Vice President’s foreword

In this month’s bulletin, we are excited to share some truly insightful contributions, including an article from Australian Privacy Commissioner Timothy Pilgrim, as well as a snapshot of some upcoming privacy events for Privacy Awareness Week (PAW) to add to your calendar.

We are especially delighted to announce that The Hon. Michael Kirby AC CMG, has accepted our invitation to be our inaugural Honorary iappANZ member. He has also been included by our President, Emma Hossack, in our special member profile in this month’s edition for your reading pleasure. It’s not often you can get such a mix of brilliance, honesty and compassion! And, this kick-starts our call out for more member profiles! Please consider putting yourself forward (or nominating someone) for a profiling opportunity in our monthly bulletins. We hope to have at least 1 member featured each month. Please do not be deterred by the stellar status of first member profile in this edition! We are interested to know what has driven your passion for privacy, where it came from, where you see it going and perhaps (if not too private!) something personal about what you love to do outside of your profession.

If you are not keen on a profile, you may still want to share your movements with other members through our bulletin (even if it’s already on Linkedin). We want our members to connect in every possible way. Contact our Editor Kate.Johnstone@me.com if you are interested and we will arrange for a Board Member to speak with you.

Our Board recognises that iappANZ members provide us with great support as well as contributing valuable ideas for ways to improve privacy connections. To say thank you, we are offering 2 complimentary tickets to the OAIC business breakfast on Monday 29 April at the Hilton in Sydney (travel to/from venue excluded). The theme for the breakfast will be the launch of the OAIC’s new Guide to Information Security and you will be seated with some of our iappANZ Board Members.

The first 2 members to contact our General Manager, Judith Cantor, at judith.cantor@iappanz.org will each receive a complimentary ticket.

We are fortunate this month to have a diverse range of articles from authors in different disciplines: government, law, academia and health addressing some challenging issues in media and privacy, information management and use of big big data in the medical context.

Before I sign off, I wanted to share something that I recently read and which struck a nerve with my privacy conscience -- perhaps it will with yours too! Jeff Hindenach, Director of Content at

Media Privacy in Print Media: Read all about it

Using Big Data to improve health and maintain individual privacy

Children’s Privacy – An Area to Watch

Nudges and Defaults – what have they got to do with privacy? The Answer is a lot.

What has recordkeeping got to do with privacy? Managing privacy at the University of Sydney

Upcoming Privacy Events

IAPP Certification
NextAdvisor.com posted an article in The Huffington Post titled: "The Most Popular Online Password Is ‘Password’ Yet We Blame Our Privacy Problems on Facebook". As the name suggests, the article addresses our own personal accountability for safeguarding our online activities. We often talk about data security in the corporate world as corporate citizens, BUT do we protect our own personal digital footprints with the same rigour? I must confess that I have used some pretty generic passwords in the past for some pretty important information. This PAW, I will be turning my mind to my online presence and security. Take a minute to construct a roadmap of all of your online transactions, interactions and interests and pretend for a second that you are the business owner of this roadmap – are you happy with what you see?

Finally, stay tuned for the announcement of a prize give-away in next month’s bulletin – more details to come.

Anna Kuperman
Vice President

We encourage a diversity of views in our Bulletin and sometimes you may not agree with these. Have your say! Respond and put forward your case. We aim to represent the views of all of our members *subject to iappANZ approval

Privacy law reform: a milestone for privacy

There have been big changes in privacy since I spoke to many of you at the iappANZ conference in November 2012. The passing of the Privacy Amendment (Enhancing Privacy Protection) Act 2012 on 29 November 2012 was an important milestone for privacy in Australia. While the amendments don’t come into force until 12 March 2014, I am encouraging privacy professionals in both the public and private sectors to start preparing now.

As you know, the reforms introduce a unified set of Australian Privacy Principles (APPs), new credit reporting laws, and greater enforcement powers for the Commissioner to resolve complaints, conduct investigations and promote privacy compliance.

- **The Australian Privacy Principles**
  Under the reforms, there will be 13 new APPs to replace the existing Information Privacy Principles (IPPs) and National Privacy Principles (NPPs) that apply to Australian Government agencies and businesses respectively. The APPs aim to more closely reflect the information lifecycle - from notification and collection, through use and disclosure, quality and security, to access and correction. They are structured to simplify privacy obligations and reduce confusion and duplication.
  The single set of privacy principles should make it easier for individuals, business and agencies to understand the laws that protect personal information. However, as you are no doubt aware, there are a number of important changes, including in the areas of direct marketing, cross-border disclosure of personal information and the handling of unsolicited information.

- **Credit reform**
  There are a number of significant changes to credit reporting laws, including the introduction of comprehensive credit reporting. These changes are designed to provide consumer credit providers with sufficient information to adequately assess credit risk while ensuring the protection of personal information, and to encourage responsible lending.
  The system will be underpinned by a new industry-agreed Credit Reporting Code of Conduct. On 20 December 2012, I exercised the power to request a code developer to develop a code of practice about credit reporting. The Australasian Retail Credit Association (ARCA) was given 120 days to develop a code and apply to the Commissioner to have that code registered. I recently extended this deadline to 1 July 2013.

- **Enhanced Powers**
  There has been much discussion about how the reforms will increase to the powers of the Commissioner. I will be able to conduct Performance Assessments of private sector organisations to determine whether they are handling personal information in accordance with the new APPs, the new credit reporting provisions and other rules and codes.
  This power will consolidate existing discretions to conduct audits of Australian Government agencies, tax file number recipients, credit reporting agencies and credit providers, and extend the discretion to include private sector organisations.

