The heatwave moving up the Eastern Coast assures us of a very warm Christmas as we pack up our offices ready for the summer holidays. A perfect time to reflect on some of the major privacy shifts in Australia and overseas. Both the 2012 whitepaper by Professor Cate and the recent address by Viktor Mayer-Schoenberger at the iapp European Data Protection Congress propose a new approach to privacy. It is suggested that traditional consent, notice and specified use could possibly be replaced by an obligation upon organisations to take responsibility for the protection of individual’s privacy.

Here in typical Australian fashion, we are just getting on with it. APP 1.2 will make APP entities responsible for having and implementing a privacy framework. Australia will be putting into practice the proposals discussed overseas. Is this a world first?

Australia has always liked to stand up for the little guy. We loved watching Darryl Kerrigan in the film “The Castle” take on the big end of town and win. “The vibe” of powerful large organisations destroying simple lives just seems wrong to most Australians and this is mirrored in our new privacy laws. The recent OAIC survey on consumer’s attitudes to privacy also indicates that over 60% of Australians will not do business with organisations who do not respect their privacy. Consequently even organisations not bound by the APPs are likely to take notice and review their practices to protect their market. Let’s hope that the new laws are rewarded with some other world firsts in creative privacy frameworks.

Merry Christmas everyone and a wonderful 2014 from the iappANZ Board.

President’s Letter

By Emma Hossack
President
emma.hossack@iappanz.org
m:+614111478799
Our last bulletin follows for 2013, and with the launch of the Privacy Unbound title with thanks to past Board Director, Samantha Yorke for inspiring the name to carry us into what will be an exciting time for privacy professionals throughout our region. For those of our members that could not attend our Privacy Unbound summit last month, we are pleased to include a snapshot of some of the presentations that were given by experts from all parts of the world. We have sent video links to all the presentations to our members who will have immediate access to some insightful presentations by our international and local speakers. I am certain that this will be particularly useful in early 2014 when we return to our professional lives after some well deserved leave and launch into further preparations for compliance with new privacy regime that will become reality in the not too distant future. I know that I will most certainly be returning to view some of the key messages around data security, credit reporting, big data and global privacy regulatory trends that were discussed at the summit. For those that missed the winning article from James Kelaher on information and its value, we have republished the thoughtful article along with a profile so you can learn more about the author.

Many thanks to all of our contributors throughout 2013 with their valuable insights and thought provoking pieces on significant issues and trends in privacy. We are fortunate to have an engaged network of professionals who generously share their know how and continue to inspire dialogue, debate and raise awareness amongst us all.

Happy holidays to all and happy reading.

---

**Privacy Unbound Summit Wrap**

*by the iappANZ Board of 2013 and iappANZ sponsors*

**Introduction**

In the luxurious surrounds of The Westin Sydney, the 2013 iappANZ Privacy Summit was kicked off by a lively and interactive speed-dating session for the early risers. Seven speakers and privacy professionals moved (and grooved) around the tables and spoke briefly on a range of privacy topics. The Summit was officially opened by The Hon. Michael Kirby AC CMG who cast us back to the development of Australia’s inaugural privacy principles.

**Keynote International Speakers – Danny Wietzer, Richard Thomas and Mikko Niva**

**Danny Wietzer MIT USA** *(by Melanie Goldwater)*

Daniel Wietzer enlightened us about the path to genuine privacy protection in today’s world, challenging current illusory definitions and frameworks. Given that personal information is often already out there – and what isn’t can often be inferred without any involvement from the data subject (for example, from shopping purchases and social networks), Daniel encouraged practitioners to recognise that current privacy mechanisms such as consent no longer protect real privacy risks. He challenged the modern mantra that “privacy is dead”, demonstrating that whilst secrecy may no longer be valued and hence protected in an interconnected world, privacy...
(conceptualised as legitimate usage and disclosure) is not. Finally, Daniel put forward a model of accountability by which entities could examine and demonstrate how personal information is used by them and the degree to which they comply with any given set of rules. This type of model would enable us to address the “difficult bits” openly and transparently with the core values of our community at the centre—a “no fig leaves” reality check on privacy.

Richard Thomas CBE LLD (UK)

The delightful Richard Thomas shared with us some of the major privacy issues and cases he worked on whilst UK Information Commissioner. The life of the Commissioner is clearly anything but dull. Cases such as the British Government losing 25 million child benefit records on two discs, the leaking of the personal information of Muslim soldiers leaked and the loss of the data base of a whole prison population database lead to changes to the Commissioner’s audit powers and the ability to impose fines—which Mr Thomas noted have since been used by his successor Christopher Graham.

In 2006, Mr Thomas tabled a special report in Parliament, What Price Privacy, recommending jail sentences to deter the illegal trade of confidential personal information. The British Government agreed to introduce but not activate the sentences. Six months later the phone hacking scandal erupted. However this well within the remit of the police rather than data protection. The reports from the Leveson Inquiry recommended activating the privacy prison sentences and while this still has not been done, Mr Thomas observed that the public profile of privacy has been raised in the UK.

In relation to proposed changes to EU data protection laws, Mr Thomas expressed the view that they are too prescriptive in seeking to mandate exactly what organisations must do, making this even more burdensome than the current regime.

