President’s Letter
By Anna Kuperman
President
M: 0419 803 263

Dear Members

Welcome to our Privacy Awareness Week 2015 journal edition.

On behalf of the iappANZ Board and all of our Australian and New Zealand Sub Committee Members, I would like to thank all of our members who supported our events and contributed to our discussions in each of the Melbourne, Sydney, Auckland and Wellington sessions. It was certainly Privacy everyday in the PAW event planning camp and I extend my gratitude to all of our sponsors, event hosts and members for continuing to support us.

During a very busy week filled with a multitude of (often simultaneous) privacy gatherings, we are proud that each of our events had capacity audiences and our guests had time to engage with our guest speaker, Professor Cate, local privacy regulators, specialists and commentators. Professor Cate surpassed our great expectations during his ANZ road-show of 4 cities, 2 countries in 5 days by bringing insightful commentary on managing privacy in a digital world with great humour and personality. We are fortunate to have had his support during the week and hope to have him visit our shores again. In fact, we increased the odds of his return by gifting him with a Taronga Zoo sponsorship of a platypus!

To wrap-up, below is a snapshot of some key releases and messages during PAW 2015.

• ‘Privacy – living in the future’, OAIC releases a privacy management framework that is designed to assist organisations to take reasonable steps, as required under APP 1.2, to implement practices, procedures and systems that ensure compliance with the APPs. Commissioner Pilgrim expects all organisations bound by the Privacy Act to make a commitment to implement the framework.

• Commissioner Pilgrim releases the results of a privacy assessment under section 33C of the Privacy Act of the online privacy policies of 20 APP entities against the specific criteria set out in APP 1. The assessment covered all four major banks, technology companies, media companies and government departments. The results were that while 55 per cent of the entities had privacy policies that did not adequately address the
content requirements in APP 1.4. Specifically, some of the privacy policies did not:

- outline how an individual can request access or correction of their personal information;
- outline how the organisation would deal with a privacy complaint it may receive;
- adequately describe how they protect the personal information that they hold; or
- outline whether the organisation was likely to disclose personal information overseas and the countries in which such recipients are likely to be located.

The OAIC conveyed that the next spotlight will be on websites and mobile apps to assess the extent to which 44 websites and mobile apps targeted at children aged 12 and under protect privacy. As part of this assessment, the OAIC will be looking at whether such websites and apps:

- collect children's personal information and, if so, whether protective controls exist to limit that collection;
- seek parental involvement;
- allow users to be redirected off the site;
- make it easy to delete personal information; and
- whether any privacy communications are tailored to the age group through approaches such as simple language, large print, audio or animation. The results of the audit will be made publicly available later this year.

Finally please follow these simple steps:

1. Open your calendars.
2. Open Wednesday 18 November 2015.
3. Create new entry for All Day Event – iappANZ Privacy Summit PRIVACY@WORK (Enter Location: Zinc, Federation Square Swanston Street & Flinders Street Melbourne CBD)
4. Look out for Early Bird Registrations – coming SOON!

Happy reading, Anna
This month, we congratulate Alex Bayley, winner of a complimentary ticket (plus flights and accommodation) to this year's iappANZ Summit in Melbourne on 18 November. Alex entered a winning business card into the iappANZ draw at the Identity Conference 2015 in Wellington on 18 and 19 May.

We hope you too can join us at Zinc, Federation Square Melbourne for the iappANZ's 2015 Privacy Summit. Stay tuned for details of our early bird tickets.

This month's Privacy Unbound kicks off with our usual Questions for the Privacy Commissioner, Timothy Pilgrim. This month, he reflects on the OAIC's fully booked Privacy Awareness Week (PAW) events. We also ask him about the response he has had to the Grubb v Telstra decision and the work of his office over the coming year.

In the next feature article Diane Gibert looks at the significant challenges that recruitment agencies face in managing the large quantities of personal information they collect. Having assisted many agencies to develop privacy management systems and data cleansing procedures, Diane shares her insights on the unique challenges facing recruitment agencies and offers a case study on data cleansing.

Then you can be regaled by the memories of PAW with our write up of events in Sydney, Melbourne, Wellington and Auckland. We highlight some of the key events and contributions of our international guest Prof Fred Cate, as well as a range of other illustrious panellists. Fred has also contributed a feature article on "Big Data and the Future of Data Protection" (read on for more).

Read on to learn about why Marie Shroff was recognized by iappANZ during PAW as its inaugural Privacy Hall of Fame recipient.

We also have some reflections from David Gerber and Dr Mark Wiese on cyber risk management, privacy and insurance, specifically on the growing recognition in Australia of the widespread risk to Australian businesses of all sizes of cyber-attacks and data breaches. They detail the potential costs of a cyber-attack or data breach, involving possible breaches of privacy laws and outline the ins and outs of cyber risk insurance policies.

Turn to our next report from inaugural NZ Subcommittee Chair, Emma Pond to find out about the three strategic priorities of that subcommittee, as well as profiles on each of its stellar members: Annabel Fordham, Tom Bowden (iappANZ Board director), Jacqui Peace, Dawn Swan, Daimhin Warner, Katherine Gibson and Ella Biggs who are all supported by Emma Hossack (current iappANZ Board director and former President) our ANZ Chair of Strategy, who has been working on the ground in NZ during PAW.

Our next feature article is by international thought leader and iappANZ PAW celebrity Prof Fred Cate. Entitled "Big Data and the Future of Data Protection". Fred suggests key steps that can be taken to deal with the significant privacy issues brought about as a result of the proliferation and interconnection of big data sets.

Finally, Jennifer Mulvaney, Intel's Director of Cloud Policy and Government Affairs in Australia proclaims herself as a “Privacy Paradox” (and also an eternal optimist). Jennifer discusses the significance of trust to Intel's entire business and the way that privacy is physically embedded in Intel's technology, and is as palpable in its culture. She also shares the results of Intel’s recent public surveys on attitudes towards company behavior and what consumers understand about data generally, before reflecting on how this influences her own level of comfort as a consumer.

Will any of these authors be the winner of this year’s writing prize? If you’d like to know (and perhaps assess them for yourself), turn to page 25 for the rules!

We hope you enjoy this edition of Privacy Unbound.

Melanie
A message about iappANZ 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 public entities across all industry sectors as well as Privacy Commissioners 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.

In this context, should you not wish for iappANZ to confirm your membership details 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
We are pleased to announce that Alex Bayley won the iappANZ Business Card prize at the Identity Conference 2015, Enabling digital identity and privacy in a connected world which took place on Wellington on 28 and 19 May.

He is the winner of a complimentary ticket (plus flights and accommodation) to this year’s iappANZ Summit in Melbourne on 18 November.

Alex is the Manager of the 2018 Census, Respondent Focus at Statistics New Zealand. When our General Manager informed Alex of the prize he replied: Thank you for the prize, it will be great to attend the summit and very relevant to my role!
Questions for the Australian Privacy Commissioner

by Timothy Pilgrim, Australian Privacy Commissioner and Melanie Marks

The OAIC organised a number of fully booked events for Privacy Awareness Week (PAW) this year. In this edition, we ask the Privacy Commissioner about the feedback he received during PAW, the response to the Grubb v Telstra decision which was published at the start of PAW and the work his office is doing in the year ahead.

1. During your PAW presentations, what did you find are the kinds of issues on the minds of privacy professionals?

A lot of the organisations that we have been engaging with have told us that law reform implementation has been the focus of their attention over the last 12–18 months. This has coincided with increasing community concern around the rise of integrated technology. This means that privacy is never far from the headlines, so it has really grabbed the attention of the business community.

Over the last year we have worked closely with organisations in many sectors to ensure our guidance is as helpful as possible, and we have given more guidance on issues raised with us, for example the new Privacy business resource 8: Sending personal information overseas.

