Dear Members

This month I am very happy to announce that this year’s ‘Trust in Privacy’ iappANZ Summit will be held on Monday 14th November at Dockside in Darling Harbour, Sydney. Watch this space for more details about registration and our line-up of speakers, which is looking great. We have a number of other events coming up soon, including a workshop in Brisbane on during Privacy Awareness Week (May 17th) on Data Security and Data Breach - Protecting Your Critical Data with an array of engaging speakers and hosted by Queensland’s Privacy Commissioner Philip Green. Also during Privacy Awareness Week, we encourage our Melbourne based members to join us for a Privacy After Dark networking event on May 19th at the Arbory Bar and Eatery. For more information, please contact our General Manager Emma Heath.

Looking a little further ahead we have a Mandatory Data Breach Notification workshop lined up in Adelaide for June – more details to follow.

Looking back over the last month or so, we’ve had some really great events across Australia and New Zealand that have received brilliant feedback from our members about the quality of the events and speakers. I’d like to thank everyone who helped make those happen, many of you have generously given your time and effort to help us and it’s highly appreciated by us all.

With privacy awareness weeks kicking off in ANZ (albeit not quite at the same time!) there certainly seems to be a lot happening out there. We’d love to hear about any activities or campaigns you might be running in your organisations to help raise awareness of privacy, so if you’ve got anything you’d like to share please drop us a line.

I look forward to seeing some of you out and about during Privacy Awareness Week in Australia.

Kate.
Dear Members

Privacy Week is kicking off in New Zealand from 9-14 May 2016, closely followed by Privacy Awareness Week (PAW) in Australia from 15 to 21 May 2016.

In this edition, Sam Grover (Communications Advisor from the Office of Privacy Commissioner in New Zealand) provides a snapshot on topical issues of intelligence, security and privacy in NZ. Striking a balance between personal privacy, national security, transparency and trust continues to occupy the minds of regulators, legislators and policy makers. The recent review into NZ’s intelligence and security legislation provides a timely opportunity to assess its continuing fitness for purpose during Privacy Week. Sam also introduces Professor Joe Cannataci, the UN Special Rapporteur on the Right to Privacy. Professor Cannataci will be visiting Australia and NZ and sharing his views on surveillance and oversight of intelligence gathering.

Privacy Commissioner Timothy Pilgrim provides a teaser on what to expect for PAW in Australia and notes that the Office of the Australian Information Commissioner (OAIC) will be launching a range of resources, including on rights to access and correction, resources specifically for parents and young people, and a template for developing a privacy management plan. PAW 2016 will take on an international perspective this year with Professor Cannataci presenting on the global privacy agenda, as well as the promotion of awareness and discussions amongst businesses, government agencies and the broader community on how we can protect and respect the privacy rights of all Australian citizens.

Mr Pilgrim has recently welcomed the Government’s decision, outlined in this weeks’ budget, to allocate $37 million over the next four years to fund, ongoing, the OAIC’s privacy and FOI regulatory functions.

Dawn Swan (Privacy Officer at Inland Revenue NZ) in Wellington, and Katherine Gibson (Director at Gibson Law Limited) in Auckland provide an informative report on recent seminars held in Wellington and Auckland on the topic of Aligning Privacy and Security. A common theme emerged from presenters in the public and private sector; namely, if customers are to have trust and confidence in an agency or business to look after their information, then the privacy and security functions must work together. Agencies and businesses that empower customers to have a say in controlling the use of their data build trust in their privacy programs and ultimately protect their business.

Turning from privacy governance to wrestling privacy rights and freedom of speech in the US, Taryn Wood (Corporate Counsel at Southern Cross Austereo) looks at the recent Hulk Hogan case where the Court found in favour of Mr Hogan and awarded him US$115 million in compensatory damages – US$55 million for economic loss and US$65 million for emotional distress – as well as an additional US$25 million in punitive damages. In this surreal tale of sex, lies and digital tapes, Mr Hogan sued the Gawker after it posted a video clip showing the wrestler having sex with the then-wife of his then-friend, the radio personality ‘Bubba the Love Sponge’. The high profile privacy breach case casts a spotlight on what rights (if any) individuals have in Australia to claim similar relief without a statutory tort for the invasion of privacy.

We are also pleased to be able to profile, the award-winning Director of Legal and Regulatory for Dun & Bradstreet, Mary O’Leary.

Finally, we publish the results of an online survey conducted in January-February 2016 by Service Excellence Consulting, in conjunction with WorkPro of 1800 individuals about their understanding of privacy. The results show that despite all the attention given to privacy in the last few years, there is plenty of room for improvement in the level of awareness and understanding of privacy in relation to personal information and for businesses to clarify privacy controls and provide adequate training.

In our next journal edition, we will report on PAW and Privacy Week events and as always, welcome member contributions on any insights or learnings that we can share.

For now, enjoy all things privacy in the next few weeks!

Anna

Foreword

By Anna Kuperman
(Joint) Vice-President
A message about iappANZ membership:

Membership benefits

iappANZ has grown into the pre-eminent forum for people with an interest in privacy in Australian and New Zealand, offering our members a wealth of opportunities to expand their privacy knowledge, compliance, interests and networks. We continue to work with private entities across all industry sectors as well as regulators in both countries.