From 12 March 2014, I will be able to accept enforceable undertakings from both the private sector and Australian Government agencies, and I may seek civil penalty orders of up to $340,000 for individuals, and up to $1.7 million for companies in instances of serious or repeated breaches of privacy. While my goal is to resolve most complaints via conciliation, I intend to exercise these powers in appropriate cases.

Get involved

The OAIC has already commenced developing guidance to assist agencies and businesses. Reference to these resources will be essential when advising on what the new laws require, and what changes clients need to make to their personal information handling policies and practices.

The OAIC has a role in educating all organisations and agencies, as well as the community more generally, about the reforms. Key guidance material will include a detailed set of guidelines on the APPs. The OAIC also has a range of other important responsibilities, including the drafting of binding guidelines, rules and other statutory instruments. We are hopeful that some of this material will be ready by mid-2013.

The OAIC plans to conduct targeted and public consultation processes to assist us to develop further guidance on the reforms, including talking to industry bodies and consumer groups. One of the early consultations will be on the guidelines on the APPs. Make sure you participate in this and future consultations to ensure your views are taken into account. Information about these processes
Privacy Awareness Week 2013

Privacy Awareness Week 2013 (PAW) will be held from 28 April to 4 May. Not surprisingly, the theme this year is privacy reform. I encourage your organisation or agency to sign on as a PAW partner. There will be a range of awareness materials available for partners to use during the week, including e-posters, web banners and buttons, intranet and newsletter content, videos and training slides.

We are also planning a number of activities to promote our privacy messages, including our launch event, a business breakfast on Monday 29 April at the Hilton in Sydney. The theme for the breakfast will be information security requirements, and OAIC’s new Guide to Information Security (the Guide) will be launched. More information will be available soon via the OAIC website.

Keep informed and spread the message

The OAIC has not received any additional funding to conduct an education campaign about these reforms, so we are asking you as privacy professionals to help us spread the message. You can keep up to date on the OAIC’s law reform implementation progress by visiting the ‘Privacy law reform’ page and subscribing to our mailing lists on our website (www.oaic.gov.au). You may also like to join our Privacy Connections network (http://www.oaic.gov.au/news/networks/index.html#PCN), a free network for the private sector to keep in touch about upcoming law reform events and newly released resources.

2013 is certainly going to be a busy year for privacy professionals. The large scale of these reforms presents interesting challenges and opportunities for all of us, as privacy laws are brought up to date with today’s technological landscape and business practices. Please take advantage of our resources as they become available to fully prepare for the changes to come.

Timothy Pilgrim
Australian Privacy Commissioner

Introducing the iappANZ inaugural Honorary Membership and Profile of The Hon. Michael Kirby AC CMG

iappANZ Board is delighted to announce The Hon. Michael Kirby AC CMG, as the inaugural Honorary iappANZ member.

Emma Hossack was fortunate to gain an insight into The Hon. Michael Kirby.

What was the catalyst for your interest in privacy and involvement with the OECD?
The catalyst for my interest in privacy, and engagement with the OECD expert group on privacy protection, was the decision of the Fraser government to give the ALRC a reference to develop laws for the better protection of privacy in Australia. Before that step, initiated by Robert Ellicott QC MP in the fragile days that followed the dismissal of the Whitlam government by the Governor General, I had not given a lot of thought to the legal protection of privacy. The announcement of the commitment of the Coalition to giving such a reference was a great relief to the ALRC. It meant that the commission would survive and flourish. During the Whitlam government I had taken pains to brief the Opposition on the work and potential of the commission. Mr Fraser’s announcement was a vindication of that approach. When, after 1976, the commission began work on the privacy project, we saw how urgent and various were the challenges. Looming up at us was 1984, George Orwell’s metaphorical year. So when the OECD created its expert group, and I was sent to Paris to join it, I was fully aware of the global and national importance of better privacy protection. Joining that group, and being elected its chairman, was a great career opportunity for me. But it was also a challenge to the ALRC, and Australia, to see its problems of privacy protection in the context of global technology and global dangers.

What is the most fascinating aspect of privacy protection in your view?
There are so many aspects of privacy that are fascinating. On the one hand the remarkable technology of Informatics that has arisen in the past forty years. It has an enormous potential to expand the utility of information to the benefit of humanity. But it also has a great potential to enhance the power of government and corporations to invade individual privacy and the control that individuals have over private aspects of their lives. Back in 1976, I was generally very private about my sexuality. That was how one was expected to be in those days. I therefore knew the importance of privacy and the need to respect and protect it in a society (and a world) that was very hostile to gay people. Beyond this experience, I found it fascinating to explore why people actually feel strongly about privacy, beyond self protection. It has something to do with our desire to find private spaces in which we each, individually, can flourish and expand our personalities and inner peace in conjunction with a chosen few other individuals, as distinct with the community and world about us. There is something about the peace of that private space that explains the human desire for privacy. It helps to explain why respect for privacy is found in the international human rights statements, beginning with The Universal Declaration of Human Rights, 1948.
Nudges and Defaults – what have they got to do with privacy? The Answer is a lot.

I have just attended the IAPP Global Privacy Summit 2013 which was, you guessed it, the biggest single conference on privacy in history. Trevor Hughes, President and CEO of IAPP said so.

The conference puts on an immense variety of sessions – plenary and parallel. There is a strong focus on the trans-Atlantic debate about whose privacy framework is best and why ‘theirs’ will be the ruination of commerce or civilisation depending on which side you are on. There is also a lot on domestic US issues which can be tedious.

But that is nit picking. There is something in the conference program for almost any privacy professional. I strongly urge you to attend.

So what has all this to do with Nudges and Defaults?

The first Keynote Speaker this year was Cass Sunstein. He is famous for his book Nudge: Improving Decisions about Health, Wealth and Happiness and has just launched a new book, Going to Extremes: How Like Minds Unite and Divide.

