioner also emphasised it’s not about doing the bare minimum for legal compliance, it’s about doing more for customers and making privacy part of the services being offered.

In Hong Kong, high profile breaches (such as the Octopus Card controversy) influenced the revision of the Ordinance, which has led to increased regulation of direct marketing and sales of personal data. Accompanying that has been the Commissioner’s policy of naming organisations that breach the law. Unsurprisingly, the results have been that companies are becoming more responsive – and striving to have privacy part of their DNA (including Octopus)!

In conclusion – while the countries in the Asia Pacific region are at different stages of implementing regulatory frameworks for privacy and data protection, there are many common themes, including active and engaged regulators. We are all on notice!
The Asia-Pacific panel – with Allan Chiang beaming in from Hong Kong!
Workshop: Crisis management – coping with data breaches and emerging cyber threats

Review by Veronica Scott

Anne-Marie Allgrove from Baker & McKenzie chaired this experienced panel from government and the private sector on managing data breaches and their impact, both on individuals and organisations, with a focus on the challenges of dealing with cyber threats.

Anne-Marie highlighted the possible claims that could result from a data breach including breach of confidence negligence and misleading and deceptive conduct, as well as the more direct privacy related issues, the reasonable steps obligations under Australian Privacy Principle 10 and the day to day management of a data breach crisis.

Take away messages

Some of the key messages from this workshop included:

- the importance of reporting and sharing information on data breaches - in particular cyber attacks;
- the need for a crisis management plan;
- the ability to access and use your own back up data held by third parties;
- the impact on individuals of identity theft as a result of cyber breaches; and
- the need increasing complexity of the cyber threat.

Lessons from the Distribute.IT cyber hack

Alex Woerndle (Commercial Manager, CQR Consulting) was very generous in sharing his intimate experience of the data breach no-one wants to have whilst he was owner of web hosting company Distribute.IT. He explained all the things that could go wrong and did as a result of a malicious third party attack in 2011 on Distribute.IT’s systems. Looking back on the media reports the following statement issued by the company at the time is sobering: "The overall magnitude of the tragedy and the loss of our information and yours is simply incalculable".

As an ICANN-accredited domain name registrar Distribute.IT was subject to a mandatory data breach notification regime and had to report the breach to its governing association. In the end it lost its accreditation.

The task Distribute.IT faced was immense - it had to try and recover and rebuild a network. Alex talked about the waterfall effect of the delays or misfocus on issues that undermined their recovery. The most critical thing was not having access to their own data. The contracts they had in place did not enable them to access and retrieve their own data held by third parties when the attack hit.

There was also the impact on staff, the loss of their know how when they had to be let go, the daily media coverage and the huge overall costs. Without a crisis management plan, the directors got too involved in the day to day response and could not focus on making decisions on the issues they were responsible for.

In the end, Distribute.IT had to sell its business in order to continue the recovery efforts.
A key point that this data breach identified was importance of contractual provisions that allow organisations to access, retrieve and protect their data held by third party providers.

Identity Theft

Andrew Rice (Assistant Secretary, Cyber Identity Security Policy Branch, Attorney General's Department) talked about the difficulty of cyber identity theft and rebuilding your identity. His office he says receives about 5,000 calls a year from people asking for help. There is a real case for resources and support for people rebuilding their stolen identity.

Don't give up - "It's better to keep building the jet while you are flying than not fly at all"

With this quote, Russell Burnard (New Zealand Government's Chief Privacy Officer based in the Department of Internal Affairs) gave us his take on things from his perspective in a newly created role. When things go wrong you need to keep flying. That's the reality. He said we need better reporting as we can only manage what we measure. There is a great push for mandatory data reporting in New Zealand which he believes will come.

Gary Blair (Principal Consultant, Imali, Adjunct professor Edith Cowan University Security Research Institute) explained the need for funding in and more work to be done on cyber-security research with the huge threats of cyber crime and frequency of cyber attacks. He explained the work of the Government's Computer Emergency Response Team (CERT) established last year to enable the sharing of information and reporting of computer/cyber crime incidents.
Workshop: The Internet of things

Review by Carolyn Lidgerwood

The ‘internet of things’ is one of the buzziest of buzz phrases right now. We have all heard about it, but there are so many questions about what it really means in practice.

An excellent panel of VSPs (very smart people) gave us some answers at the Summit.

Peter Leonard introduced the session by referring to the obvious hype around the internet of things, noting that in the ‘hype cycle’, high expectations often precede the ‘trough of disillusionment’. Peter’s description of us all ‘peering over the precipice of the Trough of Disillusionment’ is another contender for the quote of the Summit!