As an iappANZ member you are entitled to receive a range of great member benefits as outlined at: www.iappanz.org.

Through our affiliation with the global body, the International Association of Privacy Professionals (iapp), you are also entitled to additional member benefits, including the knowledge and resources located within the members’ only area of the iapp website at: www.privacyassociation.org.

You can access benefits available to you through your iapp account. Simply login to your MyIAPP account using your email address as the username. If you do not yet have a password or have forgotten yours just click on the ‘Reset your password’ link and instructions on how to create a new password will be sent to you. If you don't want us to confirm your membership details to iapp in accordance with iappANZ's privacy policy, please let me know by emailing me at emma.heath@iappanz.org.

I hope that access to these additional privacy resources will be of benefit to your work as a privacy professional.

Emma Heath, iappANZ General Manager

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

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

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

Our LinkedIn group is: http://www.linkedin.com/groups?qid=1128247&trk=anetsrch_name&goback=.gdr_1281574752237_1

Follow us on Twitter at: https://twitter.com/iappANZ
Privacy Week, Surveillance and the United Nations

by Sam Grover

Privacy week in New Zealand (9-14 May) is here and intelligence, surveillance and privacy are topical issues.

Earlier this year, Sir Michael Cullen and Dame Patsy Reddy finished their independent review of New Zealand’s intelligence and security agencies. They found that current legislation governing these agencies has inconsistent and unclear elements, which make the agencies unsure about what they can and cannot do.

At the same time, a significant number of people in New Zealand are concerned about privacy and security. The 2016 World Internet Project survey found that 32% of the people surveyed were concerned about government surveillance of their online activity. This closely mirrors results from a similar survey we undertook in 2014; the 2016 results will be released this week.

UN Special Rapporteur on Privacy

In order to contribute to the ongoing discussion on these issues, we are pleased to welcome Professor Joe Cannataci, the UN Special Rapporteur on the Right to Privacy, to New Zealand. He is the world’s first privacy investigator at this international level, appointed by the United Nations to the new position in 2015.

For privacy authorities and anyone who works to ensure the security and integrity of personal information, the creation of a rapporteur devoted to privacy is a singular universal elevation of privacy rights. It is more than symbolism; it is a reflection of the growing international convention that privacy is a value that needs special attention in changing world.

As Special Rapporteur, Prof Cannataci has a mandate to review government policies and laws on the interception of digital communications and the collection of personal data. He also has a mandate to help countries develop procedures and laws that are consistent with their international human rights obligations. Prof Cannataci says one of the main areas of his work is to raise awareness among the public.

Since taking up the role in July last year, Prof Cannataci has spoken out about government and corporate surveillance on the Internet and overreaching intelligence gathering. He says proper oversight is the only way. An important piece of his vision is a universal Geneva Convention-style law that safeguards people’s digital information.

We are looking forward to Prof Cannataci’s visit to New Zealand and hearing his views on surveillance and oversight. We expect that he will add a significant amount of insight to the New Zealand discussion on these issues.

Oversight of intelligence gathering

Public attitudes towards surveillance and the independent review indicate that oversight of intelligence and surveillance agencies is a critical part of the privacy discussion. Effective oversight helps allay individual concerns, as well as providing an incentive for agencies to seek the clarity they need about where their powers end.

The Privacy Commissioner is part of New Zealand’s oversight mechanism, helping ensure that government surveillance and intelligence-gathering powers are used appropriately and lawfully.

There have been parallel debates and a discernible movement by our Five Eyes partners - the USA, Britain, Canada and Australia - towards more formalised oversight of intelligence agencies and their legal obligations.

This gives surveillance and intelligence an international context. Since global surveillance and intelligence agencies work together, then so too should the oversight bodies tasked with monitoring these agencies.

As a global collaboration with other regulators, Privacy Week forms part of this approach. By working formally and informally with other regulators, we develop relationships and open lines of communication that can strengthen international oversight efforts in the future.
Privacy Week

Prof Cannataci’s visit is one part of a wide range of activity during Privacy Week. There are a significant number of other activities to help raise awareness of privacy:

- Two Technology and Privacy Forums in Wellington on 9 and 10 May. These are free presentations from experts in the technology field.
- Privacy Forums in Wellington and Auckland, on 11 and 12 May (respectively). Prof Cannataci will be speaking at these forums, as well as a variety of other speakers such as Australian Information Commissioner Timothy Pilgrim (Auckland forum only).
- Right to Know Day on 12 May. This is New Zealand’s first Right to Know Day, designed to raise awareness of people’s rights to access and annotate their own information that agencies hold.
- The launch of AboutMe on 12 May. This online tool helps people request their personal information from agencies by creating a templated email with all the relevant information they need to make a clear request.
- A privacy art project throughout the week. We have worked with a number of art galleries to commission art with a privacy theme. We will be displaying these artworks every day during Privacy Week.