Nikko Miva, Director of Privacy, Nokia Corporation (Finland) (by Veronica Scott)

The take-away from Nikko's presentation was a better sense of how to approach privacy compliance. First it is important to understand the problem—whether complex or simple information flows. Then a solution needs to be implemented with the aim of respecting individual privacy. Nikko explained that implementation is done through:

- executive accountability and oversight;
- policies and processes to implement executive accountability and oversight—specific policies and processes for different products and services, code of conduct, a general privacy statement, identifying repeatable patterns (eg. cookie notices);
- staffing and delegation and
- education and awareness.

Big Data Panel: Privacy and Big Data Panel (Insights from McAfee by Joel Camissar, McAfee Asia)

Joel was a speaker and panel member. This is an abridged excerpt of his presentation prior to the panel discussion.

We’re still very much in the early stages of a big data revolution, and issues around customer privacy are still emerging. In fact, big data is a mystery for many organisations; everyone talks about it and assumes others are all having a great big party with it, but the truth is that right now, only a relatively small number of organisations regularly employ big data tools and techniques. As a result, big data stories related to privacy invasion are limited to rare occasions, such as the infamous case of Target allegedly using an analytics program that enabled the company to predict a teenage girl was pregnant before her father heard the news. But it’s not hard to imagine things changing—of the public becoming increasingly wary of big data as it starts to become more intrusive on our lives.

Despite the teething problems, big data is a powerful platform. It can offer great leaps forward in medical research and through smart profiling reduce fraud and malicious internet activity to keep us safe.

However, guidance from industry advisors, government manuals and existing data mining platforms is largely lacking any reference to privacy or security in recommendations on big data collection and usage. And so we find ourselves in a kind of Wild West for Big Data where we are still working out what best-practice security and privacy standards should look like.
Our parent company Intel is helping to shape the agenda in the technology and security open source community to put an enhanced array of security enhancing provisions around big data platforms, such as Hadoop.

Intel’s open source effort is called Project Rhino and, using Hadoop as an example, aims to create a common framework for encryption and authorisation to prevent operators from having access to customers’ personally identifiable information (PII).

Intel also offers the capability through its hardware acceleration AES-NI chipset the ability to encrypt at speeds of up to 20 times faster big data platforms like Hadoop. This removes a common argument that encryption adds too much overhead cost to such a platform and also helps provide an enhanced platform for data security. When big data becomes democratised, powerful, easy to use and inexpensive, programs will become widely available that allow users to comb through large data sets and identify meaningful patterns useful to their business strategies.

On the road to this level of accessibility, businesses need to look at how privacy is built into big data projects at the organisational level. Big data analytics processes need to follow the same processes as other organisational systems containing customers’ PII, which are designed to protect privacy. It’s clear to me that if we are to shape the regulatory debate and influence public policy to protect privacy, we need to ensure businesses understand the importance of responsible use of big data against competing interests that sometimes puts privacy on the backburner.

Timothy Pilgrim, Federal Privacy Commissioner, OAIC on what to expect from the privacy reforms (by Melina Rohan)

Characterising the 2014 reforms as the third act in the Australian Privacy story (where the first act was the introduction of the Privacy Act in 1988 and the second was the introduction of the National Privacy Principles in 2000) Australian’s Privacy Commissioner, Timothy Pilgrim, addressed the following questions on all privacy professional’s minds in Australia:

a) What will be the OAIC’s approach to enforcement post 12 March 2014?

b) The drafting style of the supporting guidance and the OAIC’s interpretation of the new laws?

c) What will a post 12 March 2014 world look like?

Before addressing these questions, the Commissioner warned that Australian privacy professionals should not expect to see a final act, because privacy continues to be a dynamic concept. He noted though that the one thing that remains unchanged is the community’s attitude to privacy as confirmed by the 2013 Community Attitudes to Privacy Survey.

What will the OAIC’s approach to enforcement be post 12 March 2014?

In response to the question of whether the OAIC would take a softly softly approach to compliance from March, given the changes will have just taken effect, the Commissioner explained that the OAIC will always look to work within its ‘enforcement pyramid’ of seeking to resolve privacy matters through conciliation and allowing the organisation to resolve the issue in the first instance. However this did not mean that he would be taking a soft approach to conciliation. He intends to use his new monitoring and enforcement powers through own motion investigations, privacy audits (to check compliance with the Act), making determinations and accepting enforceable written undertakings, and, if necessary, applying for civil penalty orders (which can be up to $340 000 for individuals and up to $1.7m for companies).

The bottom line is make sure that any changes your organization needs to make to be ready for compliance with the new privacy regime, are in place by March 2014.

The drafting style of the supporting guidance and the OAIC’s interpretation of the new laws?

The Privacy Commissioner also provided an update on the work that is currently occurring to develop privacy guidance.