The theme of his keynote was to explain how the nature of the default settings put in front of us influence our decisions and how this can be used for good (or not so good). Cass described this as a “trilogy of options”, namely Mass Opt Out, a binary choice where you Opt In or cannot proceed and finally personalised default rules in respect of aspects of our lives like travel and credit. The biggest example in privacy is ‘opt out’ versus ‘opt in’ to receive mail marketing.

Cass gave us three reasons why defaults affect our decisions, complete with experimental evidence to prove the point. These are:

Inertia – put on a popular TV show and the ratings of the following TV show go up dramatically. People just don’t get around to changing TV channels

Implicit endorsement – the default indicates ‘what sensible people think is best’, with the outstanding example being organ donation, where donation rates are incredibly high in countries in which everybody is signed up for organ donation but can opt out, but are very low in countries where everybody is encouraged to opt in. Australia very sadly has an opt in system and yes, our
Reference point – the default sets the reference point for decision making. The experiment he cited here was in relation to teaching to achieve a performance standard in the class. Some teachers were given the bonus up front with the risk of losing it if they didn’t attain the standard obtained, while others were only paid the bonus if they did manage to attain the standard. The former group achieved significantly higher results. Apparently, humans hate losing a lot more than they love winning: behavioural economics again, as we learnt from Alessandro Acquisti at the iappANZ Annual Conference in 2011.

One way in which these biases can be overcome is by forcing a choice from alternatives without a pre-set default, which he calls Active Choosing, for example neither ‘yes’ or ‘no’ is filled in for an option but you cannot move to the next screen until you make a choice.

However, this comes at a cost: irritating the individual, especially if they think it is a trivial issue. Cass also noted that Active Choosing had a different impact on the poor compared with the more wealthy. Generally speaking, the less well off an individual is, the more active they have to be in making the basic decisions of life. In effect, ‘do nothing’ leaves the wealthy on the right track because they have so much taken care of for them but ‘do nothing’ leaves the less well off on the wrong track. The result of forcing too much Active Choosing can be very poor decision making by people who just need to get on with their lives.

Cass had so much more to say. If you want to know more, you have to read his books.

So when you are designing the web page or designing the form, think about the defaults you are introducing – is the default nudging the user towards safer privacy and security settings or not? Does it matter? Are we nudging users in such a way that we are ‘making the safe way the easy way’?

Yes, nudges and defaults have a lot to do with privacy.

Malcolm Crompton CIPP is Managing Director of Information Integrity Solutions Pty Ltd. He is a Director on the iappANZ Board and was its founding President. Malcolm was Privacy Commissioner of Australia until 2004. He received the Privacy Leadership Award at the IAPP Global Privacy Summit 2012.

Children’s Privacy – An Area to Watch

Children’s privacy will be an area to watch for developments in 2013. Entities need to assess the applicability of the Children’s Online Privacy Protection Rule (Rule), updated by the Federal Trade Commission (FTC) on Dec. 19, 2012, as well as carefully monitor guidance and enforcement from the FTC and state attorneys general. Children’s Online Privacy Protection Act enforcement actions by the FTC and state attorneys general often involve social media and increasingly involve mobile applications. A recent example is the FTC’s enforcement action involving the through its mobile application and website, as more particularly described below.

The updated Rule continues to cover operators of websites or online services that are either directed to children under age 13 or which have actual knowledge that they are collecting personal information from children under age 13. An operator generally must (1) provide notice on the website or online service of the information it collects from children under age 13, how it uses such information and its disclosure practices for such information, (2) obtain verifiable parental consent before any collection, use and/or disclosure of personal information from children under age 13, (3) provide a reasonable means for a parent to review the personal information collected from a child under age 13 and to refuse to permit its further use or maintenance, (4) ensure that disclosing more personal information than is reasonably necessary to participate in an activity is not a condition to a child’s participation in a game, the offering of a prize or another activity, and (5) establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children under age 13, among other things.

This article focuses on changes in the definitions in the updated Rule that impact its application. Entities that operate websites or online services need to review their privacy policies and practices and those of any integrated outside services such as such as plug-ins (e.g., social plug-ins) or advertising networks to determine their compliance obligation. Any changes should be implemented before the July 1, 2013, effective date of the updated Rule. Specifically, entities must determine: (1) the types of personal information that the website or online service collects, (2) whether the website or online service integrates outside services (e.g., plug-ins or advertising networks) and whether the outside services collect personal information, (3) whether the website or online service is directed to children under age 13, and (4) whether the website or online service has actual knowledge that it collects personal information directly from users of another website or online service directed to children under age 13.

Which types of personal information does the website or online service collect?

The updated Rule expands the types of personal information covered to include: (1) geolocation information sufficient to identify a street name and the name of a city or town, (2) a screen or user name functioning in the same manner as online contact information (meaning an email address or any other substantially similar identifier that permits direct contact with a person online, including without limitation, an instant messaging user identifier, a voice over internet protocol (VOIP) identifier, or a video chat user identifier), (3) a photo, video or audio file containing a child’s image or voice, and (4) online contact information.

Covered personal information also was expanded to include a persistent identifier that can be used to recognize a user over time and across different websites or online services, including, without limitation, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or a unique device identifier. An operator will have no notice and parental consent requirements under the updated Rule where it collects a persistent identifier and no other personal information and such identifier is used for the sole purpose of providing support for the internal operations of the website or online service. This means activities necessary to: (1) maintain or analyze the functioning of the website or online service; (2) perform network communications;
The following types of personal information continue to be covered: (1) first and last name, (2) physical address including street name and name of a city or town, (3) telephone number, (4) Social Security number, and (5) information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described above.