Sam Grover is Communications Adviser at Office of the Privacy Commissioner, New Zealand
A message from Timothy Pilgrim, Privacy Commissioner and Acting Information Commissioner (Australia)

Well, this month we are all about Privacy Awareness Week (PAW), which is just around the corner. This year's PAW theme, privacy in your hands, reinforces the message that organisations, agencies and individuals must be vigilant in maintaining a good understanding of their rights and responsibilities for the handling of personal information.

For organisations, that means incorporating privacy into strategic planning, making privacy a governance priority, and taking a ‘privacy by design’ approach to integrate privacy management into all projects, products and practices that deal with personal information.

We will be releasing a range of publications and facilitating events and activities to help organisations reach their full potential in this regard — not to merely meet compliance with regulation, but to achieve their best possible privacy practice.

The week will kick off with the our most exciting PAW breakfast yet, with special guest Professor Joe Cannataci, the United Nations Special Rapporteur for Privacy. Professor Cannataci’s awareness-raising visit to Australia will provide a number of interesting opportunities — in addition to the breakfast, Professor Cannataci will be speaking at a public event at ANU and participating in a number of media interviews throughout the week. With a background in information and technology law, and a long career in European privacy, Professor Cannataci will provide a global perspective on privacy issues of interest to us all.

Then throughout the week we will be launching a range of resources, including on rights to access and correction, resources specifically for parents and young people, and a template for developing a privacy management plan.

A privacy management plan is key to helping you meet your privacy governance obligations, as outlined in our Privacy management framework (Framework). The Privacy management plan template is a companion piece to the Framework, to help your organisation both address and comply with it.

With the template we are continuing our conversation about privacy governance, but in a lot of the other work that we are doing at the moment we are talking specifically about the intersection between privacy and technology.

During PAW, we also want to continue the conversation on how the APPs apply in the big data context. As we all know, big data, and technology more generally, has become this era’s major issue for privacy. As information gathering increases, changes, aggregates and is analysed, it has become essential that all users of information — business, government, the tech industry, academics, lawyers, individuals... — take part in the conversation on how to address the challenges that arise... So stay tuned.

And finally I would like to close by encouraging all organisations to sign up as a PAW partner — this is a simple way to publically show your commitment to privacy. So, get onto the PAW website, get involved, and I hope to see you there.

For a limited time, we are offering a 10% discount on tickets for a full table of eight people for the breakfast.

To register for the Business Breakfast, become a PAW partner or to simply find out more about the week’s events, please visit www.oaic.gov.au/PAW

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

[Editors’ note: Privacy Awareness Week in Australia is from 15 to 21 May 2016, following Privacy Week in New Zealand from 9-14 May 2016].
Keeping promises to look after customer information

by Dawn Swan and Katherine Gibson

If customers are to have trust and confidence in an agency to look after their information then the privacy and security functions must work together – that was the key message from all speakers at recent iappANZ events in New Zealand.

The seminar, Aligning Privacy and Security, was held in Wellington and Auckland during April. Speakers were from the Office of the Privacy Commissioner (OPC), NZ Intelligence Community, Microsoft New Zealand and Spark New Zealand.

We all know that privacy and security responsibilities are often split between two separate functions: security managed by IT, and privacy managed by the legal or compliance teams, each with their competing demands where achieving a balance can be a challenge. However, aligning security and privacy functions is crucial to achieve comprehensive compliance and can be enabled by effective collaboration.

Some key “take homes” from the seminars included:

- Recognise that privacy and security are co-dependent and the sum of the two functions will be greater than if the functions act alone.
- Consider reframing privacy compliance and technical security standards as promises organisations have made about protecting customer information.
- Privacy can provide a framework for security and security enables privacy.
- Decentralising the privacy and security functions into the business may assist in achieving alignment.
- Working together can be achieved by having respect for each other’s subject matter, recognising there is some fluidity between functions and agreeing common ground.
- It is all about how people in organisations work and they must know what to do and not to do – so get those information security policies out of the cupboard and make them easily accessible and searchable. Forget the old manuals!
- It’s old news, but it is still happening – emailing spreadsheets, inadequate security on BYOD and “doing business in cabs”.
- Stop talking about security and privacy as compliance functions – instead recognise that they are core business enablers that are critical foundations to managing data and information as a strategic asset.
- Change the objective from achieving privacy and security “compliance” to ensuring organisations can give the appropriate “assurances” to customers about keeping their information safe.

Tim Henwood, Senior Policy Adviser, Technology, at the OPC, in Wellington said agencies entrusted with information must do what they can to look after it and privacy and security go hand in hand. “Security and privacy professionals have a lot to learn from each other. Security people have been dealing with privacy before the C-Suite got involved to use it for executive decisions”.

This message was echoed in Auckland by Sarah Thompson, Policy Adviser (Special Projects) at the OPC who cautioned “even with the forces of privacy and security combined, we still get bogged down with lawyers focusing on black letter legal interpretation or security professionals fixating on technical standards” which is not “always that accessible or persuasive to anyone who is outside the privacy/security bubble.”

The OPC is encouraging agencies to consider reframing privacy and security as promises made by organisations rather than legal requirements or technical standards. Tim said “When you make promises about the collection of personal information, you enter into a relationship with your customer—what promises have you made and what more can you do to keep them?”