We have also received feedback that a lot of organisations are very interested to see more case law, more precedent, on how we will interpret the new laws. We publish all my determinations along with enforceable undertakings, so organisations can access those into the future.

Another key issue for all privacy regulators is international interoperability. Businesses are increasingly global operations, working across many countries, whereas privacy regulation is local. This means that business has to adjust to different regulatory frameworks. However, the Office of the Australian Information Commissioner (OAIC) is working more and more in the international arena, engaging on joint investigations and participating in joint awareness campaigns. When we developed our recently released Privacy management framework we were also very aware of the need for it to be interoperable across many regulatory environments.

During PAW, I was pleased to hear a range of questions from organisations about implementing our new framework. People were very interested in how to approach developing a privacy culture and I look forward to seeing the results of an increased focus in this area.

We also saw a great demand for our privacy impact assessment workshops, demonstrating that organisations are determined to get this right and consider privacy by design principles in their project planning.

2. How have you found the response to your decision on Ben Grubb’s complaint?

In Ben Grubb v Telstra Corporation Limited I found that certain customer metadata held by Telstra constituted the complainant’s personal information and that Telstra was obliged to give him access to that information.

I found that Telstra had the operational capacity to extract the complainant’s personal information from its various networks and records management systems and that the complainant was entitled under the Privacy Act 1988 (Privacy Act) to be provided with access.

In terms of any precedential issues rising from this case, whether or not metadata held by an organisation meets the definition of personal information under the Privacy Act depends on the circumstances of each case, subject to variables such as the operational capacity and practices of the organisation which has been requested to provide access.
It is important to note that this determination has no impact on the newly commenced data retention laws which deem a prescribed set of data under that regime to be personal information for the purposes of the Privacy Act.

Telstra has announced that it will be appealing my decision to the Administrative Appeals Tribunal.

3. **You referred to and have released for consultation further chapters on the guide to regulatory action. Can you tell us a bit more about these chapters?**

We are currently seeking public comment on the clarity of the remaining three chapters of the OAIC’s [*Guide to privacy regulatory action*](#). These chapters relate to our privacy complaint handling processes, determinations, and injunctions.

- **Chapter 2: Privacy complaint handling processes** — deals with how the OAIC handles and investigates privacy complaints from individuals as well as representative complaints; how complaints are conciliated and the types of outcomes that can be achieved; when a complaint may be declined and when it may be referred.
- **Chapter 5: Determinations** — deals with when the Commissioner will make a determination; what information will be included in a determination; when compensation may be awarded; and review rights of parties.
- **Chapter 6: Injunctions** — deals with when an injunction may be granted; procedural steps in seeking an injunction; what happens after an injunction has been granted and how the injunction will be communicated.

The guide, when finalised, will provide more detailed information on how the OAIC will exercise its regulatory powers, and, read in conjunction with our [*Privacy regulatory action policy*](#), will be a very useful resource for privacy and compliance professionals in developing and reviewing processes.

The consultation closes on [5 June 2015](#) and I welcome any feedback that you would like to give.

4. **For those of us who didn’t make it to your presentations can you tell us briefly about the matters that you spoke about / were on your office’s agenda for this year?**

We are over a year into the new privacy laws and while we’re expecting organisations to continue taking a proactive approach to privacy we’re also expecting them to commit to robust privacy governance.

Privacy governance is essential to make sure you have the leadership, resources and accountability to put the necessary practices, procedures and systems in place to ensure good privacy management. Our Privacy management framework will assist organisations develop, implement and review their privacy management program and related governance structures, to help organisations meet their ongoing compliance obligations and embed a culture of privacy.

The OAIC will continue to develop new resources to assist organisations and provide information and advice. We will also continue to assess organisations’ compliance with the APPs through dealing with individual complaints, data breach notifications, Commissioner initiated investigations and assessments.

During PAW I talked about our assessment schedule, and working with telecommunications providers to ensure that the privacy of individuals’ personal information is protected once the Government’s data retention laws come into force. We are also planning a big year working with agencies from across government on a broad range of privacy matters, including contributing to the Government’s cyber security review, and taking an active role in the implementation of the recommendations that have come out of the review of the eHealth system. We will also be working with the Attorney General’s Department on the development of the mandatory data breach notification scheme.

**Timothy Pilgrim is the Australian Privacy Commissioner**

**Melanie Marks is Executive Manager - Digital Trust and Privacy at Commonwealth Bank and the Vice President of iappANZ**

*If you would like to suggest a topic for an upcoming edition, please email it to [melanie.marks@cba.com.au](mailto:melanie.marks@cba.com.au)*
Data Storage and the Recruitment Process

by Dianne Gibert

Recruitment agencies face a significant challenge in managing the large quantities of personal information they collect. Having worked with many agencies to assist them to develop an appropriate privacy management system and to establish suitable data cleansing procedures, Diane Gibert reviews some of the complexities facing recruitment agencies, and offers a case study on data cleansing.

The Challenge

As we hurtle through the technological era we are inundated with an overabundance of data: it has never been easier to collect, capture and (electronically) store vast amounts of information for a seemingly indefinite period of time.

Managing this vast amount of data with proper respect is the basis for the Privacy Act and the Australian Privacy Principles (APPs). Many industries have access to and use personal information: health services, financial institutions, government – to name a few. The recruitment industry collects and uses quite a range of personal information, including sensitive information.

The Recruitment process – Data Collection

Seen through the lens of privacy, the recruitment industry is very complex: a lot of personal and sensitive information may be collected; sometimes the personal information “morphs” into a record of a business activity which should be retained for business purposes; and sometimes personal information on candidates is retained for extended periods because the candidate may return in the future looking for another job.

When a candidate applies for a job with a recruiter, they will usually start by providing a copy of their current resume. The modern style of writing a resume is to keep it brief, list the activities and responsibilities the candidate has, and their qualifications and skills. This is the information the recruiter needs to identify the type of role they could place the candidate into. The old style of writing a resume is to include interests, contact details of referees, date of birth, gender, marital status and sometimes even the names of children and their ages! This level of detail is not needed and could even provide grounds for accusations of discrimination – “I didn’t get the job because I am too old”, “You don’t think a women can do the job”. Recruiters need to recognise this kind of information as unsolicited, and deal with it according to APP4.

In addition to the resume, a good recruiter will usually ask for evidence of the candidate's skills and qualifications, right to work, identity, referees, contact details, licenses, police records, medical history, work experience and more. Some of this information has to be collected under Australian legislation. Right to work is essential, as it is illegal to employ a worker who does not have the right to work as an Australian citizen or under a current and appropriate visa. Medical history can be very important for certain jobs, as it would be inappropriate to place an asthmatic into a job in a dusty environment, or a person who is allergic to peanuts into a food facility.

Some of this personal information is defined as “sensitive” by the Privacy Act, and other information either on its own or grouped with other information could have serious adverse consequences if misused.

Post-recruitment Data Collection

A recruiter provides a recruitment service to a client. The recruiter always seeks to make a happy match so the client and the candidate work together well and hopefully for a long time; but on occasions this doesn’t work so well. The client may come back and ask the recruiter “what on earth were you thinking when you gave me this person?” The recruiter needs to be able to refer to the records of the candidate interview, comments from the referees, and the other evidence provided to them, and give a proper answer. In addition, some personal information shifts into becoming records of the service and the activity of the business. There might be legislation or service contracts compelling retention of certain business records for certain periods. This can complicate the record retention policy of the recruitment agency - the referenced personal information may be out of date and no longer necessary for the primary purpose for which it was collected, but as a business record it may need to be retained.