Collecting personal information means the gathering of any personal information from a child under age 13 by any means, including (1) requesting, prompting, or encouraging a child under age 13 to submit personal information online, (2) all means of passively collecting personal information from children online, regardless of the technology used, and (3) enabling a child under age 13 to make personal information publicly available in identifiable form. An operator that provides a field or open forum for a child under age 13 to enter personal information will not be shielded from liability because entry of personal information is not mandatory to participate in the activity. An operator will not be considered to have collected personal information if it takes reasonable measures to delete all or virtually all personal information from the postings of a child under age 13 before they are made public and also to delete such information from its records.

Does the website or online service integrate any outside services (e.g., plug-ins or advertising networks), and do the outside services collect personal information?

The FTC and state attorneys general vigorously enforce COPPA. COPPA enforcement actions have implicated and likely will continue to implicate websites and increasingly mobile applications with social media or interactive features. By way of recent example, in the Path enforcement action, Path was charged with knowingly having collected the personal information of children under age 13 and enabled children under age 13 to publicly disclose their personal information through the Path social networking service via its mobile application and website. According to the FTC’s Business Center blog, some key take-aways for entities from this enforcement action are that COPPA is not just for kids’ sites and that entities in the mobile marketplace must comply with COPPA and other laws and requirements. Other companies that were the subject of such FTC enforcement actions include: Artist Arena, RockYou, Skid-e-kids, Playdom (Disney), Sony Music, Imbee. com, and Xanga. Civil penalties of $3 million were imposed in Playdom (Disney) and $1 million were imposed in Artist Arena, Sony Music, and Xanga, respectively. The California and Texas attorneys general also have enforced children’s privacy, and COPPA enforcement actions were brought in 2011 by the FTC against mobile application developer W3 and by the New Jersey attorney general in 2012 against mobile app developer 24x7digital LLC.

Immediately before the FTC issued the updated Rule, the FTC issued its second staff report on Dec. 10, 2012 on kids and mobile applications, including those linked to social media. The FTC urged industry participants to work together to develop accurate disclosures about data collected through kids’ applications, how it will be used, who it will be shared with and whether the applications contain interactive features such as advertising, the ability to make in-app purchases, and links to social media. Also, according to this report, the FTC staff is launching multiple non-public investigations regarding whether certain companies in the mobile application marketplace have violated COPPA or engaged in unfair or deceptive trade practices in violation of the Federal Trade Commission Act. In addition, the FTC recently issued a staff report that provides best practice recommendations intended to improve mobile privacy disclosures and a business guide for mobile application developers regarding security. When the New Jersey attorney general announced the settlement of its enforcement action against 24x7, it noted that the New Jersey Division of Consumer Affairs was continuing its investigation of other mobile applications and their possible unlawful sharing of users’ private information. The California attorney general also is enforcing mobile application privacy. The California attorney general also is working on best practices for mobile privacy with Facebook and six other major mobile application platform companies and recently issued guidance as a step in the development of these best practices.

The updated Rule provides the FTC and state attorneys general with an additional basis for enforcement. Entities that operate websites and online services, including mobile applications, particularly those that collect the types of personal information of children under age 13 now covered under the updated Rule, integrate outside services (e.g., plug-ins or advertising networks), or are child-directed, could attract scrutiny by the FTC and state attorneys general. Accordingly, entities that operate websites or online services must assess the application of the updated Rule to them and review their privacy policies and practices and those of any integrated outside services to determine their compliance obligations. Any changes should be implemented before the July 1, 2013 effective date of the updated Rule. Entities should also carefully monitor FTC and state attorneys general COPPA and related guidance and enforcement, especially in the mobile application and social media areas.

Melissa J. Krasnow is a corporate partner with Dorsey & Whitney LLP. Her practice encompasses privacy, electronic and mobile commerce, social media, anti-money laundering, corporate governance and compliance law, and mergers and acquisitions. She is a Certified Information Privacy Professional/US (CIPP/US) who serves on the Certification Advisory Board for the CIPP/US program and the Canadian Advisory Board of the International Association of Privacy Professionals.
The majority of the personal information held by the University is contained in its business systems such as those for student administration, HR, research management and alumni. The corporate recordkeeping: Records Management

Records continuum:
...a consistent and coherent regime of management processes from the time of the creation of records (and before creation, in the design of recordkeeping systems), through to the preservation and use of records as archives. (Australian Standard AS4390-1996); and

Records Management Recordkeeping:
...making and maintaining complete, accurate and reliable evidence of business transactions in the form of recorded information. (Australian Standard AS4390-1996, Records Management).

The majority of the personal information held by the University is contained in its business systems such as those for student administration, HR, research management and alumni. The corporate recordkeeping system, administered by ARMS, manages correspondence (primarily email) and the transactional records relating to students, staff and the broad range of functions and activities of the University. To give some idea of the of the recordkeeping system, it currently holds more than 5.5 million electronic documents. In 2012 it grew by 25,000 documents per week, so far this year the average has been 57,000 documents a week. Individual members of staff can file electronically, or on paper if they really must, in the traditional registry style of operation. Our preferred method of operation is to implement workflows or link the business systems with the recordkeeping system where the business system does not meet mandatory recordkeeping standards under the State Records Act. In this way recordkeeping happens automatically, without active intervention by staff members.

It might be starting to be apparent why privacy, recordkeeping and access are dealt with by one unit. If you can exercise control over the collection and management of an organisation's records, you are in a very good position to address many aspects of privacy and in a better position to deal with requests for access to the organisation’s information by members of the public.