It is all about customers having confidence in how agencies manage their information. Both Sarah and Tim noted the synergies to be achieved here - privacy can provide a framework for security and privacy needs security to be successful and together these things are greater than the sum of the parts.
This was clear at Microsoft New Zealand, when legal counsel Michael Brick, said that trust is the foundation of customer relationships and Microsoft sees privacy and security as a crucial dependency. “People won’t use technology they don’t trust.”

Microsoft has evolved from a software provider to an online service provider and Michael said it is ultimately a security company. More than 100 privacy professionals employed at Microsoft acknowledge that privacy and security is partly compliance but it’s also about building trust of customers.

Microsoft’s relationship with customers focuses on six key privacy principles: Control (customers are in control of their own privacy with easy-to-use tools and clear choices); transparency (being transparent about data collection and use); security (protecting data through strong security and encryption); strong legal protections (respect for local privacy laws and fighting for legal protection of privacy as a fundamental human right); no content-based targeting (not using personal content to target ads); benefits to you (using data to benefit customers).

Michael said Microsoft was an early advocate and influencer of privacy by design which it applies to products and how the company operates its services. It also has security by design as it evolves to an online service provider. When developing new systems, it has a Security Development Lifecycle which is a company-wide mandatory development process that embeds security into every phase of the developing process.

“Security enables privacy and there is a partnership with the privacy and security teams. A lot of security is automated, so there is a different mind-set which is not just focused on managing personal information. Privacy is more nuanced and requires a human touch.”

One of the ways Microsoft ensures privacy and security work together is through a decentralised structure where the privacy professionals sit alongside the security professionals in the product team “and not in their own ivory towers”.

In a New Zealand context, Sarah Auva’a, Head of Compliance & Privacy and Joshua Bahlman, Manager Security Services at telecommunication company, Spark, agreed and said customers get to tell you if you’re not doing it right.

“Customers and stakeholders play a major role in driving privacy policies and providing a seamless customer experience.” They noted there used to be separate requirements for privacy and security but there is crossover between the two, and they work together to support business needs, and focus on business outcomes.

For instance, Sarah noted that Privacy Act requirements for security can be quite prescriptive, and deciding what a reasonable safeguard is can be difficult without security advice and support.

At Spark, Sarah and Joshua have formal and informal meetings, agree on common ground, have comfort there is some fluidity between functions, and respect each other’s subject matter expertise.

They also share objectives, for instance protecting privacy with security safeguards, limiting access to information to those who need it, being made aware of unauthorised disclosures, and work to shut down unauthorised access as soon as possible.

Sarah said it was like a jigsaw puzzle – each issue is like finding the right place for a piece of the puzzle. The privacy and security professionals both have different skills and expertise, yet they are both working on the same piece of the puzzle and they both need to put that piece in the right place of the puzzle to achieve the right outcome for the business.

In the government sector, New Zealand’s core public sector agencies are required to report on privacy and security maturity using two frameworks: privacy and Protective Security Requirements (PSR). Protective security is about protecting people, information and assets. Good security practices assist with the protection of privacy.

Andrew Annakin from the Intelligence Community explained that PSR and Government Chief Privacy Officer (GCPO) frameworks were established after high profile data breaches in 2012 highlighted a lack of support for agencies, out of date standards and that security and privacy were not being seen as business enablers.
Both frameworks are risk-based and have online tools for agencies to self-assess maturity. The PSR framework focuses on governance, and physical, personnel and information security. It is supported by an outreach capability to support implementation and regular reporting from agencies on capability improvements. However Andrew emphasised this is not a “cookie cutter” solution as every agency is different. What does apply to every agency however is the need to change the question from what we need to do to “comply” with our privacy and security obligations to what “assurances” can we give to people about keeping their information secure.

Andrew says the PSR is “big on governance and a lot of energy has been put into building a strong security culture”.

“Good security practices assist with privacy protections. You need to understand current capability, where you want to be and fill in the gaps.” The PSR tool assists with that assessment and is also available for private sector agencies to use.

Andrew said the PSR team works with the GCPO to provide clear and consistent expectations so that agencies understand that privacy and security are critical foundations to manage data and information as a strategic asset.

Andrew says it provides a “value set for trust and confidence which was rocked in 2012 in the public service” and allows agencies to determine where their weaknesses are, “you can fix problems quickly if you know the environment.”

Under the frameworks, accountability for privacy and security rests with Chief Executives.

“Public trust and confidence in the way that government manages data and information is critical to achieving the business and service transformations needed to enable economic and social outcomes for New Zealanders.”

The first self-assessments in privacy and PSR were completed at the end of March and both the PSR team and GCPO will report to Ministers on capability in June. This will provide a new baseline for privacy and security in New Zealand and ultimately increase trust and confidence for customers and in customer-centric services.

All of the speakers were clear that in order to be successful in gaining customer confidence and trust, you needed to understand the importance of customer information and customer expectations. Having privacy and security functions collaborate is important to that success.

Finally, we leave you with a useful “house” analogy given by the Spark presenters:

Security is like my house. My house has a 20 foot barbed wire electrified fence.