One of the reasons that employers seek the services of a recruiter is that the skill set they need is not easy to locate. In the IT industry there are legacy systems that still operate today, built in a code that new the crop of IT graduates haven’t even heard of. An IT recruiter who still has the details of a “DB2 programmer” might be just who you need. However, a direct application of the primary purpose rule might result in the details of the DB2 programmer being deleted many years ago.
Case study – Data Cleansing

The recruitment agency in this case study has been operating very successfully for 25 years. During that time records had been collected from candidates, and everything had been kept in case it was needed again. The records were stored on paper in large boxes and included CVs, police checks, references and other personal and sensitive information.

The volume of records was taking up quite large areas in the office and was even becoming an issue of safety. Much of the information hadn’t been used for many years. The business hadn’t developed a policy on what information it needed to keep or how it should archive or eventually delete or de-identify the information it held. There was a potential for a breach of security or misuse of the data. This had become a real liability for the business, but the business didn’t know where to start and didn’t have the knowledge or the resources to solve the problem.

Our first step was to transfer the paper records to a secured site so the office was immediately relieved of the congestion. Then we reviewed the type of information held and checked against relevant guidelines for record retention such as those set by the ATO, by the industry, by clients and contracts, and by the policies of the business itself. We developed a records table which considered when the candidate has been last placed and the type of information which needed to be retained.

Over the next three weeks the team worked through well in excess of ten thousand records. Some records were scanned and stored electronically; others were binned and disposed of securely. The client was closely involved as there were always exceptions to the rules that had been agreed.

At the same time we worked with the agency to update their privacy policy and collection notice, to document procedures for responding to candidate requests to access or update their data or to lodge complaints. The data cleansing process was fine-tuned and documented. A training program was developed around these procedures and all current staff went through this training.

At the end of the three weeks, the agency was relieved of the stack of out of date information, and had a new process in place to ensure that data was maintained in a manner which was easy to sort and archive or delete as required in the future.

Summary

Whilst it remains a complex industry in the context of managing personal information, it is important that recruiters manage personal information securely and properly. The confidence of both candidates and clients depends on it. There have been a number of cases – mainly private but some public - where legitimate complaints have been raised about the handling of personal information by recruiters. There have also been claims that are not legitimate, but without a good understanding of requirements and clear guidelines, any complaint could cause the business to lose time and money just through the distraction of responding to such complaints.

These challenges apply not just to recruitment agencies, but to all Australian employers who collect the personal information of candidates for the purpose of recruitment. They should all consider how they collect, disclose and use, and cleanse their records for this purpose.

Privacy Awareness Week has offered us a timely reminder of the importance of managing personal information properly and taking appropriate steps to identify data for retention and data which should be destroyed.

Dianne Gibert, MBA AGIA, is the director of Service Excellence Consulting, a consulting company that specialises in recruitment best practice and privacy management. Dianne can be contacted via the website www.seconsulting.com.au
Privacy Awareness Week May 2015

Privacy Awareness Week (PAW) took place between 3-9 May this year. iappANZ, as well as many of our member organisations, were OAIC PAW partners – www.oaic.gov.au/paw

An initiative of the Asia Pacific Privacy Authorities forum (APPA), PAW is held every year to promote awareness of privacy issues and the importance of the protection of personal information. Activities are held across the Asia Pacific region by APPA members.

To mark PAW, iappANZ organised a number of events in Australia and New Zealand. For the first time, iappANZ also arranged for an international privacy expert to join us for the week as our guest, to meet with our members and sponsors and to speak at our events. We are very pleased to report that this was a great success – and the theme for our events was “Privacy Everyday”.

Professor Fred H. Cate

In our last edition, we introduced you to Professor Cate, our inaugural international guest for PAW 2015. He travelled to Australia from Indiana University where he is Distinguished Professor and C. Ben Dutton Professor of Law. He did not disappoint.

Over seven remarkable days Professor Cate travelled between Australia and New Zealand speaking at various events, meeting our sponsors and speaking to the media. Among other things, he:

- was interviewed by ABC Television in Australia for Lateline;
- fielded dozens of questions from our New Zealand members in the “Ask Me Anything” online forum. The questions included, whether he thought Edward Snowden’s disclosures makes him a hero or a traitor in response to which Professor Cate said that he would argue that Snowden is a hero for providing information on surveillance activities that both stretched the limits of the law but also were being actively denied by the US government even before the US Congress. However, at the same time, (while not calling him a traitor for exposing highly classified information) Professor Cate said he is troubled that Snowden disclosed as broadly and apparently indiscriminately as he did, after taking a pledge to follow the law concerning the secrecy of the information he was handling and continues to believe there must have been other ways to focus attention on the extent of the government’s activities. However he believes that there is no question that we are all better off because of the disclosures; and
- spoke to iappANZ Gold sponsor Intel at a lunch following the launch of Intel’s key initiative in support of PAW, its Privacy Research Survey.

iappANZ PAW events

In Melbourne, Professor Cate led a guest panel of speakers at an event hosted by Minter Ellison. Each of Professor Cate, Timothy Pilgrim, Australian Privacy Commissioner and Associate Professor Dr Margaret Simons gave presentations and Carolyn Lidgerwood, Global Privacy Counsel, Rio Tinto and iappANZ Board director chaired the session.

Professor Cate highlighted issues that face us all as privacy professionals. He spoke of how we are now “overwhelmed with data” and how far the world has come since the 1970s focus on data handling by “big companies” using mainframe computers. Professor Cate described “the cult of data” and its new value, and changing attitudes to what privacy actually means. Information sharing is more common now - and while that doesn’t mean people no longer care about privacy, exactly what they care about is different. He also referred to the collection of data by government which he said is driving a privacy debate of its own, and expressed the view that the information he was handling and disclosed as broadly and apparently indiscriminately as he did, after taking a pledge to follow the law concerning the secrecy of the information he was handling and continues to believe there must have been other ways to focus attention on the extent of the government’s activities. However he believes that there is no question that we are all better off because of the disclosures; and

Commissioner Pilgrim provided a practical explanation of how his Office will approach “Privacy Everyday” - by introducing the OAIC’s new publication: Privacy management framework: enabling compliance and encouraging good practice which was launched earlier in the week. The Commissioner emphasised the importance of fostering privacy by design and building a culture of privacy – this is a “bed rock” principle. The Commissioner urged organisations to commit people and resources to getting this right, and also highlighted the importance of governance. It’s not enough just to have a privacy policy – it needs to be implemented and it needs to be monitored. The Commissioner described the very large volume of complaints handled by his office and noted the survey result that 60% of
Australians surveyed have decided not to deal with a specific company because of concerns about privacy. In this context - his observation was that privacy compliance is an opportunity to build customer trust.

Dr Simons then presented interesting observations from her perspective as a journalist – contrasting the Edward Snowdon approach (“without privacy we have no freedom”) with the contrary argument (“what have you got to hide?”). Dr Simons described the practical challenges faced by journalists in protecting their sources citing her own recent personal experience communicating with a source and noting surveillance risks across different communications platforms and CCTV. Dr Simons emphasised privacy as a human right - and the panel discussed whether this had become a “tradeable” human right. She also reminded us that the concept of ‘the public’ as opposed to the private) is a relatively new concept.

A panel discussion then followed – and unsurprisingly, much discussion focused on the definition of “personal information” and the Grubb decision that had been announced the previous day. The Commissioner emphasised the importance of the context for this decision (as he also emphasises in the Q&As for this edition of Privacy Unbound).

In Sydney, Professor Cate was again joined by Australian Privacy Commissioner Timothy Pilgrim, together with Dr Elizabeth Coombs, NSW Privacy Commissioner and Sarah Davis, Director of Commercial Legal Services at Guardian News and Media.