There have been three stages of consultation with submissions on the final stage due on 16 December 2013. The Commissioner highlighted the great and largely positive responses received via the consultation process and the useful feedback that will inform the final guidance documents.
Key changes that privacy professionals should expect to see in the final guidelines include:

- Addition of further nuance with respect to the use of ‘must’ to reflect mandatory practices required to comply with the law as opposed to ‘shoulds’ which highlight areas where the guidelines seek to outline best practice and ‘coulds’ which are steps that are not possible for all organisations;
- More practical examples
- Further clarification with respect to definitions such as ‘Australian link’, ‘use’ and ‘disclosure’; and
- Further information on how to create layered privacy policies through linking APP1 and APP5 obligations.

What will a post 12 March 2014 world look like?

The amendments to the Privacy Act will result in quite a different privacy regime in Australia to the current system. APP 1 introduces the important obligation to take a ‘privacy by design’ approach as well as sets out that APP entities must be open and transparent in their management of personal information. APP1 sets the ground for compliance with the other 12 APPs and Mr Pilgrim noted that APP 1 was an important place to start when assessing compliance with the changes.

The strong relationship between APP1 (open and transparent management of personal information) and APP 5 (notification of the collection of information) which outlines the circumstances in which an entity must notify an individual of the collection of their personal information and details the matters about which the individual must be aware. APP 5 is, in the majority, the same as the currently requirements with the exception of the new requirement to notify individuals about the access, correction and complaints processes in their APP privacy policies and also the location of any likely overseas recipients of individuals’ information.

APP8 addresses the growth of global flow of personal information and the many different ways in which personal information is used, disclosed and stored overseas these days. APP 8 states that in certain circumstances entities will remain accountable for an act or practice engaged in by the overseas recipient of personal information, if that recipient does something that would be a breach of the APPs.

Final Remarks

The Privacy Commissioner concluded by advising that APP entities should be taking steps to ensure that they are fully compliant with the new privacy obligations come March 2014. Key steps to achieve this include:

- Reviewing and updating your APP privacy policy
- Reviewing information security arrangements
- Reviewing data breach plans
- Conducting privacy impact assessments for new projects consistent with a privacy by design approach.

Chris Gatford of Hack Labs on Security Breaches (by Kate Reynolds)

Chris Gatford, who ‘hacks the corporate world for a living’ shared some fascinating insights into some of the ways that companies fail to protect themselves from security attacks. Chris’s company, HackLabs, performs penetration testing on organisations to test both their physical and IT security postures. While very well known on the IT Security circuit, the Summit was the first time Chris has spoken to privacy professionals, and he acknowledged that security and privacy professionals need to work together now more than ever before.
Chris shared with us several entertaining anecdotes about how simple mistakes can undermine security controls including:

- the security camera in a Sydney rooftop car park which could have its view blocked simply by parking a van in front of it;
- the office building where one set of turnstiles did not work because they had not been paid for, so anyone could walk into the building; and
- photos posted online where usernames and passwords are clearly visible stuck to the wall in the background.

He reminded everyone that it is often the simple attacks that are the most effective and that organisations and individuals make this easier by posting a wealth of information online that can be used to craft exploits.

Chris also shared some scary statistics. Over the last year and the 100 penetration tests that companies had asked HackLabs to conduct, 33% of the time they managed to get system level access to the operating system. Furthermore, 65% of all vulnerabilities exploited in web applications during testing led to the extraction of personal information.

Chris wrapped up his session by sharing with us some of the inventive ways that HackLabs manages to circumvent physical and IT security controls during their testing. The audience were encouraged to join in, and it appears we may have some potential penetration testers amongst our members as some of the suggestions were spot on!

Privacy Workshops:

**Health Check-up** (by Emma Hossack)

If you thought privacy of health information was just one of the most critical areas of privacy, this workshop would probably have changed your mind. Privacy can be a matter of life and death in healthcare.

Dr Richard Kidd, eHelath champion and former AMA Qld President gave a compelling presentation about handling the conflict between accessing and protecting health information. Dr Kidd discussed youth suicide which resulted from mismanagement of personal information. Dr Kidd also highlighted the difficulty for clinicians who naturally need as much information as possible to make the best decisions. He strongly supported the use of appropriate shared electronic health records and noted concern with the usability and privacy of the National personally Controlled Electronic Health Record system.

Andrew Took, a lawyer with clinical qualifications who works with the AMA in medico legal cases provided a fascinating presentation, well worth watching as he gave us many ‘war stories”. These covered an explanation of circumstances in which ‘imminent threat to a third party’ would apply (including patient disclosing to psychiatrist homicidal intentions), the importance of having procedures in place to protect against vicarious liability (eg. employees incorrectly accessing and disclosing personal information) and the sensitive issue of when it would be appropriate to deal with couples together (on the basis that they have the same doctor).