Privacy allows me to give access to this house and certain parts of it to the people who I want to access my house, and also protect parts of my house I don’t want people to have access to.

The Cops: They don’t have access to my house, but may need it. How should they get access to my house? Knock the door down? Or ask for access?

Dawn Swan is Privacy Officer at Inland Revenue NZ in Wellington, and Katherine Gibson is Director, Gibsons Law Limited in Auckland. Dawn and Katherine are both members of iappANZ’s New Zealand subcommittee.
Decision in Hulk Hogan sex tape case places limits on freedom of the press in America

by Tarryn Wood

In what has become a highly publicised case, Hulk Hogan, whose real name is Terry Bollea, has successfully sued the owner of gossip website gawker.com, for invading his privacy by publishing a video of Mr Hogan having sex with a friend’s wife.

The encounter between Hogan and the former wife of his former friend, Bubba the Love Sponge Clem (yes, that is his legal name) took place in the mid-2000s and was filmed by Clem. The full thirty minute video was leaked to Gawker Media in 2012 by an unknown source, and went viral after Gawker Media published edited excerpts on its website.

Hogan testified that he was not aware that he was being filmed at the time and a sought to draw a distinction between the public persona of the character “Hulk Hogan” (see photo at right), and the privacy of Terry Bollea, private citizen (see photo below).

Mr Hogan also said that Gawker failed to contact him before publishing, and contended that the video was not newsworthy.

Lawyers for Gawker Media invoked the First Amendment and argued that they were entitled to publish the video in circumstances where Mr Hogan had himself brought the subject of his sex life into the public arena on numerous occasions.

Mr. Bollea’s lawyer countered that if there was one thing America’s founding fathers did not have in mind when they wrote the First Amendment, it was “uncensored sex tapes and secretly filmed private conversations in a bedroom.”

Ultimately, the jury found in favour of Mr Hogan and awarded him US$115 million in compensatory damages – US$55 million for economic loss and US$65 million for emotional distress – as well as an additional US$25 million in punitive damages.

What would happen in Australia?

The level of damages awarded to Mr Hogan differs markedly from the AUD$40,000 that Ms Giller was awarded by the Victorian Court of Appeal in Australia in 2008 after her former partner showed videos of them having sex to her family, friends and employer.1 There the Court found that the former partner’s actions amounted to a breach of confidence, but avoided the issue of whether a tort of invasion of privacy should be recognised in Australia.

Indeed Australia has not recognised a right to personal privacy to date. This is despite numerous inquiries by the Australian Law Reform Commission and state law reform commissions on the issue and a scratching of the surface by the Queensland District Court in Gross v Purvis.2

For now, breach of confidence remains the only possible avenue for Australians seeking redress for a breach of their privacy, and damages are highly unlikely to ever reach the heights of these awards in America.

---

1 Giller v Procopets [2008] VSCA 236
2 [2003] QDC 151
What’s next?

There is still a lot to play out in this saga, as Gawker has already filed motions for a new trial or for the damages award to be vacated or significantly reduced in the alternative. There are also suggestions that contrary to his evidence, Mr Hogan may have in fact known he was being filmed. However the consensus among most commentators in the US seems to be that while the damages are likely to be reduced on appeal, the decision will nevertheless stand.

This comes on the back of sports journalist Erin Andrews being awarded US$55 million for invasion of privacy after nude photographs were taken of her while she was in her room at a hotel and subsequently published on the internet, going viral. Although Andrews’ suit was not against a media outlet, she successfully argued that public figures are still entitled to their privacy.

This marks a significant shift in America, with the court giving a clear message that even freedom of speech and freedom of the press have their limits.

Tarryn Wood is Corporate Counsel, Southern Cross Austereo

---

3 Andrews sued the man who took the photographs (who was also found guilty) as well as the hotel whose employees told the man what room she was staying in.
In this month’s edition we profile Mary O’Leary, the award-winning Director of Legal and Regulatory for Dun & Bradstreet’s Australia and New Zealand businesses (D&B).

Mary leads the in-house legal team, providing critical support to D&B as it evolves in response to the opportunities and challenges that come with being in the business of enhancing the financial health of its clients. Mary loves communicating in a way that people connect to, making her D&B’s informal “Privacy Queen”.

We’ve referred to Mary as “award-winning” – and here’s why!

In 2015 Mary won the Victorian ICT/Telecommunications Team Award from the Australian Institute of Project Management for Dun & Bradstreet’s multidisciplinary approach to its Australian and New Zealand Privacy Compliance Program refresh. That is the sort of achievement that we love to hear about at iappANZ.

Also, this year Mary won the Asia-Pacific General Counsel Award in Regulatory (Financial Services) conferred by the International Legal Office in collaboration with the Association of Corporate Counsel.

As well as dealing with “big data”, Mary has almost 20 years’ experience in the energy, gas, government, healthcare, pharmaceutical and telecommunications sectors – as well as being a graduate of the Australian Institute of Company Directors and having formal qualifications in law, psychology and corporate governance.