This was a pure “Q&A” event, chaired by Peter Leonard, Partner, Gilbert + Tobin who also hosted the event. A lively discussion covered a broad range of issues, including:

- **Notice and consent**: the whole panel identified privacy policies as a particular area for improvement. The Privacy Commissioner emphasised that privacy policies are still too lengthy. Professor Cate pointed to a 2014 White House 'Big Data' report which recommended that "only in some fantasy world do users actually read these notices and understand their implications." The Privacy Commissioner recommended that organisations should be embracing technology to write privacy statements that are more readily digestible. Professor Cate suggested that notice and consent need to be separated to be effective.

- **General approach of Australians to privacy**: Professor Cate suggested his week in Australia had given him the impression Australians were particularly pessimistic about privacy. He noted that he had heard problems presented throughout the week without the recognition of examples of policy and industry responding to these challenges. Dr Coombs said that in her 3 years in the job, she had seen an increasingly active public interest in the area. Professor Cate queried the value of privacy surveys, suggesting that people know the answers they should give in surveys but, practically, don't care about privacy.

- **‘Personal information’ in the age of the Internet of Everything**: the panel discussed how a static definition of ‘personal information’ was problematic as technology progressed. Ms Davis commented that technological advancement is a major challenge for lawyers and that fixing privacy policies to solve for today likely renders them not fit for purpose tomorrow. Commissioner Pilgrim acknowledged the difficulties of keeping pace with technology but said that he had the power to make privacy codes to extend regulatory coverage to new technology. Professor Cate said the legislative lag was inevitable, identifying an irony in that "laws are passed more quickly when they are hurting privacy."

- **New information sheet on APP 8**: Peter Leonard noted that the OAIC has issued a new information sheet on APP 8 and queried whether it marked an indication that the OAIC was moving towards a risk based approach. The Privacy Commissioner did not confirm this, but emphasised that the underlying concept is accountability. That is, under the Privacy Act, if information is ‘disclosed’ overseas the organisation may be accountable for breaches by the overseas recipient, but if information is ‘used’ instead of being ‘disclosed’ the organisation is still accountable if something goes wrong. The fundamental proposition is that you will remain accountable, so you should put in place appropriate protection mechanisms.

- **Government surveillance**: Sarah Davis suggested that the public’s bargain (accepting surveillance with appropriate oversight) was violated in recent years (The Guardian was influential in the Snowden leaks). Professor Cate said the cause of the problem in the US was not that oversight wasn't used but that it didn't work. The directors of security agencies and judicial officers charged with oversight had, he claimed, “drunk the Kool Aid.” Ms Davis said that regardless of well documented breaches, there was not much public appetite for government surveillance media coverage.

- **EU data flows**: The fact that Australia's privacy law has not been assessed as “adequate” by the Article 29 Working Party was discussed. The Privacy Commissioner noted that in 2005 businesses were asked if this was affecting business and most said it was not an issue. Since then no businesses have made any complaints to his office about this.
- The place of privacy in Australian business: Ms Davis concluded in commending Australian businesses for having managed to make privacy "live in their organisations" rather than sitting siloed with a data compliance officer, as she said too often happens in the UK.

Our thanks to Helen Patterson, Senior Associate and David Seilder Lawyer, Minter Ellison for providing this report on the Sydney session.

More from New Zealand on their PAW events and work next month.

Thank you - Thank you so much to our sponsors, hosts, members, speakers and particularly Professor Fred Cate for making these events such a success. Particular thanks also goes to our General Manager Emma Heath who worked tirelessly behind the scenes.
iappANZ inaugural Privacy Hall of Fame

Marie Shroff announced as the recipient of the 2015 award

During PAW, the iappANZ Board was delighted to recognise Marie Shroff’s substantial contribution to the development of the privacy profession in New Zealand, Australia and globally, by announcing her as the inaugural Privacy Hall of Fame recipient.

Malcolm Crompton, founder and current director of iappANZ and a former Australian Federal Privacy Commissioner commented that:

“Ms Shroff was the pre-eminent privacy regulator in our region. She led by example. She made sure that privacy protection for the people of New Zealand was implemented in a practical and effective way. She was also a global leader in international forums as a voice of reason and commonsense”.

Marie held the position of New Zealand’s Privacy Commissioner from 2003 to 2012. During her time as Privacy Commissioner, Ms Shroff’s major achievements include:

- The strong contribution by her office to the Law Commission’s 2011 review of the Privacy Act, which hadn’t been updated since 1993. The review recommended that the Privacy Commissioner be given more direct power to deal with privacy issues by means of compliance notices when previously, the Commission could only encourage or warn.
- In 2012, the New Zealand Privacy Laws were deemed of high enough standard to be accepted “adequate” within the European Union, making New Zealand only one of five countries outside of the EU to hold this distinction. This translated into easy data flow between New Zealand and EU without controls or regulations.
- As Privacy Commissioner, Ms Shroff was involved with the launch of the Own, Wait, Lock and Safety (OWLS) first program which teaches Privacy Awareness in schools. This built greater general public awareness and as Ms Shroff noted, “a big re-assertion of control by the citizen over the information.”
- In 2012, Marie's office dealt with a number of high profile privacy breaches by agencies and was personally involved in the ACC breach inquiry which she saw as a turning point in privacy in New Zealand, changing the way companies and government value personal information and how they operate to prevent breaches.

Marie Shroff pictured receiving her award with Souella Cumming and Emma Hossack
Cyber risk management, privacy and insurance

by David Gerber and Dr Mark Wiese

In March this year, the Australian Securities and Investments Commission (ASIC) released a report aimed at increasing awareness among Australian businesses of cyber risk and the importance of cyber resilience. ASIC's report reflects the growing recognition in Australia of the widespread risk to Australian businesses of all sizes of cyber-attacks and data breaches. Entitled 'Cyber resilience: health check', the report can be found here.

ASIC's report recognised the potential for a cyber-attack or data breach to place an organisation in breach of Australia's privacy laws. There are a range of potential costs of a cyber-attack or data breach, involving possible breaches of privacy laws. They include the costs to investigate and remedy the breach, interruption to business, public relations costs, the costs of ongoing support to clients or customers, and regulatory compliance costs. Under the Privacy Act 1988 (Privacy Act), the Australian Privacy Commissioner has substantial powers to investigate entities covered by the Privacy Act, whether in response to a complaint or of its own motion. Investigations such as these will give rise to legal and other costs.

Traditional property and liability insurance policies are unlikely to be triggered by cyber risk events, which tend not to involve physical damage to tangible property or physical injury to persons. There may be some limited cover for certain cyber risks through extensions and endorsements to different types of policies. However, that cover may be disjointed or inadequate. It is not uncommon for the policies which form the traditional foundation of a company's insurance protection to have gaps in cover for cyber risks.

Cyber risk insurance policies are designed to deal with cyber risks specifically and broadly. But the nature and extent of coverage can vary significantly. This reflects insurers' different appetites for the risks. It also reflects the fact that the market for this insurance in Australia is relatively new.

Any proposed cyber risk insurance policy needs to be reviewed carefully. The insurance should match the specific risks to which the particular insured entity is exposed. The insurance is usually divided between first party loss (losses incurred by the insured itself) and third party liability (liability of the insured to third parties). First party loss coverage may extend to:

- damage to property, both physical and electronic;
- costs of investigation, remedy, repair, restoration, or replacement;
- costs of regulatory compliance, in terms of notification and investigation by regulators;
- public relations costs;
- costs of ongoing services to clients or customers, for example credit monitoring; and
- business interruption costs.

Third party liability cover may include:

- compensation or settlement of claims against the insured, including in respect of breach of privacy;
- fines and penalties; and
- legal costs of defending claims and regulatory proceedings.