Alison Flannigan, a partner at Holman Webb Lawyers gave an overview of health privacy laws at both State and Commonwealth level. We came away with some tips on the application of the changes to the Privacy Act on health records:

- there are special rules for health records: use or disclosure is permitted if there is a serious and imminent threat to the health and safety of an individual; disclosure is permitted for compassionate reasons (eg. where the person is unconscious) and there is a restriction on access if providing direct access would pose a serious threat to life or health of an individual (although there is the possibility of providing information to an agreed intermediary).
- public interest determination No. 12A allows for collection of family, social and medical histories in certain circumstances
- the new definition of personal information may capture photographs of individual body parts (if distinctive enough eg. birthmark);
- there is now more uniformity between NSW and Victorian legislation and Commonwealth legislation with the inclusion of ‘permitted health situations’ as a general exception for operation of APPs;
Data Transfers and Breaches

Anne-Marie Allgrove from Baker & McKenzie, Steve Wilson, Lockstep Privacy & Engineering Consultants and Julie Inman Grant, Managing Director, S2P2 took the workshop through a hypothetical data security breach (we all hope not to have to go through) where a rogue employee in a local online mobile application business transmits a virus leading to personal information being leaked in various jurisdictions where its own cloud storage facilities and cloud storage facilities operated by third party service providers on its behalf are located. Encryption was discussed and it was noted that this is not a magic solution and would not have stopped a rogue employee who would likely have had the encryption keys. Access controls is a key issue as well as the certification of vendors.

The session also considered how to decide what jurisdictions are ‘substantially similar’ to the APPs for the purposes of APP8.2. The adequacy findings in the EU were identified as possibly providing some assistance or at least could assist with due diligence on the jurisdiction in which the overseas recipient is located.

The balance in favour of policy rather than technology responses to security events was noted as a key area for improvement to ensure technical engineers did not get mixed messages that ‘privacy is not a technology issue’. The use of language that technology people understand was needed. For example, with data breaches where there is a ‘real risk of serious harm’, it was suggested that risks can be mapped in accordance with risk management standards that technology engineers work with every day (such as AS/NZS 4360 and ISO 31000). Privacy risks should be added to the IT security threats that are already identified.

Credit Reporting (by David Templeton)

I moderated this session which was presented by Olga Ganopolsky, General Counsel at Veda, Australia and New Zealand’s largest credit reporting bureau who delivered an overview of the comprehensive consumer credit reporting system that will be introduced in Australia on 12 March 2014.

The new system will add data about consumer credit commitments and repayment history to the credit database. The new data will sit alongside the existing data sets that focus on enquiry and default data and critically, identification data needed to ensure that credit information is properly associated with the correct subject. The addition of the new data will bring Australian credit reporting into line with other developed economies.

Olga personalised the session by taking a note of each attendee’s particular concerns and addressing each in the course of her presentation, which was clear, succinct and cleverly structured to keep her audience engaged at each step of the journey through a complex raft of provisions. She led us through key matters including:

- the important distinction between consumer credit information (regulated) and commercial credit information (unregulated), and the revised treatment of investment lending related information which will be brought within the definition of consumer credit information
- notice and consent requirements
- a short survival guide of the key definitions
- changes to the scope of currently reported data
- interaction between the Privacy Act, regulations and new Credit Reporting Code
- the importance of prompt resolution of consumer concerns, and the important consumer-centric rationale for the first point of contact system which will allocate responsibility for managing consumer concerns
- the right of consumer’s to freeze their credit information where they are a victim of identity takeover
- the practice of pre-screening and the prohibition on use of credit information for marketing; and
- new powers to the OAIC and new penalties.

There was general consensus that the new credit reporting provisions, which entirely replace the existing Part III A of the Privacy Act, are just as complex as the old. Credit reporting remains an area that is regulated separately from other forms of sensitive personal
information, and the legislation is drafted to subject use and disclosure of credit information to blanket prohibition unless all the conditions of the exceptions required to deal with credit information legally are met.

All said and done, Part IIIA is dead, long live Part IIIA!

**Global Panel: What's next? Predictions and challenges?** (by Veronica Scott)

To wrap up the Summit, our three international speaker participated in a panel discussion and gave us their insights into the future and where Australia stood in relation to global privacy. It was food for thought.

*How has Australia fared?*

In short Mikko Niva said that Australia has been identified by global organisations as being a privacy risk and Danny Weitzner was not sure how well privacy is in fact understood in Australia. While we have a similar approach to the UK, he finds our government intelligence access to personal information feels closer to the USA. Richard Thomas thought that overall the perception of Australia is that privacy is taken quite seriously but it is not so deeply rooted as in European whose system is based on privacy as a fundamental human right. This has its roots in history- where most European countries know what impact an impact a system of tyranny can be, where personal information is misused.

*The global privacy blocks*

Richard described the global blocks of privacy as:

- the broad European approach (with UK and Ireland detached);
- the North American approach (Canada and Mexico detached);
- the Asia Pacific approach (comprising New Zealand and Australia and Hong Kong, and the rest of the region detached); and
- finally, the rest of the world (including India, China, Africa, but noting that South America is largely heading down EU route).

*A multi-jurisdiction approach leads to innovation...*

Danny's view is that diverse approaches to privacy are not a problem, he believes they foster innovation/productivity, although he does consider that the global principles of APEC are important. Richard agreed, expressing a preference for the interoperability between jurisdictions rather than an internationally standardised privacy law.

'We are sleep-walking into surveillance'

Richard also sounded a note of caution in relation to the increasing surveillance of society by government agencies in the name of security and questioned how much privacy regulators and laws could do about it. A limitation on the uses of this information was important.

*What about privacy by design?*

Mikko noted that the concept of privacy by design was critical but had not been discussed in great detail at the Summit.