We caught up with Mary at the recent iappANZ mandatory data breach reporting seminar in Melbourne, where Mary asked some particularly good questions! Now it’s her turn to answer some of our questions ...

**How did you get into privacy? Was it choice or chance?**

Before I graduated I was fortunate to work for the ACCC, so working with consumer protection and marketplace economic issues has been the background to my entire legal career. As businesses and life generally have become more data driven, being involved in balancing consumer and industry interests in the context of privacy has been a natural evolution for my career and a rewarding journey.

**What do you enjoy the most about your job?**

As Dun & Bradstreet is involved in commercial credit insights, consumer credit insights, debt collection and marketing solutions, privacy law questions come up everywhere. What I enjoy the most is working with quality people within Dun & Bradstreet who are technology, data and solutions specialists keen to innovate, as well as engaging with industry associations and regulators to explore what the future of privacy law might be.

**What do you see as the biggest challenges for privacy professionals right now?**

The pace of technological change is always accelerating, and the situations for the application of law are increasingly new, novel and different. Where people want either a legal “yes” or “no”, taking the time to crystal ball gaze, understand commercial alternatives and predict the practical knock-on impacts of a decision becomes critical. Doing this quickly in a changing landscape is the biggest challenge.

**Do you have any tips for young players - people who are just starting out in privacy?**

Connect with others to share insights through iappANZ, law societies and the Association of Corporate Counsel as well as industry bodies for industries that you work in. Just listening to the way others have solved problems inspires creativity.
Can you share with us something quirky about you?

I will do anything to promote privacy education. As proof of how far I will go, I dressed up as D&B’s internal “Privacy Queen” as part of our awareness program for privacy law change on 12 March 2014.

While I won’t be donning a queenly outfit again for PAW, I would love to remind everyone that checking their credit file is a great way to prevent against identity theft and fraud. There are a range of free and paid services available to obtain your personal credit information. Checking your own information won’t affect your credit score, and the information you’ll get from credit reporting organisations is impartial - they don’t make credit decisions, their role is to take reasonable steps to ensure accurate credit information for the benefit of industry and consumers equally. D&B’s credit reporting services are available from: http://dnb.com.au/personal.html and http://dnb.co.nz/personal.html.

Mary O’Leary in conversation with Carolyn Lidgerwood.
Privacy Survey – how well do you understand privacy?

by Service Excellence Consulting* in conjunction with WorkPro**

In January-February 2016, Service Excellence Consulting, in conjunction with WorkPro, conducted an online survey of 1800 individuals about their understanding of privacy.

The results were surprising and somewhat disappointing.

Privacy affects all individuals - as customers who share their personal information with businesses and services providers; and as employees working in those organisations who collect and use this personal information to provide a service at some level.

The importance of dealing with personal information with care and respect has been raised in recent years. In 2012 there were some amendments made to The Privacy Act 1988, and more recently there have been a host of media stories over breaches of privacy as a result of system hacking, data theft, negligent releases and other inappropriate data practices.

Despite all this attention the results from this survey indicate that there is plenty of room for improvement in the level of awareness and understanding of privacy in relation to personal information.

Summary of findings:

- The "don't knows" were in the outright majority in most of the questions.
- Only 3% of respondents were confident their businesses understands privacy, and even fewer were confident that appropriate data security measures are in place.
- Only 1% of respondents had seen the privacy policy of their business, but strangely
- More than half the respondents had undertaken some form of training on privacy.

The results are so startling, that even considering only the order of magnitude of responses (rather than the actual result), results strongly suggest there is far more to be done to raise awareness of privacy matters by individuals, and for businesses to clarify privacy controls and provide adequate training.

How the survey was conducted

Nine questions were presented on the WorkPro website and over the months of January to February a total of 1800 responses were received. Almost all respondents were engaged as employees or contractors but some were seeking work, and came from across all industries and their roles ranged from blue collar trades to senior management and other professional roles.

The survey consisted of nine questions which were designed to assess:

- their knowledge about how their business should manage personal information; as well as
- their awareness of their rights surrounding how their own personal information ought to be managed.

The questions were:

1. On an individual note, do you feel your organisation or business understands the privacy requirements?
2. Does your organisation have a Privacy Policy?
3. Is there a distinction between privacy and confidentiality?
4. On an individual note, has your personal privacy been breached by an organisation or business?
5. What industry, profession or trade do you work in?
6. Do you think your business has appropriate data security measures in place to protect the privacy of the people you collect information from?
7. Are you aware that organisations and businesses must make their privacy policy available to the public?
8. To which industries, trades or professions does the privacy of personal information apply?
9. Have you ever been trained on privacy management in a work environment?

Q 1: On an individual note, do you feel your organisation or business understands the privacy requirements?

Only 2% of respondents could confidently state that their organisation understood the requirements of the Privacy Act. Over 60% thought (hoped) the privacy procedures should be OK, and a significant 37% did not know. So a total of 98% were not too sure about this at all.

Q 2: Does your organisation have a Privacy Policy?

Only 19 respondents out of 1800 (1%) indicated that they had read their company’s privacy policy.

The Privacy policy is a mandatory document for privacy entities, and it does not exist simply for the customers to read: staff must be thoroughly aware about the company's approach to privacy management.