Underwriters may exclude from cover, risks such as exposure to self-replicating viruses and liabilities such as criminal fines and penalties. Other exclusions to note when taking out a cyber risk policy include:

- Unauthorised collection of customer data - a potentially significant limitation on cover for some companies where collection of data is central to the business.
- Contractual liability exclusion - excluding cover for liability assumed under contracts which would not otherwise exist at law. Companies whose contracts with third parties involve cyber related risks (e.g. data hosts) should consider the extent to which they assume liability (e.g. through indemnities).
- Betterment exclusion - excludes cover for costs to restore, re-create or replace systems and software to a higher level of functionality than they had before the loss occurred.

Under section 16C of the Privacy Act, an entity subject to the Australian Privacy Principles (APPs) can be responsible for the conduct of an overseas entity to whom the Australian entity has disclosed personal information about an individual. This can arise where (i) the conduct of the overseas entity would breach the APPs, if they applied to that entity, and (ii) APP 8.1 applies to the disclosure that was made to the overseas entity. Liability under the Privacy Act, including for breach of the APPs, can therefore arise from conduct over which the organisation taken to be in breach had no effective control (even where it has complied with APP8.1 and taken reasonable steps to ensure the overseas entity complies with the APPs).

In principle, cover for liabilities arising in this way can be covered by a cyber risk policy. However, an organisation engaging in cross-border disclosure of personal information to which APP 8.1 applies should consider carefully whether any cyber risk insurance policy it proposes to purchase extends to cover this kind of liability, and whether it does so in all cases. The underwriter of a cyber risk policy is likely to take a close interest in the policyholder’s systems and procedures for mitigating the risk that an overseas service provider will engage in conduct that causes the insured to become liable under section 16C.

**Financial loss and reputational damage**

A significant risk in the event of a cyber-attack or data breach is reputational damage. Policyholders need to understand the type of cover that is available in relation to this risk. There may be cover for the costs of advice and support from a public relations firm and crisis management consultants, engaged to mitigate damage to an organisation’s reputation. However, cyber risk insurance does not indemnify against adjustments made to the organisation’s goodwill asset if it is written down in consequence of an event that is covered by the policy. That is, while cyber risk insurance can assist an organisation to minimise reputational damage, it will not cover actual financial loss to the reputation of the insured.

**David Gerber** is a partner of Clayton Utz and **Dr Mark Wiese** is a lawyer at Clayton Utz.

*Disclaimer: This article is intended to provide commentary and general information. It should not be relied upon as legal advice. The authors may not be admitted in all jurisdictions. Formal legal advice should be sought in particular transactions or on matters of interest.*
Kia ora from NZ!

As the inaugural Chair of the freshly minted iappANZ NZ subcommittee I am thrilled to provide this report for Privacy Unbound, to celebrate what we on the NZ subcommittee all believe is the beginning of a beautiful thing.

While the long distance benefits of iappANZ are nothing to be sneezed at, I think I speak for the majority of our members who live in Aotearoa NZ when I describe the feelings of wistfulness and envy of the opportunities and collegiality our Australian colleagues enjoy through iappANZ being active in their community. When Tom Bowden, CEO of HealthLink Ltd, became the first NZ member elected to the iappANZ board last year at our Summit – there was a frisson of interest amongst the privacy professional community here in NZ in anticipation of the opportunities to share more actively in the benefits of iappANZ membership. I jumped at the opportunity to join this sub-committee that is charged with growing the NZ part of the IAPPANZ membership.

With a stellar starting line up (our sub-committee member bios are on the next page, so you can start to get to know them) the NZ subcommittee has three initial goals: (i) to grow IAPPANZ membership in NZ; (ii) to host educational and networking events for those members; and (iii) to work with the wider iappANZ board towards the development of an Australian/NZ focussed certification for privacy professionals. The plan is to work alongside the established Privacy Officer Round Table (PORT) network, providing additional opportunities to further their professional development. We have representation on the NZ sub-committee from both the public and private sectors.

The timing of an increased focus on NZ is particularly relevant as everyone anticipate the forthcoming Privacy Act 1993 reforms, which will take us down a change process similar to the process Australia has recently undergone. Amongst other things, this law reform is likely to introduce compulsory breach notification, and to boost the Office of the Privacy Commissioner's enforcement powers, creating new challenges for those of us working in privacy to make sure our organisations are meeting their privacy obligations. I for one have been watching the change process in Australia with interest, and feel fortunate to be able to learn from that experience when our turn comes here.

It is of course also just a generally exciting time to be working in privacy. When I started twelve years ago I could never have conceived that privacy would become a ‘thing’ in the way that it has today (let alone a valid career path!). I don't see this trajectory changing course any time soon, what with the public's increasing awareness of the value of their personal information, and corresponding interest in who has it and what is being done with it. This, combined with the seemingly inexorable march of smart techy ways to hoover up and manipulate every piece of data available, I think there is a reasonable amount of job security.

Privacy, as we all know, is very much not dead. It's not even dying; it's just a bit different. In the end, regardless of the pervasiveness of the digital soup we all swim in, in one key way I don't think privacy has moved all that far from one of its original incarnations, of the ‘right to be let alone’. To me, privacy is first and foremost about humans and the ways they choose to interact - which is of course what makes it so very interesting.

On behalf of the NZ sub committee, we hope those iappANZ members who live and work in NZ, and were able to take up the exciting opportunity to hear Professor Cate speak at our events during Privacy Awareness Week in Auckland and Wellington, enjoyed the experience. I have enjoyed meeting so many of you and hearing about your experiences and interests in what iappANZ is doing in NZ. I look forward to working with and serving you through our fabulous new sub-committee with the full support of our Board behind us.
Together with our iappANZ past president and founder of the iappANZ New Zealand Sub-Committee, we are pleased to introduce all the members of our new committee –

**Emma Pond (Chair)** is ‘Legal Counsel – Privacy’ at Southern Cross Health Society, a non-for-profit, health insurer which provides health insurance to over 800,000 New Zealanders. Emma provides legal advice, guidance and training to the business in respect of the handling of personal and health information. Prior to this, Emma worked for the Office of the Privacy Commissioner for 11 years. Emma is the current convener of the Privacy Officer’s Round Table network in Auckland.

**Annabel Fordham (Government representative)** joined the Office of the Privacy Commissioner New Zealand in September 1999. She has a background in social science and law, and her previous roles included working as a survey designer for Statistics New Zealand. Annabel manages the public affairs, communications, publications and media work for the New Zealand Privacy Commissioner’s Office. She also oversees the education function, which is being transformed to online learning modules, enabling privacy training resources to be easily and freely available. She has worked with all three New Zealand Privacy Commissioners.

**Tom Bowden** is Chief Executive Officer of HealthLink Ltd, a company he co-founded in 1993 under an agreement with the New Zealand Government. Much of Tom’s work is in developing business models to enable government and private sector organisations to work together to accelerate health system transformation.

HealthLink provides electronic communications and data security services to more than 11,000 individual healthcare organisations, across New Zealand, the Pacific Islands, Australia and Canada, enabling the delivery of more than 65 million items of clinical information annually. Tom is also our very own New Zealand iappANZ Board director.

**Jacqui Peace** has worked in global privacy and data protection roles since 2004. Working with GE Capital, Standard Chartered and BP in the UK, she has provided advice on compliance, governance, risk and regulatory issues related to the safe guarding of personal data and records. She led the strategic development of GE’s privacy programme across 26 countries in EMEA, building and implementing a governance framework and a strong network of privacy professionals. With a background in Management and IT Consulting prior to specialising in privacy related issues, Jacqui provides practical and proactive solutions that follow the latest legal and regulatory requirements. She sits comfortably amongst the key players in an organisation (Legal, Compliance, IT, Security and Audit), often bringing the parties together to enable businesses to use personal information properly in the interests of their organisation.