*The end of the notice and consent model*

And on a final note, a challenge for all organisation in Australia, Richard questioned the modern day consent model where collection notices are longer than a Shakespearean play. His challenge – that notice and consent models have perhaps now run their course.
Conclusion

So what should the new model approach be? How will Australia fare with the commencement of the reforms to the Privacy Act - will we embed privacy by design in our organisation? How will we deal with the challenges of a surveillance society as we learn that Telstra is vacuuming up huge amounts of metadata for the Australian Government intelligence agencies.

Join us again at next year’s Summit in November 2014 (which we are already planning) to find out more.

Winner of the iappANZ inaugural writing prize

*** James Kelaher ***

It is with great pleasure that we re-publish the winning article of this year’s inaugural writing prize written by James Kelaher as published in the May 2013 Bulletin. James has also joined the iappANZ 2014 Board. James kindly agreed to be profiled for the Bulletin too.

Security and Privacy – A rethinking Information and its value

As an accountant who has developed an interest in privacy as a result of my work in government and business, I am continually surprised by the different perspectives that I encounter as I commute between these four worlds.

Information as an Asset

Increasingly many businesses are founded on the way that they collect, compile and use data; in fact one will often see businesses claim that ‘information is the key to our business’. The same is true of government, where information about program registrants and recipients of services, collected from the public over many years, is fundamental to the fulfilling of their service delivery charter. In both these cases, information could be correctly – and often is – called an ‘asset’.

Certainly, if a business or government agency lost access to, or confidence in, its information holdings, it would struggle to function. In both cases, the cost and inefficiency of operating would be prohibitive. In the case of government there would be a huge tax-payer backlash if an agency was required to start from fresh and had to re-collect all the data that people have previously provided. In fact we often see this playing out when an agency is unable to access existing client data for privacy or data accuracy reasons and needs to initiate some kind of stand-alone registration process; new registration levels are low and clients and staff are frustrated by the processes involved. In other words the creation of ‘information’ can be costly for all parties concerned and there can be good reasons for getting as much (re)use out of it as possible.

Information as a Liability

However, from a legal and privacy perspective, many categories of information holdings should be kept to just the minimum necessary for functions to be performed and legislation to be complied with. Certainly any personal information held needs to be carefully
secured, kept up to date and accounted for. (By the way, the same can often be said of commercial information.) In many respects, this kind of information is not so much an asset, but a potential liability; because of the potential risks and costs that are entailed for both the organisation holding the data and the other parties to whom the information relates, if a breach occurs.

So, it appears that information can be an asset for some and a liability for others, depending on the circumstances.

Accounting for Information

According to the accountants, whose standards are now part of the global fabric of government and business accountability, information – especially personal information – is generally neither an asset nor a liability. This is because, according to international accounting standards, an asset basically represents ‘future economic benefits, controlled by the entity as a result of past transactions or other events’. In other words something that has a calculable financial value and can be converted to cash now or in the future, such as raw materials, a licence, a machine, a building and so forth; something tangible.

That is why you don’t see in the annual financial statements of Medicare, Telstra, NAB, Wesfarmers, BHP-Billiton, Centrelink, Australia Post or the ATO the billions of dollars spent on collecting and compiling all of the data about customers, patients, families, employees, suppliers, hospitals, income, and so forth. This information is not tangible.

Interestingly, in the 1970’s about 80% of an organisation’s value was determined by the tangible assets it held. Nowadays, according to a study of the top 500 listed companies in the US, only 20% of those companies’ value is represented by tangible assets, the rest is made up of brand, knowledge and information – these are the assets that generally determine the value of a modern organisation. But, for the most part they are not on the ‘balance sheet’, even if the computers, whose only function is to collect, store and use the information, are.

Over many decades we have all been inculcated with the need to preserve assets: to guard against stock leakage or inventory theft, to sign for the custody of goods delivered and to participate in stock takes. We implicitly understand these practices to be part of the organisational custodianship process. In more recent times, we have come to recognise the importance of ‘human capital’ and the associated processes of caring for and investing in people. I am sure you can see where this is heading.

But what about the other side of accounting: liabilities, where accountants record the value of ‘future sacrifices of economic benefits that an entity is required to make as a consequence of past transactions or events’. If an actual event has occurred (such as the delivery of goods which must be paid for by a certain date) or it is known that it will very probably occur (such as an obligation to pay a settlement in a commercial dispute), then a firm must record a liability for the amount concerned on its balance sheet.

But an organisation cannot create a liability on its balance sheet ‘just in case’ a possible adverse event might happen in the future. That would be equivalent to reaching into the pocket of the owner or the tax payer to say, ‘look, I am a bit anxious that there is going to be a stuff up – so give me some money now, so that if it happens, I can use your money to buy my way out of trouble’. That is what good management practices, and sometimes insurance, are for – to mitigate risks.

So, while the potential for a privacy breach cannot be recorded as a liability on a firm’s balance sheet, if one does actually occur and compensation or fines must be paid, then it can be. Ah, the logic of accounting!

Should we Change the Rules?

Yes, I say! Because if people thought about information differently, they would do a better job of collecting, using, protecting, disclosing, and governing it.