Recordkeepers must have a wide knowledge of their organisation, its structure, functions and priorities. They liaise and work across their organisation in a way that most staff members don’t. Knowing the detail of an organisation is essential to enable a corporate recordkeeping system to manage the records over time. A person cannot exercise his/her rights over information about themselves unless the information exists in an organisation’s records, is known to exist and can be found and retrieved. These are some of the functions of recordkeeping system. It has been said since the introduction of FOI that its success depends on good recordkeeping. In a very large measure that same can be said for privacy regimes.

Like Privacy by Design, the Records Continuum approach widely followed in Australia requires intervention by recordkeepers at the stage of business system design. The Continuum approach, as it is commonly called, was a response to the avalanche of electronic records. These records cannot be managed retrospectively, as was often did in the days of paper. Business systems must meet recordkeeping standards to ensure that reliable and useable records are created. The analysis of recordkeeping needs includes consideration of the nature of the information that will be held in the records. This analysis and discussion provides the opportunity for questions of privacy and access to considered and addressed in the system design.

The need to ensure compliance with information protection principles sits happily with the need to meet the recordkeeping standards that apply to the University and which meet its own business requirements. One simple example is that of how long particular records must be retained and what it is to happen to them. In the University’s case this means complying the disposal authorities issued under the State Records Act. Ensuring compliance with the disposal authorities also means ensuring that personal information is not being kept for longer than is necessary. Where records disposal (I should stress that disposal does not necessarily mean destruction) is addressed in system design, there need be no concern in the future about how long particular records need be kept. In addition, the basis for retention or destruction is documented and linked to a legislative requirement. Needless to say, the success of this approach also requires close co-operation with our information and communication technology colleagues. In many areas, such as system security, our concerns coincide exactly. In others, we bring new perspectives to the discussion of business systems based on our knowledge of the operations of other parts of the University.

To a recordkeeper, being responsible for privacy has other advantages. It is sad but true that to most people recordkeeping does not figure highly in their consciousness, not many people are excited by filing! (Which is one of the reasons we want to make it automatic and invisible.) However, our experience has been that everyone has an interest in privacy. University staff are concerned to protect the information about students, alumni, employees and research participants. It is often simpler to initiate a conversation on privacy matters that have at their core a records issue. In a similar way, questions arising from new systems or processes about possible privacy implications often highlight recordkeeping concerns that need to be addressed to meet both the University’s own needs and to ensure compliance with the standards.

The above is a very broad overview of the role of ARMS in the University; many things have been glossed over or omitted entirely. I’m always happy to talk to colleagues about what we do. My email address and phone number are below and I’m always pleased to talk about what we do.

**Tim Robinson** is the University Archivist and Manager, Archives and Records Management Services. Tim is a graduate of Macquarie University and the University of NSW. An archivist since 1980 he has spent 27 years working in tertiary education. In addition to his other duties, Tim has managed privacy and access to information at the University of Sydney since 1993. He is the Chair the NSW Right to Information/Privacy Practitioners Network.

---

**Using Big Data to improve health and maintain individual privacy**

---

"Lest there be any doubt: big data saves lives."

*Big Data: A Revolution that will transform how we Live, Work, and Think*, Viktor Mayer-Schönberger and Kenneth Cukier 2013

The recent IAPP Global Privacy Summit 2013 had a full day dedicated to Heath - the Health Super Day, followed by 2 days covering a multitude of topics. Big Data was one of the hottest, with the launch of *Big Data: A revolution that will transform how we Live, Work, and Think*, and a dramatic presentation by the authors of the value and danger of Big Data. The example of a positive use of Big Data to achieve real time reporting in respect of the outbreak of H1N1 in 2009 was discussed, as it trumped traditional methods of disease management and response and it saved lives. There are plenty of other examples of how Big Data has been used in health and other fields, and this got me thinking about the different approaches to this by different societies and what direction Australia may take.

Researchers,Clinicians, Insurers, Regulators, Governments and of course consumers all have disparate agendas when it comes to health data. They do however generally share the goal of maintaining individual privacy and improving healthcare, so finding a balance between these competing demands in Australia will inevitably involve consideration of our particular philosophical approach to privacy. I will consider just two approaches to privacy which I believe are the most interesting in this context. On the one hand, there is the European rights based model (deontological approach) and on the other, there is the American market, or interest based model ( consequentialist). Deontology demands absolute respect for the moral integrity of the individual, irrespective of whether or not the actions result in 'good' outcomes, whilst consequentialist approaches are utilitarian, working out the desired outcome, and then deeming the means to be a right. Lindsay has described the differences between the two approaches as ‘…a choice between policies which have the objectives of maximising social welfare (usually conceived as the aggregate of summed utilities), and policies based on the protection of fundamental rights.'

It has been said that ‘...the utilitarian psychology in Australia legitimises the pursuit of interest, while the dominance of the [Benthamite] ideology negates the possibility of a genuine battle of ideas.' Consequently, it is possible that Australia would align itself with the United States in the view that data protection should be self-regulating to allow the free flow of information and commerce, rather than the European model which is concerned with the dangers of the free flow of data for what it could do to personal dignity and autonomy. It is suggested however, that when the data is as highly sensitive as health data, the expectations of society may shift to a desire for the higher forms of protection offered by a rights-based approach which will have significant implications for the degree of protection afforded by the remedies. Lindsay has argued that a rights-based approach would assist in regulating particularly intrusive forms of data processing, ‘thereby shaping technologies, whereas a consequentialist approach may be inclined to allow technological developments to be determined by the market.' So just where does that leave us with health, privacy and Big Data in Australia? It helps to consider what definition of privacy works best in this context.

Privacy goes to the heart of “individualism and individual autonomy” and health data is universally considered to be sensitive information which deserves the highest privacy protection. Privacy definitions have been attempted often and it has been said that all attempts fall short. President Obama recently referred to privacy as “the right to be let alone”, in reference to the famous statement by Judge Brandeis in 1927, and this definition works in respect of the challenges of big data and health information. It encapsulates the sense of each individual or ‘data subject’ having control over what information they release and the right to participate in information exchange at their chosen level.