Having left New Zealand in 1992 for a 23 year ‘OE’, Jacqui has recently returned with her Danish husband and eight year old daughter to explore life in Auckland. She’s delighted to be part of the new iappANZ New Zealand sub-committee and looks forward to participating fully in the world of privacy down under. These are interesting times!
Dawn Swan is the privacy officer at New Zealand’s Inland Revenue department whose key responsibility is to oversee Inland Revenue’s performance in the management of personal information. Previously Dawn spent eight years at the Office of the Privacy Commissioner - first as an investigator then as team leader of the Wellington investigations team. She has specialist Privacy Act knowledge through managing hundreds of investigations and enquiries, advising agencies on how to comply with privacy obligations and presenting training in the Privacy Act and Health Information Privacy Code. Dawn is the current convener of the Privacy Officer’s Round Table group in Wellington and attends the Government Chief Privacy Officer’s privacy leadership forums.

Daimhin Warner  Daimhin is Privacy Officer for Sovereign, a company focused on building and protecting the lives, health and wealth of New Zealanders. In this role, Daimhin provides operational advice and strategic guidance to the company in respect of the collection, management and disclosure of customer information, including medical information. He works alongside technology and risk staff to ensure that privacy lies at the heart of Sovereign’s business. Prior to this, Daimhin worked for the Office of the NZ Privacy Commissioner for 8 years, most recently leading the Commissioner’s Auckland Investigations team. Daimhin started life in Ireland, has an LLB from Edinburgh University and LLM in Public Law from the University of Auckland, and has been living and working in NZ for 13 years.

Katherine Gibson is Legal Counsel for Centrix Group, a company providing credit risk management solutions to businesses. Centrix operates a consumer credit bureau where getting privacy right is paramount. Working with senior executives and staff, Katherine provides practical and strategic advice on privacy and business related issues. Through her legal practice, Gibsons Law, Katherine works with small and large organisations, some handling sensitive personal information, as they grapple with not only privacy compliance issues, but in understanding what people expect them to do (or not do) with their personal information. Katherine has over 20 years legal experience and has a B.Com and LLM(Hons) from Auckland University and is admitted to practice in New Zealand and NSW (Australia).

Ella Biggs is a solicitor in the litigation team at Chapman Tripp in Wellington. She advises clients on a broad range of commercial disputes, focusing on disputes with international elements. Prior to joining Chapman Tripp in 2014, Ella was a lawyer in the Insurance and Corporate Risk team at Minter Ellison in Melbourne, where she specialised in media, privacy and intellectual property law. Ella has published several articles on the difficult interaction between traditional legal principles with the digital environment.

Emma Hossack is an iappANZ Board director and immediate past President, as well as iappANZ Chair of ANZ Strategy. Emma helped to found the NZ subcommittee. Emma is commercial lawyer and CEO of medical software company Extensia and CEO of Edocx. She is a Board advisor to CIRCA and current Chair of MSIA.
Big Data and the Future of Data Protection

by Fred H. Cate

The Data Explosion

We live in a world increasingly dominated by the creation, collection, aggregation, linkage, storage, and sharing of vast collections of data pertaining to individuals. Some of those data we generate and reveal by choice, for example, through social media and email, or through compulsory disclosure, for example, as a condition of banking or traveling.

Other data are collected by sensors that surround us in our smart phones, tablets, laptops, wearable technologies and even sensor-enabled clothing, cars, homes, and offices. Increasingly, even public spaces are equipped with video cameras that recognize faces and gaits and microphones that record conversations and detect ambient noises. With the growth of the Internet of Things, connected sensors process an astonishing volume and variety of data without our even being aware. According to a 2014 study by HP, nine out of ten of the most popular internet-connected devices carry personal data.¹

Still more data are calculated or inferred based on demographic information and past behavior. Those data are created, not collected. Moreover, data that may not originally appear personally identifiable may become so or may generate personally identifiable information through aggregation and correlation.

A large volume of these data are held by businesses with which we have infrequent contact (such as when we buy a car or appliance) or by third parties with whom we have no direct dealings. According to the New York Times, Acxiom alone engages in 50 trillion data transactions a year, almost none of which involve collecting data directly from individuals.²

As a result, we are witnessing an explosion not only in the volume of personal data being generated, but also in the comprehensiveness and granularity of the records those data create about each of us. It is part of a phenomenon we often describe as “big data.”

The proliferation and interconnection of big data sets raise significant privacy issues. The challenge we face literally around the world is to evolve better, faster, and more scalable mechanisms to protect data from harmful or inappropriate uses, without interfering with the benefits that data are already making possible today and promise to make even more widespread in the future. Five key steps might help:

1. A More Systemic and Well-Developed Use of Risk Management

Risk management is the process of systematically identifying harms and benefits that could result from an activity. Risk management does not alter rights or obligations, but by assessing both the likelihood and severity of harms and benefits, risk management helps organizations identify mitigation strategies and ultimately reach an optimum outcome that maximizes potential benefits while reducing the risk of harms.³

The ultimate goal of risk management, after taking into account those measures that the data user can take to reduce risk, is to create presumptions concerning common data uses so that both individuals and users can enjoy the benefits of predictability, consistency, and efficiency in data protection.

For example, some uses in settings that present little likelihood of only negligible harms might be expressly permitted, especially if certain protections such as appropriate security were in place. Conversely, some uses in settings where there was a higher likelihood of more severe harms might be prohibited or restricted without certain protections in place. For other uses that present either little risk of more severe harms or greater risk of less severe harms greater protections or even specific notice and/or consent might be required so that individuals have an opportunity to participate in the decision-making process.

Data protection has long relied on risk management as a tool for complying with legal requirements and ensuring that data are processed appropriately and that the fundamental rights and interests of individuals are protected effectively. Yet these risk

¹ HP, Internet of Things Research Study (2014)
management processes, whether undertaken by businesses or regulators, have often been informal and unstructured and failed to take advantage of many of the widely accepted principles and tools of risk management in other areas.

In addition, institutional risk management in the field of data protection has suffered from the absence of any consensus on the harms that risk management is intended to identify and mitigate. This is the starting point for effective risk assessment in other fields. As a result, despite many examples of specific applications, a risk-based approach still does not yet provide a broad foundation for data protection practice or law. But it could.

In 2013 the Council of Ministers of the Organisation for Economic Co-operation and Development (OECD) revised the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, first adopted in 1980, to “implement a risk-based approach.” In the accompanying Explanatory Memorandum, the drafters noted the “importance of risk assessment in the development of policies and safeguards to protect privacy.”

The draft text of the European Union General Data Protection Regulation focuses significantly on risk management. The text that emerged from the European Parliament stresses the need for “the controller or processor” to “evaluate the risks inherent to the processing and implement measures to mitigate those risks.”

And formal risk assessment is required by data protection laws in Australia and New Zealand, for example, through Privacy Impact Assessments and when determining whether notification is required for information security breaches.

Risk management holds special promise in the world of big data by facilitating thoughtful, informed decision-making by data collectors and users that takes into account not only their risks but those of data subjects, by explicitly considering both harms and benefits, and by focusing increasingly scarce resources of both data processors and government regulators where they are needed most.

2. **A Greater Focus on Uses of Data**

There is often a compelling reason for personal data to be disclosed, collected, or created. Assessing the risk to individuals posed by those data almost always requires knowing the context in which they will be used. Data used in one context or for one purpose or subject to one set of protections may be both beneficial and desirable, where the same data used in a different context or for another purpose or without appropriate protections may be both dangerous and undesirable. As a result, data protection should, in the words of the U.S. President’s Council of Advisors on Science and Technology, “focus more on the actual uses of big data and less on its collection and analysis.”

Focusing on the use of personal data does not eliminate responsibilities or regulation relating to data collection, nor should a focus on consent in specific or sensitive circumstances be abandoned. Rather, in many situations, a more practical, as well as sensitive, balancing of valuable data flows and more effective privacy protection is likely to be obtained by focusing more attention on appropriate, accountable use. This is especially true if use is defined broadly to include relying on personal data for decision making or other assessment concerning an individual, using personal data to create or infer other personal data, or disclosing or disseminating personal data to a third party.