Perhaps this explains why 98% of respondents were sure that their organisation understood their privacy requirements!
Q3: What industry, profession or trade do you work in?

This lack of awareness about privacy management procedures is even more concerning when you factor in that 93% of respondents work in areas that deal with large quantities of personal, and often sensitive, information. The finance sector (which had over 300 respondents), administrative support staff and medical centres would routinely manage highly personal information including pay records, contact details, and health records.

Q4: To which industries, trades or professions does the privacy of personal information apply?

Respondents tended to expect that all businesses are subject to the Privacy Act. In fact, the Act makes exceptions for businesses with a turnover of less than $3 million, except where the business deals with or trade in personal information, such as recruitment, health and finance, in which case are all subject to the privacy legislation, regardless of their size or turnover.
Q5: Do you think your business has appropriate data security measures in place to protect the privacy of the people you collect information from?

Only 1% of respondents were confident appropriate data security measures are in place. A key element of data security is permissions and access levels granted to individuals: who has full and partial access; how well are access restrictions implemented; how well are passwords controlled; what protocols are in place regarding data edits and data downloads?

A sound privacy management system would be understood by all those who have access to personal information. Does this result indicate a disjuncture between what information that employers are providing and what information employees are retaining? Are companies failing to have adequate systems in place? Or is it that their employees don't know about them?

Either way, there appears to be a large risk here.

Q6: Have you ever been trained on privacy management in a work environment?

It is somewhat reassuring to note that 56% of respondents indicate that they have received some training in privacy. But if 56% have been trained, then why did 99% state earlier (Q2) that they have never even seen their company's privacy policy?

This indicates significant gaps in knowledge and begs the question: what kind of training was provided and how long ago was it delivered?

Have these organisations been regularly monitoring and updating their employees' understanding of the company's privacy procedures? Have they taken the approach of “I told you once and that should be enough”?

Or have they failed to provide proper training altogether?
Q7: On an individual note, has your personal privacy been breached by an organisation or business?

4 respondents indicated their personal privacy has been breached by an organisation or business. A further 452 indicated that their privacy may have been breached but they weren't very sure.

No one should have their personal privacy compromised, and businesses must be aware that individuals can lodge complaints with the OAIC if they believe that there has been a breach in the management of their personal information.

However, the fact that 452 respondents were not sure leads to another question: do they know and understand what their privacy rights are in the first place?

Q8: Is there a distinction between privacy and confidentiality?

The purpose of this question was to determine the level of understanding of the concept of privacy. Whilst the terms are often used interchangeably, technically the term "privacy" relates to personal information as described in the Privacy Act, and "confidentiality" relates to protecting information which relates to the business (strategic and commercially sensitive information about a business and information about individuals managed by lawyers and health practitioners). It was assumed that a strong understanding of the privacy concepts might differentiate between these two terms. A significant portion of respondents indicated there is a difference - our next question would be to ask what the difference is.

Q9: Are you aware that organisations and businesses must make their privacy policy available to the public?

To end on a positive note, it is pleasing to see that most respondents were aware that their privacy policy must be made publicly available.

It remains to be seen whether this translates in reality: does the company have privacy policies? Are they available in multiple formats? Are they located in an easy-to-find location on the website?

Conclusions
The Privacy legislation has been around for over 20 years. But it just now seems to be waking up. The dual threats of cyber hacking and of poor data management will no doubt continue to grow, and more stories of breaches will hit the headlines. More legislation and controls may yet emerge and impose even more obligations on businesses that handle personal information. Individuals, both as customers who share their personal information with businesses and services providers; and as employees working in those organisations who collect and use this personal information, will need to learn far more about how to manage data better.

This survey indicates that we all need to do far better than we have to date.

The federal government will soon be considering whether to implement mandatory data breach notifications for serious breaches of privacy. It would require all privacy entities to notify both the privacy regulator (the Office of the Information Commissioner) and the affected individuals when a breach occurs.

Your company’s reputation will take a big blow if these laws come into effect and you are forced to explain a breach to your clients.

And even if it doesn’t? Customers and employees can still lodge a complaint with the OAIC that their personal information has been mishandled. The Information Commissioner can determine whether or not he wants to open an investigation into the matter and this too, will be publicly listed on the OAIC website and news bulletins.

Privacy and the management of personal information is an issue that has always been bubbling just beneath the surface. But as we hurtle further into the technological era and struggle with data controls and security, this issue could explode.


SEC works with service businesses to help them improve the management and delivery of services. They have over a decade of experience in quality management, privacy management, safety management, and in improving business processes. They offer health checks and certification of business practices including privacy management. SEC is the expert adviser on quality and compliance management in the recruitment industry. SEC can be contacted on 03 9555 3877 or info@seconsulting.com.au.