Big Data however, depends upon participation for the collection of amounts of data which were not dreamt of when Australian privacy legislation was framed, or indeed when the OECD Guidelines or the EU Data Protection Directive were formulated. The interrogation of Big Data through algorithms provides us with invaluable research but renders our established privacy protections largely impotent.

Just as Facebook users have created their own levels of trade-off between the value of using the platform and the potential third party use of their data, we must now create a working model with medical data. Clearly there is no alienation among people, the very data subjects whose health researchers are attempting to improve. So for Big Data to be used for population health, the model needs change. As Professor Froomken put it, “…the great diversity of new privacy destroying technologies will have to be met with a legal and social response that is at least as subtle and multi-faceted as the technological challenge.” Given the widespread adaptation to social media platforms, loyalty programmes and the growing collection of Big Data and its potential benefits, such a response is warranted and possible.

Everyone needs to feel free from “dataveillance”, because being observed impacts on our right to live freely. However in the context of Big Data, “opt in” and other accepted privacy protections such as informed consent at the point of collection are largely impractical and ineffective. But just how worthwhile are these protections now? Consents are traditionally written in legalese and largely neither read nor comprehended – an ‘empty exercise’. Furthermore, consents are often binary in their terms, that is click here to consent, and if you don’t, click off. This means the consent is not truly voluntary or meaningful. In the context of Big Data, you can’t ask the data subject to consent, because there is no certainty about what their data will be used for, or when, because the value of the data is not readily apparent until analysis has begun. Indeed there are instances where data is being collected, such as Google searches on symptoms and cures, when individuals are not even aware that their data is being collected.

The *Personally Controlled Electronic Record Act 2012* (Cth) specifically requires optin, and as we know from statistics for organ donation, rates are very low when it’s opt in and up to 99% when it’s opt out. So is there a parallel with Big Data? It’s hard to imagine otherwise. If people are informed about the use of their body parts for the good of society and then not forced to actively make a choice, they appear to agree to donation. On the other hand if people have to actively make a choice and opt in, they seem to refuse. Privacy of sensitive information needs to be considered in the context of clear medical benefits versus the possible breaches of privacy. To this end the establishment of a workable approach to consent and opt out in a Big Data age is crucial. And trust in the ethics and safeguards will be a key part of any approach.

No discussion of Big Data in the health context would be complete without consideration of de-identification, re-identification and security. Internet generated attacks comprise “the most significant threat we face as a civilised world, other than a weapon of mass destruction.” These threats are global ones and there is little merit in attempting to combat such dangers with local rules.
Consequently attention to recent developments such as the release of the UK *Anonymisation Code* by ICO are instructive for Australia, together with recognition that most health consumers are now familiar with the risks and convenience of electronic transactions, and may welcome appropriate framework in the light of well publicised breaches. Providing transparency through public education about the benefits of using health data, not for specific detailed analysis but for massed correlations, as well as respecting consumer’s dignity through the most appropriate level of security and governance, are achievable and would seem one way of achieving privacy and using Big Data for health outcomes. This is consistent with a deontological approach, which seems reflected in the statement by the Office of the Privacy Commissioner in regard to protection of ownership rights and appreciation of the changes in the e-health space:

‘As health services are amalgamated and corporatised, and as e-health initiatives evolve to simplify the transmission of health information between providers, it is likely to be increasingly important for the use and disclosure of health information to be sufficiently regulated, and that health service providers and individuals share common understandings of how it will be handled. This is important to continued trust and quality assurance in the healthcare professions, as well as to patient’s autonomy and peace of mind, and the continued effectiveness of the Privacy Act.’

Healthcare Professionals are one of the most trusted groups in society. The fact that they are also usually at the collection point for health data means that their ability to harness the power of Big Data is not impeded by the usual barriers – lack of trust and access. Consequently there is a compelling case for the establishment in Australia of a workable governance structure around the collection and use of Big Data, which should also avoid the emergence of “Data Barons”; envisaged by Cukier and Mayer-Schonberger in *Big Data*.

**Emma Hossack,**
**President of iappANZ**

---

**Media Privacy in Print Media: Read all about it**

The Australian Government’s media regulation reform package, introduced into the Federal Parliament on 14 March 2013 and then unceremoniously abandoned 12 days later, gave prominence to the application of privacy law to Australian news and current affairs journalism. That prominence was unusual, unexpected and unprecedented.

One aspect of the Government’s response was particularly unexpected. The Federal Attorney General in September 2011 released an issues paper *A Commonwealth statutory cause of action for serious invasion of privacy* and called for submissions as to whether Australian should have a cause of action for serious invasion of privacy. Over 60 submissions were received. That review process has now been shelved without any Government substantive response to those submissions. The issue of whether Australia should have a new privacy cause of action has now been referred back to the Australian Law Reform Commission (ALRC).

The ALRC had already considered whether there should be a privacy cause of action and reported on it at length in Chapter 74 of the ALRC’s 2008 Report *For Your Information: Australian Privacy Law and Practice* (ALRC Report 108): this Report is, of course, what kicked off the privacy reform process. In 2008 the ALRC recommended that Federal legislation provide a statutory cause of action where the claimant shows that there was a reasonable expectation of privacy, where the act or matter complained of is highly offensive to a person of ordinary sensibilities and is either intentional or reckless, and where the interest of the person in privacy is not outweighed by any matters of legitimate public interest. It will be interesting to see now whether the ALRC comes to different conclusions following developments in judge-made law in other comparable jurisdictions (in particular, Canada and New Zealand) and criticisms of the ALRC’s formulation of the proposed cause of action that were made in submissions to the Attorney General’s review process.