Just imagine the attention that would be focussed on government information custodianship if the information held by agencies was valued and treated as an asset – imagine the size of the balance sheet numbers.

Imagine the impact on company management practices of information holdings that had to be classed as a potential liability, or which had to be written down due to impairment.
Just imagine if the market required that a data breach notification be accompanied by a financial statement, which set out the value of – and impacts on – an organisation’s information asset holdings. I think you would see some new management practices and priorities emerge very quickly.

Knowing the speed with which accounting standards change, it could be quite an ambitious undertaking to get the value of an organisation’s information recorded on its balance sheet – as either an asset or a liability. But I think it is high time that we started to debate this, because even the debate and awareness will produce a positive change in attitudes and greater awareness of good information and privacy practice.

Surely in this new information economy, we should be recognising that, implicitly we are already attaching value to information. At present those values are somewhat subjective, and in some cases only used when it is advantageous to do so. I guess if the traditional accounting profession does not take up this challenge, we may see a new discipline of ‘information accountants’ emerge and as experts in this field, maybe they will go after 80% of the fees!

---

Profile of James Kelaher

By Veronica Scott, iappANZ Board

James Kelaher, is a Director of the Smart Group, comprising Smartnet. He is a Fellow of the Australian Society of Certified Public Accountants, a member of the Australian Institute of Company Directors, the Risk Management Institute of Australia and the Institute of Privacy Professionals. He is also now an iappANZ Board Director.

1. Congratulations on winning the inaugural prize James. Can you tell us what motivated you to write about what privacy means for you?

I came to privacy quite late in my professional career, most of which has been about implementing major projects. After working in fields such as defence and homeland security, I found myself working in the health field just as technology was starting to move out of corporate environments and into the hands of consumers. I also started to do more travel in a professional capacity, looking at how technology was being used to deliver services, as the internet started to open up. So I was fascinated and challenged by the tensions between powerful new ways of enabling people to benefit from the digital economy at the same time as there were all sorts of concerns that needed to be addressed. It seemed that wherever I went there were examples of projects which had lost momentum or failed because the people responsible had lost the confidence of key stakeholder groups, Frequently there was a privacy dimension involved, especially with government projects.

One of the key reasons why projects lose stakeholder support is that the risks start to outweigh the potential benefits for one or more key groups. When this starts to happen with privacy or information security it can be difficult to reverse, because as we all know, retrofitting a bad design often makes the situation worse, or even terminal.  I have learned through experience that it is better that privacy is a fundamental building block, especially when these days, most projects have a very large technology and service delivery component. So I chose to write about privacy from a slightly different perspective, designed to get people thinking about some of the dated preconceptions that can lead to blinkered thinking about privacy and to highlight some examples.

2. How did you come to be a privacy professional – tell us a bit about your company Smartnet?

Smartnet was formed about eight years ago, after I had been working on some large government projects in the human services area, such as taking Medicare online and enabling health funds to share data with Medicare so that if someone received treatment in a private hospital, they could receive a single estimate for any out of pocket expenses and a single bill. I learned a lot on these projects and could see from my interactions with other countries in Europe, Asia and North America that chip technologies, mobile devices and cloud services were going to change everything. I wanted to be a part of that in a way that was not possible within government at the time. So I left and set up a business that was focussed on these things. Over time we have grown to also become investors in
technologies and solutions, but we still maintain a very active consulting practice, focussed on successfully implementing large technology projects and achieving the levels of consumer adoption and process reengineering necessary to achieve game-changing returns. Recently I have also become involved with the Department of Industry, helping to develop strategies that can shift Australia back into the top league of clever, highly competitive nations; this too, is very stimulating work.

3. **What are your favourite app(s) and why?**

I have a few, of course. My current favourite is called ‘unstuck’. It is available from the iTunes store. Unfortunately it is presently only fully useable on an Apple ipad. But you can find some general information about it on the web. I like it because it takes a universal and complex problem that we all encounter (I am lost, confused, unsure what to do) and applies clinical tools and concepts in an engaging digital way that is very accessible to any person (albeit, with an ipad!). It demonstrates many of the things that can help bridge the gap between technology and humans.

I am also a big fan of Sonos, the cloud-based sound library system that enables you to stream all of the music and radio in the world to a different speaker in each room of your house, using a downloadable app (and some very nifty speakers). The area that I presently do a lot of work in and where we have made a few investments, involves apps for digital credentials and eWallets. But that is a whole other story.

4. **You have just joined the board of iappANZ for the first time – welcome. What do you think iappANZ can offer its members at this stage of privacy developments?**

I have been a member of the iapp for a little while now and have been to the annual privacy summit the last three years, I think. So I have watched it develop to some extent and in my field I often meet members. But I have been blown away by the calibre of people on the board, the way that the board operates and the induction process for new board members. So I am looking forward to the year ahead.