Under a more use-based approach, data users would evaluate the appropriateness of an intended use of personal data not by focusing primarily on the terms under which the data were originally collected, but rather on the likely risks to individuals resulting from the proposed use of the data. Such a focus on use is more intuitive because most individuals and institutions already think about uses when evaluating their comfort with proposed data processing activities.

---


6 Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (unofficial consolidated version after LIBE Committee vote, provided by the rapporteur, 22 October 2013), ¶ 66.


9 President’s Council of Advisors on Science and Technology, *Big Data and Privacy: A Technological Perspective* xiii (2015).

The terms under which data were collected would remain relevant when a specific purpose is provided at time of collection and is a meaningful factor in obtaining access to data. This would be especially clear in settings where users had made meaningful choices (e.g., specifying a preferred medium for future communications) or where the data processor had agreed to specific limits as a condition of obtaining personal information (e.g., an explicit promise not to share the data).

A use-focused approach is especially important in the context of big data because the analysis of big data doesn’t always start with a question or hypothesis, but rather may reveal insights that were never anticipated. As a result, data protection based on a notice specifying intended uses of data and consent for collection based on that notice can result in blocking socially valuable uses of data, lead to meaninglessly broad notices, or require exceptions to the terms under which the individual consented. If privacy protection is instead based on a risk analysis of a proposed use, then it is possible to achieve an optimum benefit from the use of the data and optimum protection for data fine-tuned for each intended use.

3. A Broad Framework of Harms

The goal of a risk management approach focused on data uses is to reduce the harm that personal information can cause to individuals. Accomplishing this requires a clear understanding of what constitutes “harm” or other undesired impact in the privacy context. Surprisingly, despite almost 50 years of experience with data protection regulation, that clear understanding is still lacking both in the scholarly literature and in the law.

A framework for recognized harms is critical to ensuring that individuals are protected and to enhancing predictability, accountability, and efficiency. National regulators are well placed to help lead a transparent, inclusive process to articulate that framework. The goal should not be to mandate a one-size-fits-all approach to risk analysis, but rather to provide a useful, practical reference point, ensure that a wide range of interests and constituencies are involved in crafting it, and provide the transparency necessary to facilitate fairness and trust.

There are a wide range of possibilities for what might constitute a harm, but it seems clear that the term must include not only a wide range of tangible injuries (including financial loss, physical threat or injury, unlawful discrimination, identity theft, loss of confidentiality, and other significant economic or social disadvantage), but also intangible harms (such as damage to reputation or goodwill, or excessive intrusion into private life) and potentially broader societal harms (such as contravention of national and multinational human rights instruments). What matters most, though, is that the meaning of harm be defined through a transparent, inclusive process, and with sufficient clarity to help guide the risk analyses of data users.

Risk assessment is not binary and is likely to be influenced by a number of factors within the data user’s control. So the goal of the risk assessment isn’t simply to indicate whether a proposed data use is likely to be appropriate or not, but also to highlight the steps that the data user can take to make that use more acceptable (e.g., by truncating, encrypting, or de-personalizing data).

4. Less Focus on Individual Consent and More on Responsible Data Stewardship

Effective governance of big data requires shifting more responsibility away from individuals and toward data collectors and data users, who should be held accountable for how they manage data rather than whether they obtained individual consent. The recognition that processors should be liable for reasonably foreseeable harms will create a significant incentive for greater care in the collection and use of data. It will also restrict the practice of allowing processors to escape responsibility by providing notice and obtaining (or inferring) consent.

This should thus reduce the burden imposed on individuals and focus their attention on data processing activities only where there are meaningful, effective choices to be made. Processors, in turn, will benefit by not wasting resources on, or having future potentially valuable uses of personal data restricted by, notices that no one reads or adhering to terms of consent that are often illusory at best.

5. Transparency and Redress

Data are increasingly being used to make decisions about individuals, and even to predict their future behavior, with often significant consequences. The one certainty of data analysis is that there will be errors—errors resulting from problems with data matching and linking, erroneous data, incomplete or inadequate algorithms, and misapplication of data-based tools.

Whenever big data are used in ways that affects individuals, there must be effective transparency and redress. This is necessary to protect the rights of individuals, but is also serves the vital purposes of enhancing the accuracy and effectiveness of big data tools, and

---

creating disincentives for deploying tools inappropriately. Meaningful transparency and redress, together with effective enforcement, not only provide remedies for current harms, but also help to prevent future ones.

Conclusion

In an age of big data, privacy is more essential than ever before. If we are to protect personal privacy effectively, while continuing to enjoy the benefits that data - big and small - are already making possible, we need to evolve better protections. To achieve more effective, sustainable, and scalable guarantees for privacy, we must reduce our reliance on notice and consent at time of collection and place more responsibility on data users to be responsible, rational stewards of the data they control.

Professor Fred Cate is Distinguished Professor and C. Ben Dutton Professor of Law, Indiana University Maurer School of Law; Senior Policy Advisor, The Centre for Information Policy Leadership at Hunton & Williams LLP.
I’m a Privacy Paradox, but companies should not be

by Jennifer Mulvaney

I freely admit that I don’t take protection of my personal data all that seriously. I barely skim privacy policies, and that “skimming” essentially consists of scrolling through the policy just to get to the “I agree” box at the bottom of the screen.

I’m perfectly fine being tracked in shopping malls if there’s a chance I’ll get some useful vouchers, and I rarely change my password. I am strongly of the “I have nothing to hide” camp. I’m fine with extra pat downs at the airport. Naïve? Perhaps. Lazy? Most certainly. My “creepy” threshold? Pretty high.

I certainly don’t deny that bad things could happen if someone were to hack into my information, particularly if a misfit finds his way into to my bank account, passport file or God forbid zaps away my frequent flyer miles. Those things would change my carefree attitude and surely my habits.

That being said, I proudly work for a company that literally stays up at night thinking about privacy.

Intel’s mission to connect every person on earth also means the company has an inherent responsibility to protect the data of those very people. Trust is at the heart of Intel’s entire business, not just a legal compliance function. Privacy is physically embedded in our technology, and is as palpable in our culture.

Recently in both the United States and Australia, Intel conducted public surveys on both the public’s attitude towards company behavior and what consumers understand about data generally. The results were not at all surprising.

The 2014 US survey focused on how consumers felt their personal data was being handled. The headline? “Distrust and lack of understanding.” The “lack of understanding” bit was the most troublesome: 65 per cent of respondents had no idea who was able to access their data from their devices or how that data was used (guilty).

Intel Security in Australia just this month boiled down its responses from a similar survey to a “mediocre level of trust of business.” Regardless of my own reckless approach to data protection, these findings are concerning.

A service provider might argue that the skeptical and ignorant respondents in these and other surveys should read company privacy policies more carefully before clicking away impulsively, (like me), to get their transit card or open a frequent flyer account. A service provider might further opine that customers should educate themselves better on how to more effectively control their privacy settings thereby controlling what data is revealed about them. It’s all right there on the website, after all.

Given my habits, I would stick my fingers in my ears at such a lecture. I am also put off by the notion that any company would put the burden squarely on the end user to read, much less comprehend, an online privacy policy that could range anywhere from 3,000 to 18,000 words, according to a recent survey by the Australian Privacy Commissioner. This smacks of companies focusing solely (and overly so) on privacy compliance, versus creating a privacy culture.

I recently asked my 7-year old what he thinks of when I say “trust”, and he replied “it’s when someone does something that hurts you and you are not friends with them again until they change.” Applied to company mistrust, my son’s prescription seems to apply: If trust is lost, the company has to step up to turn things around, or the customer walks.