Another aspect of the Government’s intervention was both unusual and unprecedented: specifically, a proposed linkage between the broad scheme of regulation of print media and privacy law. Journalism by individual media organisations in Australia has always enjoyed an exemption from the operation of the *Privacy Act 1988* where those media organisations are publicly committed to the Standards set by a body representing a class of media organisations.

Traditional print media (newspapers and magazines) has in recent years self-regulated as to privacy through the Statement of Privacy Principles and General Principle 4: Respect for Privacy and Sensibilities of the *General Statement of Principles* published by the Australian Press Council (APC) and administered through the complaints and adjudication processes of the Australian Press Council. Print media self-regulation administered by the APC covers many things unrelated to privacy, such as truth, balance, impartiality and fairness, corrections of inaccuracies, honest and fair investigation and preservation of confidences.

Traditional electronic media (free to air television and pay television) have self-regulated through *Codes of Practice* developed by the industry and as reviewed, registered and overseen by the Australian Communications and Media Authority (ACMA). The ACMA has also determined its own *Privacy Guidelines for Broadcasters* which the ACMA applies in administering complaints as to any non-compliance by broadcasters with these Codes of Practice. ACMA’s powers of enforcement of these Codes are significant and these powers have been exercised in a number of high profile rulings, including in the David Campbell case. The Codes and Guidelines together constitute what is now quite a prescriptive scheme of regulation of privacy in traditional electronic media, including a regulatory concept of serious invasion of personal privacy that is applied by the ACMA in determining complaints about privacy excesses in television news and current affairs reporting.

New media – blogs, online newspapers and other internet media outlets - is not so self-regulated. New media accordingly is potentially subject to the full operation of the *Privacy Act 1988*, except to the extent that particular new media outlets that are media organisations engaged in journalism publicly commit to observing journalistic standards that deal with privacy. Some new media outlets have published statements and complaints procedures that could be regarded as so complying. In 2012 probably the best known new media journalism outlet, *Crikey*, elected to join the APC.

Where a complaint about content of a newspaper or a magazine within the coverage of the APC cannot be resolved without formal adjudication of the complaint by the APC, the publisher is required to publish the Council’s adjudication in the newspaper or a magazine, promptly and with due prominence. The Council cannot require a correction or apology to be published: in the event that the matter is not resolved and proceeds to final adjudication, the Council may only require publication of the Council’s adjudication promptly and with due prominence.
The APC currently receives more than 450 complaints each year. About 75% of initiated complaints which are fully pursued by the complainant result in agreement for a correction, apology or some other agreed form of action.

The limited powers and sanctions of the Australian Press Council have proven to be controversial in recent years. These powers and sanctions were the subject of well publicised recommendations for reform made by both the Independent Inquiry into the Print Media chaired by The Hon. Ray Finkelstein QC and commonly referred to as the Finkelstein Inquiry, and the Convergence Review Committee. These bodies reported early in 2012. The media reform package introduced into the Federal Parliament on 14 March was the Australian Government’s first public policy and legislative (at the same time) response to the recommendations of those review bodies. In the meantime, one prominent media proprietor, the owner of The West Australian, had elected to disagree with rulings by the APC and struck out alone to set up its own Council, the Independent Media Council.

Criticisms of traditional print media self-regulation to date have generally not focussed upon allegations of breaches of privacy. For example, the ALRC’s 2008 Report had already considered the journalism exemption from the Privacy Act and concluded that there should be an “adequacy” criterion added to the qualified exemption. As stated by the ALRC, “[e]nforcement powers and sanctions are an important consideration to determine whether a particular media privacy standard is ‘adequate’ for the purposes of the journalism exemption.” However, there did not appear to have been a substantial unmet need for more vigorous privacy enforcement in Australian print media. Of complaints made about the Australian print media to the APC, complaints about invasion of personal privacy have (for so long as statistics have been made available by the APC) constituted a remarkably small percentage. For example, in 2010-2011 (the most recent year for which statistics are available), of a total of 566 complaints to the APC, only 30 complaints related to intrusion of privacy. Of the 85 complaints in that year to the APC that were not resolved and proceeded to adjudication, only 3 related to intrusion on privacy.

So the privacy focus of provisions of the News Media (Self-Regulation) Bill 2013 was intriguing. What was that privacy focus? The Bill operated as follows:

- The News Media (Self-regulation) Bill 2013 and the News Media (Self-regulation) (Consequential Amendments) Bill 2013 were directed at print media and associated online services rather than the television industry and associated online services. The Bills affected ‘news media organisations’, defined by reference to ‘news or current affairs activities’, but expressly exempting (1) activities relating to material disseminated by a licensed broadcasting service, and (2) activities relating to material disseminated by an online service that is associated with a licensed broadcasting service.

- The legislative package did not affect regulation of the television industry through Codes of Practice and associated regulation under the Broadcasting Services Act as administered by the ACMA. The ACMA would continue to regulate broadcasting activities and enforce industry Codes through use of the ACMA’s existing suite of powers and sanctions. The ACMA’s powers of enforcement of these Codes would remain unchanged. As already noted, the ACMA has determined its own Privacy Guidelines for Broadcasters which the ACMA applies in administering complaints as to any non-compliance by broadcasters with privacy-related provisions of these Codes.

- The Bills would have the effect that a specified ‘news media organisation’ would only continue to qualify for the ‘journalism’ exemption from the Privacy Act if the organisation was a member of a declared ‘news media self-regulation body’ and had not had its rights as a member suspended.