Of course one of the major events in the coming year will occur in March 2014, when the new Australian Privacy Principles are introduced. These will apply, as most readers know, to all federal government agencies and the private sector. Though not, for the present, to state government agencies in those states that have their own privacy legislation (which is most of them). So, while the new Australian Privacy Principles are a big step towards a standard, national privacy regime, we are still not there yet. And, it needs to be said, the new APPs contain some complexities. So a major benefit that the iapp will offer to its members is a forum for exploration and clarification of how the new regime will operate. If companies or federal agencies get it wrong, the consequences can be significant, so being able to canvass issues with professional colleagues and experts is very useful.

5. **How did you find the iappANZ Summit this year?**

I found the iapp summit to be really good. There were great speakers, I thought the ‘hypotheticals’ were a really good initiative for sharing knowledge and networking, and there were some clever new initiatives. I particularly liked the coloured badges that people wore, indicating what part of the privacy field they worked in. And of course having Michael Kirby as a keynote speaker together with other luminaries from around the world was fantastic.

6. **What books are you reading at the moment?**

I am reading a few different things at the moment. I am nearly finished a book about dogs, called ‘Inside the Dog’ which is a great read for dog owners and covers everything from the design of their snout through to how they think (or, to be more correct, how we think they think). I found it amazing to learn that dogs are descended from wolves. I look at our Maltese Terrier-Cross in a whole new light! I am also reading some beautiful poetry by a friend, Stuart Boag. I recently started Tim Winton’s latest book, Eyrie, but haven’t read enough yet to say what I think about it. And shortly, when I start my Christmas holidays, I am planning to read the Game of Thrones book set, which my wife read ages ago and, having watched the series together on cable TV, I think I’ll have a go at – though the books are BIG!
7. **Any new year’s resolutions you would like to share with us?**

I practice Yoga and in the year just ending I set myself the goal of being able to do a couple of the trickier Yoga poses, one of which is the headstand. But I haven’t really mastered it yet, so I am going to carry that goal forward into 2014, as well as starting on a new pose called side-crow. If you don’t know what that is look it up. It may take me a few years! But then as the Yogi’s say, you are always learning. A bit like privacy, I think.

---

**Update from the Privacy Commissioner, OAIC**

_by Timothy Pilgrim_

2013 is almost over and I’ve been reflecting on what a significant year it has been for privacy practitioners. Our recently released Annual Report shows that of the 18,205 telephone enquiries received by the Office of the Australian Information Commissioner, 9,009 were about privacy. This year, we received 3142 written enquiries (11% more) and handled 1496 (10% more) privacy complaints than last year. Complaint statistics from the first quarter of 2013–14 show that interest in privacy is increasing and people are not afraid to exercise their privacy rights. If the trend continues, we are on track to receive in excess of 2300 complaints by June next year, compared to the 1496 complaints we received in 2012–13. Many of you will have spent much of the year preparing for the implementation of the new privacy laws. In just under 4 months’ time we will be working with the new Australian Privacy Principles, an exciting time with some of the biggest changes to the Privacy Act we have seen since the private sector provisions commenced in 2001.

We have now released the final two draft guidelines on APPs 12 (Access to personal information) and 13 (Correction of personal information) for consultation. These draft Guidelines need to be applicable to both organisations and government agencies, and so they highlight to government agencies the interaction between their privacy and freedom of information obligations. They also set out organisations’ obligations, so it’s important that we also hear your views on how these principles apply to the private sector.

APP 12 says that an entity that holds personal information about an individual must, on request, give that individual access to the information. The grounds on which access may be refused differ for agencies and organisations. The draft APP Guidelines clarify what is meant by ‘hold’ saying that the term extends beyond physical possession of a record to include a record that an entity has the right or power to deal with. An example of this is a record of personal information stored on servers managed by a third party, where the APP entity has the right to deal with that information, such as by accessing and amending the information. This issue of the meaning of “hold” has come up in past own motion investigations (OMI) that I have conducted under the National Privacy Principles.

The draft APP Guidelines build on my most recent OMI public report: AAPT and Melbourne IT.

APP 13 sets out the conditions under which an APP entity must take reasonable steps to correct personal information it holds to ensure that it is accurate, up-to-date, complete, relevant and not misleading. These concepts are not defined in the Privacy Act so the draft APP Guidelines give guidance on their meaning. They also clarify when an entity may correct personal information on its own initiative and they stipulate procedural requirements that must be met by an entity when dealing with a requirement to correct personal information.

The OAIC has been working hard to get the draft APP Guidelines out to you as quickly as possible and to ensure they are useful, practical and relevant.

It was great to see the iappANZ Summit so well supported. Those of you that were there would have heard me speak about the OAIC’s enforcement approach to the new laws and my expectations of organisations come March 2014. To make sure your organisation is ready for March 2014 you should be: reviewing your information security and data breach response plan; working on your APP privacy policy and conducting a privacy impact assessment for any new processes you may be considering implementing.

This week I’m chairing the 40th Asia Pacific Privacy Authorities Forum in Sydney. We will be joined by Privacy Commissioners and other privacy regulators from around the Asia Pacific region including Hong Kong, New Zealand, Mexico, Korea, Macao, Japan and Singapore. I am certain there will be some lively discussions about the privacy issues facing us all in a globally interconnected world.