Maybe it’s because Intel has such a rich privacy culture that I’m so lax in my ways at home, but there certainly is something to be said for a “privacy from the top” policy that requires the protection of people’s personal information to be considered before a product ever gets beyond an engineer’s thought bubble. If privacy is not built in from a product’s birth at Intel, it goes nowhere.

To silo privacy into a separate, “We’ll check the box, call us when you have a problem” office, is terribly short-sighted given the direction that our global economy is heading. Consumer trust and understanding will certainly be no better off in a sensored world if privacy is not woven throughout all businesses, large and small, at all levels of management.

Finally, there can be hardly any doubt that “consumer mistrust” and “lack of understanding” about data is intimately linked. Some basic, spoon-fed data education would go a long way. Companies can move the needle here so that consumers feel a bit more empowered when it comes to talking about their data, and safer when it comes to protecting it.

Companies should heed this “data education” call by doing the following:
Explain what you do with personal data and why, in a language that my mother would understand.

Increase our vocabulary so we can string together a sentence about the data we generate on ourselves and how it moves through wires and tubes, gateways and the like.

Explain what form data takes when it comes out the other end and why it is so hard to show me a picture of what metadata looks like. An infographic would be welcome.

In other words, what happens behind the scenes after we hit the send button?

Perhaps its Intel’s unwavering commitment to privacy that ironically gives me a false sense of confidence when I give up my personal data, which is just about every other day. Maybe it’s the Intel in me that makes me trust other companies much more than I should.

But in addition to being a bit naïve as to how my data is being used, I’m also an eternal optimist. I ultimately believe that over the long term, companies will embrace a privacy culture, and instinctively avoid bargaining away the trust of their customers. It may take a few more surveys to demonstrate that result, but it will be well worth the wait.

Jennifer Mulvane is Intel’s Director of Cloud Policy and Government Affairs in Sydney, Australia. She is responsible for Intel’s global cloud policy and other issues such as international trade, privacy, security and Internet governance in Australia and New Zealand. Prior to her Sydney posting last year, Jennifer was Intel’s Republican liaison with the United States Senate in Washington, DC.

Intel is a Gold sponsor of iappANZ and the views expressed in this article are those of the author.
iappANZ’s writing prize 2015: entries open

Entries have now opened for this year’s writing prize for an article that is published in our monthly Journal editions from February to October 2015. Anyone can enter (you don’t have to be an iappANZ member), simply by writing and submitting an article between 500-1500 words that tells us something interesting, new and relevant about privacy.

All articles must be submitted by email, preferably in Word, to [veronica.scott@minterellison.com or an iappANZ email] by 20 October 2015. We will need the author’s email address and contact number. You can submit as many articles as you like.

The winner will be announced at our Privacy Summit in November 2015 and their name and details will be published on our website. We also hope to profile the winner in our Journal. So alert your network and get writing!

More details about the writing prize if you are interested:

▪ Our Editorial team, Veronica Scott and Carolyn Lidgerwood, plus President Anna Kuperman and Past President Malcolm Crompton, will decide on the winner whose article they judge to be the most interesting, original and relevant to our members.

▪ Some people won’t be eligible for the prize (sorry!). They are: iappANZ board members, contractors and employees and their family members.

▪ After the winner is announced we will notify them and arrange for the prize to be delivered to them if they are unlucky enough not to be at our Summit.

▪ There will (sadly) be one prize only. Its value is AUS$250, so that’s pretty good really.

▪ We may need to verify the winner’s identity so we don’t give the prize to the wrong person.

▪ If the prize is not claimed for any reason (and we hope this won’t happen) the author of the runner-up article as judged by the Editorial team will receive the prize.

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

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

No positions currently advertised.
SAVE THE DATE

WEDNESDAY 18 NOVEMBER, 2015, MELBOURNE

2015 iappANZ Annual Privacy Summit: Privacy@work

“The iappANZ Summit always provides valuable insights into the privacy challenges and opportunities currently being experienced by other businesses and industries – and more importantly, their approaches and solutions to them.”

Greer Harris, Asia Pacific Regional Privacy Officer, AstraZeneca

Camouflage 2008, by permission of artist, Alasdair Wallace

Are you up to date with ‘privacy’ issues and compliance? Are you interested in hearing from some of the world’s leading privacy thought leaders? Do you want an opportunity to network with like-minded people? Do you want to see what's coming in privacy and understand what the big issues are?

Following our highly successful 2014 Summit Privacy@Play in Sydney, come and join us this year in Melbourne for a day of ideas, views and discussions on current and future privacy issues that matter.

Early Bird registrations coming soon!

For more information email emma.heath@iappanz.org
## Privacy Events

<table>
<thead>
<tr>
<th>Time, Date &amp; Location</th>
<th>Information</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>22 – 24 July, 2015</strong>&lt;br&gt;8.00 – 5.00pm&lt;br&gt;The Grace Hotel,&lt;br&gt;77 York Street, SYDNEY</td>
<td>Records &amp; Management Forum&lt;br&gt;This Forum will showcase how you can embrace digital advancements as an integral part of your competitive strategy whilst using information management as a primary business enabler. The Forum will focus on the theme of adopting digital processes to optimise business value and feature 17 expert speakers, 11 case studies as well as 2 exclusive workshops.&lt;br&gt;Attending and speakers include:&lt;br&gt;• Katharine Stuart, Acting Director - Digital Strategy and Solutions, National Archives of Australia&lt;br&gt;• Elizabeth Tydd, Information Commissioner &amp; CEO, Information and Privacy Commission NSW&lt;br&gt;• Claire Holt, Chief Health Information Manager, Portland District Health&lt;br&gt;• Dr Monica Trujillo, Chief Medical Information Officer, UnitingCare Health&lt;br&gt;• Kate Harrington, Director - Information Management, Office of Finance and Services NSW&lt;br&gt;• Ben Dornier, Director, Corporate Community Services, City of Palmerston, NT&lt;br&gt;See the full program <a href="#">here</a>&lt;br&gt;Click here to visit the website: <a href="http://bit.ly/1E0KYdQ">http://bit.ly/1E0KYdQ</a></td>
<td>iappANZ readers receive a 20% discount off the standard price.&lt;br&gt;To lock in your exclusive discount, just contact Akolade on 02 9247 6000 or email <a href="mailto:marketing@akolade.com.au">marketing@akolade.com.au</a> and reference VIP Code: EFXB1.</td>
</tr>
</tbody>
</table>

<p>| Wednesday 5 August 2015&lt;br&gt;4pm-7pm&lt;br&gt;Baker McKenzie Lawyers&lt;br&gt;L27, AMP Centre&lt;br&gt;50 Bridge Street, Sydney | Pharmaceutical Industry and Privacy&lt;br&gt;Speakers include:&lt;br&gt;• Anne-Marie Allgrove – Partner, Baker McKenzie&lt;br&gt;• Malcolm Crompton – Director, IIS&lt;br&gt;• Jessica Kanevsky – Legal Counsel, Abbvie&lt;br&gt;• Greer Harris - Regional Privacy Officer, Asia Pacific, AstraZeneca | Free for iappANZ members&lt;br&gt;$99 plus GST for non-members&lt;br&gt;Registrations – <a href="mailto:admin@iappANZ.org">admin@iappANZ.org</a> |</p>
<table>
<thead>
<tr>
<th>All day event 8am-6pm</th>
<th>iappANZ annual Privacy Summit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wednesday, 18 November 2015</td>
<td></td>
</tr>
<tr>
<td>Zinc at Federation Square, MELBOURNE</td>
<td></td>
</tr>
</tbody>
</table>

*Details of speakers and topics to be advised shortly*

<table>
<thead>
<tr>
<th>Early bird, membership and full prices TBC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact Emma Heath for further information</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?

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.

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.

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.