- The new Public Interest Media Advocate (the PIMA) as appointed by the Government under the associated Public Interest Media Advocate Bill 2013 would have the power to declare a ‘news media self-regulation body’. That power would require the PIMA to consider various matters specified in clause 7(3) of the Bill, which include the extent to which the body’s news media self-regulation scheme provides for remedial action to be taken by the body corporate, including the power to give remedial directions (including a direction to publish an apology or a correction) to a news media organisation. This is an entirely new requirement: the APC does not have such powers today.

- The PIMA would also have the power to revoke any declaration of a news media self-regulation body. The Government stated that contemplated that this power of revocation could be exercisable if a news media self-regulation body failed to suspend an organisation for failure to comply with the news media self-regulation body’s rules and determinations. The effect of any such revocation would be to leave relevant organisations that were no longer covered by a declared news media self-regulation body (whether because they were suspended by the news media self-regulation body for infractions of its rules, which infractions might be related to any matter covered by the rules, or because the PIMA revoked the declaration of the media self-regulation body) and therefore subject to the operation of the Privacy Act.

Could a media organisation engage in journalism without availability of the journalism exemption? Probably not. Availability of this exemption is critical to news gathering and current affairs.

Investigative journalism would be severely hampered, if not made impossible, if a number of the National Privacy Principles (NPPs) (and from March 2014, Australian Privacy Principles (APPs)) applied to a media organisation. These include:

- A right for a person to access personal information held by an organisation about the person and to correct inaccuracies (NPP 6).

- A requirement for an organisation which collects personal information about an individual from someone other than the individual to take reasonable steps to ensure that the individual is aware of this, either at the time of collection or as soon as is practicable after collection, and also made aware of (among other things) the fact that he or she is able to gain access to the information, the purposes for which the information is collected, and other organisations to whom this information may be disclosed (NPP 1.3 and 1.5).

- Restrictions as to trans-border data flows of personal information (NPP 9) could significantly hamper syndication and other news sharing arrangements.

- Requirements as to data quality (ensuring that personal information retained is accurate, complete and up-to-date) (NPP 3) and limits as to the period of retention of personal information beyond the period for which it was reasonably necessary to retain it for the purpose for which it was collected could significantly hamper retention of backgrounders in newsroom libraries.
In addition, media organisations would become subject to the jurisdiction of the Australian Privacy Commissioner in relation to findings that an act or practice was an interference with the privacy of an individual. Among new penalties and sanctions which will come into effect (under already enacted laws) from March 2014, the Australian Privacy Commissioner may require a party to give enforceable undertakings and may make remedial orders in respect of a party.

So was the Australian Government’s media regulation reform package an unprecedented and fundamental attack upon the freedom of the media in Australia, as some media outlets claimed? It is certainly true that freedom of speech in Australia rests on narrow foundations, in the absence of a constitutional basis for freedom of speech outside the judge-made law around the implied constitutional guarantee of freedom of political communication and the indirect protection of human rights through Australia’s accession to the International Covenant on Civil and Political Rights. But regardless of freedom of speech concerns, the unusual and unprecedented aspect of the media regulation reform package was the linkage of the entire scheme of print media regulation to the journalism exemption from privacy law. As already noted, current standards and most complaints addresses things unrelated to privacy, such as truth, balance, impartiality and fairness, corrections of inaccuracies, honest and fair investigation and preservation of confidences. On statistics to date, over 90% of complaints that might lead to unremedied infractions of standards might be expected to be completely unrelated to privacy.

So was the linkage of the general scheme of media regulation to privacy law proportionate and reasonable regulation? Arguably not. In this context, the vociferous debate in the print media about the Australian Government’s media regulation reform package was not unexpected. What is unexpected is that the former backwater of media privacy law should be thrust into national prominence in this way.

Peter Leonard is a partner at Gilbert + Tobin Lawyers and a Board Director of iappANZ

Upcoming Privacy Events

Melbourne | ISA’s Big Data 2013 Conference April 18 & 19
Click here for more information

PAW EVENTS

Please join us for breakfast at the Office of the Australian Information Commissioner’s launch in Sydney on Monday 29 April

Data Safety Workshop in Wellington, NZ on Monday Wednesday 1 May
Whether you’re a business, a government department or a community organisation, this workshop offered by the Office of the New Zealand Privacy Commissioner as part of PAW will give you some great tips on how to get things right. Click here for more information

Lunch hosted by Corrs Chamber Westgarth in Brisbane on Wednesday 1 May
A briefing lunch by Australian Privacy Commissioner Timothy Pilgrim will take place at 12.30pm at Level 35, 1 Eagle Street, Brisbane.
Please register your interest with Sara MacQueen on (07) 3228 9406 or Sarah.MacQueen@corrs.com.au

Breakfast briefing hosted by Norton Rose with McAfee in Sydney on Thursday 2 May
More details to follow...

Breakfast briefing hosted by Norton Rose with McAfee in Melbourne on Thursday 2 May
More details to follow...

PRIVACY AWARENESS WEEK in NZ

iappANZ in conjunction with KPMG will be hosting an event in Wellington NZ, on 1 May at 4pm with former Australian Privacy Commissioner Malcolm Crompton presenting.
More details to follow...
Privacy is a growing concern across organisations in the ANZ region and, increasingly, privacy-related roles are being made available only to those who can demonstrate expertise. Similar to certifications achieved by accountants and auditors, privacy certification provides you with internationally recognised evidence of your knowledge, and it may be the edge you need to secure meaningful work in your field.

The International Association of Privacy Professionals (IAPP) says:

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

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

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

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

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

*What about testing?*

Although the IAPP website refers to US-based certification testing only, testing is available to iappANZ members locally.

The IAPP will continue to manage certification registrations and materials, but you will now be able to set an appointment to sit your exam online at a testing centre in Australia or New Zealand.