However as Peter noted, the explosion in the number of devices connected to the Internet means that we all need to come to grips with ‘the Internet of things’. He noted that today there are 6 billion devices connected to the Internet. By 2020, estimates put that number at 50 billion: that’s between 4 and 7 connected devices per person. And at present, most smart products are fragmented and do not work together: data is siloed in each product’s separate app. That will change in the future as devices grow more inter-connected. Also, Internet enabled smart meters and other smart home devices will enable tracking of movements and other activities of individuals within the home and other private places. Peter asked the panel to provide some insights.

Matthew Poblocki (Director of Legal Affairs, Paypal Australia) took us though a long list of things we need to be thinking about as the Internet of things takes hold, and an increasing number of our devices are ‘connected’:

- Data may be used in ways beyond expectation or a user’s authorisation;
- Data might not be accurate or be misleadingly incomplete;
- Tracking or monitoring is often disproportionate to the purpose of the app or device;
- Automatic data processing can happen with no human intervention – what if it goes wrong?
- Denial of access to data or devices can lead to harm to individuals: economic loss, loss of trust or even physical harm;
- Inappropriate access (eg hacking) leading to changes in device settings can also cause harm.

Lachlan Burg (Executive Group Manager for Risk and Compliance at RACQ) talked about how the Internet of things is connecting cars and car accessories— but there are questions remaining about how this data (including data about our driving locations and the performance of our cars) will be controlled and processed. In the future all cars will be connected, but is it really consent if you don’t have a choice? I don’t think so.

Ian Opperman (CEO of Rozetta Technology) then took us to Tasmania, and applications of sensoring technology in agriculture – and how this was taking us into the ‘internet of everything’. Richard Ackland’s report of Ian’s presentation (in The Saturday Paper on 24 November 2014) is too good not to share:

[Dr Opperman] gave the example of a project in Tasmania where sensors monitored the impact of pesticides on the land, their runoff effect on the water and how that water affected the oysters in the river system. There were electronic sensors on the oysters to tell whether they were happy or sad. If they got too sad, a message was sent electronically to mollusc farmers telling them not to harvest their crop. Peter Leonard ...
asked the crucial question – whether the oysters had learned to be permanently sad so as to trick the sensors and not get harvested and eaten. This is why lawyers are worth fat hourly rates.

Peter Marks (Mobile App Developer, ABC) spoke very positively about the possibilities of the Internet of things, while also delivering some cautionary messages, particularly around security settings and uses of data that we just don’t expect. No-one is going to read the licence agreements that explain how our data is going to be used – and so how can we overcome this?

Larry Irving (CEO of Irving Group) answered that question by emphasising that app developers must be consumer focussed and ‘put people first’. Larry also focussed on how some uses of data collected from the Internet of things could raise discrimination issues, as more becomes known about how people operate in all aspects of life. One example he gave was that new car apps that detect micro sleeps could impact older drivers more than younger drivers, and have employment and insurance implications. He noted that concerns as to discrimination issues had been one focus of a recent White House report and it was important to consider the broader consumer welfare issues that arise from new data analytics applications.

So much to think about. In his blog, Malcolm Crompton summed up the session in this way:

While … the Internet of Things will undoubtedly bring great benefits, tricky questions were raised with respect to personal information in particular: Who owns the data? Who gets to decide what happens to it? Can we really consent if we don’t have a choice? How is it protected from loss and misuse? Control – or rather, the lack of it among individuals – was identified as a crucial issue that needs to be addressed going forward.


These are challenging issues. But they are issues we need to start grappling with now.
Danny Weitzner  CBA Breakfast Briefing

by Kate Monckton

In the week prior to the Summit, CBA hosted a breakfast briefing with Danny Weitzner. iappANZ Board member Kate Monckton reports …

For those of you who haven’t heard him speak or met Danny in person, he’s a pretty awesome guy. He was the United States Deputy Chief Technology Officer for Internet Policy in the White House. He led initiatives on privacy, cybersecurity, Internet copyright, and trade policies promoting the free flow of information. He was responsible for the Obama Administration’s Consumer Privacy Bill of Rights and the OECD Internet Policymaking Principles. He is currently a director of the MIT Computer Science and Artificial Intelligence Laboratory, Decentralised Information Group.

Danny's presentation was a highlight at last year’s iappANZ Summit so the intimate breakfast gathering hosted by CBA for a group of iappANZ members was an opportunity not to be missed. Danny certainly didn’t disappoint; in fact the discussion continued way past the official cut off time!

The key areas of discussion included, an update on the ‘hot’ privacy topics coming out of the USA and the question of jurisdiction over security and privacy practices. He gave us the background to US privacy laws, including the sector by sector approach that has prevailed.

Danny also explained that the Snowden revelations are in the background of all US security and privacy policy discussions, especially with regards to big data privacy concerns and the potential for discriminatory impact on individuals in its use. He also talked about Snowden with regards to the impact his disclosures have had on the relationships between governments, telecommunications and technology companies, and consumer privacy trends, using examples of both Apple and Google announcing they would be shipping products with device level encryption by default.