WorkPro is a web-based employee screening and induction solution that gets individual’s ‘work ready’ quickly and simply. Providing services across Australia and New Zealand, WorkPro aggregates work health and safety e-learning, licence/ticket management and on-demand background screening in a single platform. Utilised by more an 1 million individuals and partnering with over 800 customers, WorkPro is committed to keeping compliance simple one login, one password, one destination. WorkPro can be contacted on 1300 975 776 or info@workpro.com.au.
# Events

<table>
<thead>
<tr>
<th>Where and when</th>
<th>Event details</th>
<th>Price</th>
</tr>
</thead>
</table>
| **WELLINGTON and AUCKLAND**  
Wednesday 11 May  
8.30am – 12.40pm  
Intercontinental Hotel  
2 Grey Street  
WELLINGTON  

Thursday 12 May  
8.30am – 12.40pm  
Crowne Plaza  
128 Albert Street  
AUCKLAND | **Privacy Commission – Te Mana Matapono Matatapu Privacy Week 2016 (9-14 May)**  
"Privacy in your hands"  
UN Special Rapporteur for the Right to Privacy.  

Professor Joseph Cannataci, will be visiting New Zealand during Privacy Week this year and will give keynote presentations at the New Zealand Privacy Commission's Privacy Forums in Wellington and Auckland.  

The Privacy Forums are at the Intercontinental Hotel in Wellington on 11 May and at the Crowne Plaza Hotel in Auckland on 12 May. | FULLY BOOKED |
| **BRISBANE**  
Tuesday 17 May  
12.00pm for a light lunch  
12.30pm start – 2.00pm finish  
Corrs Chambers Westgarth  
Level 42, 111 Eagle Street  
Brisbane | **iappANZ Training Workshop**  
**Data Security and Data Breach -Protecting Your Critical Data**  
Queensland’s Privacy Commissioner Philip Green will open this workshop during Privacy Awareness Week which puts the spotlight on data protection, compliance and proposed legislative changes.  

This is an interactive training workshop. Learn how to protect and respond to cyber attacks and data breaches. Hear about legal obligations in respect of a cyber attacks and data breaches including the proposed new Mandatory Data Breach Notification legislation. We will cover commercial law, directors’ duties, continuous disclosure rules APRA standards, cyber risk and insurance options.  

**Panelists include:**  
Helen Clarke, Partner, Corrs Chambers Westgarth,  
Martin Holzworth, Director, Advisory, Ernst & Young,  
Susan Elias, National Manager FINPRO, Cyber, Marsh,  
Van Karas, Director, Shred-X Document Destruction.  

**Chair - Emma Hossack**, CEO Binder, President Medical Software Industry Australia, iappANZ Director and former President. | FREE to iappANZ members  
$99 incl. GST for non-members  
[Register here](#) |
<table>
<thead>
<tr>
<th>LOCATION</th>
<th>DATE</th>
<th>EVENT DETAILS</th>
<th>RSVP</th>
</tr>
</thead>
<tbody>
<tr>
<td>MELBOURNE</td>
<td>Thursday 19 May 4.30pm – 6.30pm</td>
<td>iappANZ Privacy After Dark networking</td>
<td><a href="mailto:Emma.heath@iappanz.org">Emma.heath@iappanz.org</a></td>
</tr>
<tr>
<td></td>
<td>Arbory Bar &amp; Eatery Flinders Walk between Flinders Street Station and the Yarra River</td>
<td>Come and join us for a casual get together of people with an interest in privacy during Privacy Awareness Week.</td>
<td></td>
</tr>
<tr>
<td>ADELAIDE</td>
<td>Thursday 9 June 4.00pm for 4.30pm start 6.30pm finish including networking</td>
<td>iappANZ Mandatory Data Breach Notification training workshop</td>
<td><a href="mailto:Emma.heath@iappanz.org">Emma.heath@iappanz.org</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mandatory Data Breach Notification Law: What is being proposed and impacts.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Speaker information to be announced shortly.</td>
<td></td>
</tr>
<tr>
<td>SYDNEY</td>
<td>Monday 14 November 8.30am – 6.20pm incl. 1 hour networking Dockside, Darling Harbour</td>
<td><strong>SAVE THE DATE</strong> iappANZ TRUST IN PRIVACY Summit</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Are you up to date with the latest privacy trends, developments and issues? Are you interested in hearing from some of the world’s leading privacy thought leaders? Do you want to network with like-minded privacy people?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Come and join us for a day of insightful information and discussion on the key issues regarding privacy now and into the future.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Speakers and program agenda to be announced shortly.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Summit enquiries: <a href="mailto:Emma.heath@iappanz.org">Emma.heath@iappanz.org</a></td>
<td></td>
</tr>
</tbody>
</table>
IAPP Certification

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

Our global body, the International Association of Privacy Professionals (iapp) says:

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

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

Currently, the iapp offers six specialised credentials, two of which are particularly relevant to iappANZ members, namely the Certified Information Privacy Professional/ Information Technology (CIPP/IT) and the Certified Information Privacy Manager (CIPM).

To achieve either of these credentials, you must first successfully complete the Certification Foundation. The Certification Foundation covers basic privacy and data protection concepts from a global perspective, provides the basis for a multi-faceted approach to privacy and data protection and is a foundation for the distinct iapp privacy certifications.

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

What about testing?

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

Employment opportunities for privacy professionals

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

No current listings
Our contact details

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

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

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

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