Danny kept us all spell bound for the duration and offered valuable insight into the questions posed by the audience, which primarily focused on data retention and comparisons between Australia and the USA.

All in all, a great way to start a Friday! We hope we can welcome Danny back to Australia in the future.
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).

Commonwealth Bank
Privacy Advisor

- Privacy SMEs with the market trail blazer in Digital Technology & Innovation
- Career move with Australia's Leader in Financial Services
- World Class Facilities based in Sydney CBD

Are you currently in a Consulting or Legal Firm or Policy Advisor role in Government and looking to build on your privacy experience in a commercial role on the client side? If so, this could be the career move that launches your career.

CommBank is recognised as leading the industry in IT and operations with its world-class platforms and processes, agile IT infrastructure, and innovation in everything from payments to internet banking and mobile apps.

**What will I be doing?**

Reporting to the Portfolio Manager – Customer Privacy & Awareness, this role delivers Privacy Impact Assessments and privacy assurance services to the Bank. Responsibilities include:

- Conducting Privacy Impact Assessments and providing other privacy assurance services to customers within the Bank;
- Working across the business to influence the design of data privacy requirements in systems, projects, products and services;
- Providing SME support to internal customers through meetings and written communication and advice;
- Undertaking ad hoc research
- Maintaining awareness of new privacy and security laws and regulations as well as industry best practices and integrating these into technology and business processes;
- Monitoring legal and policy data privacy developments in countries where the organization operates;
- Participating in industry networks and associations.
Your new team

The Digital Trust and Privacy Team is an integral part of the Digital Protection Group (DPG), which has as its mandate the protection of the CBA Groups' platforms, systems, data, assets and reputation from security, privacy and operational risks. Further, the DPG is charged with leveraging our capabilities in the security, privacy and operational risk to create innovative and market-leading products and capabilities, preparing and protecting the Group for our digital future.

What are we looking for?

We expect you will have experience within Financial Services or another large corporate or leading technology provider or in a legal or policy advisory practice with recent and extensive experience in privacy and/or data security. You will possess strong knowledge and understanding of current industry practices, laws and regulations as they apply to privacy and data protection. You will be a good communicator with a strong customer focus, pragmatism and experience in service delivery.

At CommBank each of us globally is dedicated to offering outstanding service, excellent advice and intuitive solutions to help our customers manage their finances in the ways they want to.

Regardless of where you work within our organisation, your initiative, talent, ideas and energy all contribute to the impact that we can make with our work. Together we can achieve great things. Sound like you?

Apply now to take the next great leap forward in your Privacy career.

Click here to apply.
Privacy Events

<table>
<thead>
<tr>
<th>Time, Date &amp; Location</th>
<th>Information</th>
<th>Price</th>
</tr>
</thead>
</table>
| February 2015 [date TBC]  
5.30pm - 8pm  
Minter Ellison Lawyers, Melbourne  
525 Collins Street | iappANZ Victoria KnowledgeNet  
We decided to postpone our pre-Christmas get together and will instead kick off 2015 with a review of the year that was, including some of the key privacy decisions, followed by drinks and some nibbles and a chance to catch up with your fellow privacy professionals to welcome in another year for privacy.  
Stay tuned for more communications about this event when the date is confirmed. | Free member event  
RSVP your interest to Emma Heath, iappANZ GM  
emma.heath@iappanz.org |
IAPP Certification

Privacy is a growing concern across organisations 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 IAPP Certification provides you with internationally recognised evidence of your knowledge. It may be the edge you need to secure meaningful work in your field.

The IAPP says:

‘Skilled privacy pros are in high demand and IAPP certification is what employers want. When you earn an IAPP credential, you earn the right to be recognised as part of an elite group of knowledgeable, capable and dedicated privacy professionals.’

The IAPP offers three Module credentials which are relevant to iappANZ members, namely;

- **CIPP: Law and Regulations** - the global standard for the go-to person for privacy laws, regulations and frameworks (USA - Privacy or Government sectors, Europe, Canada)

- **CIPM: Operations** - the first and only privacy certification for professionals who manage day-to-day operations

- **CIPT: Technology** - the industry benchmark for IT professionals worldwide to validate their knowledge of privacy requirements

To achieve these credentials, you must first successfully complete the Certification Foundation which 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 and assesses understanding of privacy and data protection practices in the development, engineering, deployment and auditing of IT products and services.

iappANZ now has IAPP Certification Foundation and Module materials for iappANZ members.

FOR MORE INFORMATION ABOUT GETTING ‘CERTIFIED’, TRAINING AND TESTING PLEASE VISIT OUR WEBSITE BY CLICKING HERE.
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)

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