Timothy Pilgrim, Australian Federal Privacy Commissioner
35th Data Protection and Privacy Commissioners’ Conference, Warsaw, Poland
by Annelies Moens and Malcolm Crompton

At the 2013 International Conference of Data Protection and Privacy Commissioners, www.privacyconference2013.org, iappANZ was well represented with two past presidents attending: Annelies Moens and Malcolm Crompton.

The Conference was held in Warsaw in September. On 23-24 September, Commissioners met in private and on 25-26 September they held a public conference.

Commissioners were particularly active in private Conference, adopting a suite of resolutions and a Declaration. Perhaps the two most interesting to iappANZ members are a Resolution on Profiling and the “Warsaw Declaration on the Appification of Society”. The declaration focused on “surprise minimisation”. It urges app developers to ensure apps don’t have hidden features nor unverifiable background data collection. The Commissioners will be ready to enforce their respective privacy laws in a global effort to claim user control if necessary.

The Resolution on Profiling urges parties making use of profiling to:
- clearly determine the need and application before profiling
- limit use of data collected
- focus on the need for continuous validation of algorithms/profiles
- ensure individuals maintain control over their information
- inform individuals of their right to access and correction; and
- have oversight over profiling operations


In the open session, the highlight of the conference was given in the first plenary session by Professor Hiroshi Miyashita. He is a leading privacy academic in Japan and helped to start up the Office of Personal Information Protection in the Consumer Affairs Agency in Japan when its privacy law first came into effect. He brilliantly compared the different privacy expectations of different cultures around the world: US, French, Japanese and others. It was a salutary reminder to all attending that their particular perspective may not be the only approach.

Much of the conference was devoted to discussing the nuance and impact of the draft EU Regulation on data protection that has been proposed to replace the current Directive issued in 1995. The 1995 Directive has been transposed so differently into the national laws of the EU member states that the intended ‘harmony’ of an EU open market has been severely compromised. There are also arguments about the need to update its provisions. For those who follow this particular debate, we learnt little new other than to hear varying views on whether the Regulation would become law before the EU parliamentary elections in 2014 (generally accepted as less and less likely, but don’t under-estimate Viviane Reding the sponsoring Commissioner).

Another strong theme was the repercussions of the NSA and PRISM revelations. This led to discussions led by the Europeans concerning the need for the equivalent of safe-harbour for public sector organisations (as safe harbour at present only covers signed up private sector organisations) for transfers of personal information between the EU and USA. Others spoke about the need to inform individuals if law enforcement accessed their personal information.
The conference was videoed and hopefully will be posted online. Other topics covered at the conference included, big data and data analytics for development purposes, data protection and global trade law, privacy and cyber security and data use within context and compatible purpose. We expect that presentations will also be uploaded to the conference website.

Malcolm Crompton is Managing Director, Information Integrity Solutions Pty Ltd Founding President and now Director, iappANZ, mcrompton@iispartners.com

Annelies Moens is Head of Sales and Operations, Information Integrity Solutions Pty Ltd Immediate Past President, iappANZ annelies@iappanz.org

Silver Surfers’ privacy concerns don’t outweigh risky behaviour online

By Joel Camissar, Asia Pacific

This is the view of Joel Cammisar, McAfee who reports that new research from McAfee has revealed that Australians between 50 and 75 years of age, or ‘Silver Surfers’, are spending a significant amount of time on the internet (3-4 hours), and we’ve also found that they’re too trusting and share too much information online.

Despite 99 per cent of survey respondents saying they are careful about what information they post online, 76 per cent posted personal information including an email address, 51 per cent posted a mobile number and 47 per cent posted a home address, for reasons other than online shopping.

But perhaps most worrying is that 44 per cent of this demographic don’t consider sharing this personal information to be a risk to their privacy or security. Privacy is a hot issue right now in Australia, so we found this very surprising; to know that they are aware of their privacy yet they are risking it online. Clearly there is further to go in educating this group about the dangers that lurk online and to be wary of people they don’t personally know.

Seniors Getting Scammed

The Silver Surfers survey [insert link to pdf] also found more vulnerabilities with this age group, including on average, one in four have spoken to strangers online, one in five have been the victim of online fraud and seven in ten have been targeted by strangers seeking their personal information.

Detective Superintendent Brian Hay from the Queensland Police Service was at our research launch to highlight the trouble unsuspecting seniors can get into while online. Hay says he is seeing a huge representation of older Australians in those falling victim to romance-related scams. Over 90 per cent of the millions of dollars of fraud money going to West African countries such as Nigeria and Ghana every month is from love scams. He is also seeing older Australians getting caught up in lottery scams and much of this money goes to the US and Canada. Of particular concern is identity theft.

According to Hay, the key to prevention is awareness. Ongoing education must be delivered to the older community to encourage them to protect themselves and to be aware of the risks, because once scammers get their hooks in, the threats get deeper and deeper. It is also vital to educate family members, friends and support networks to look for the signs of trouble, as the earlier the intervention, the more successful the outcome, according to Hay.
Connected and Social

While the internet is proving risky for this age-group, our Silver Surfers survey also revealed that the internet can be a rewarding experience, with seven in 10 citing its importance in keeping connected with family and friends. A further one in two have used the internet to connect with lost family and friends or traced family trees.

The research also explored the Silver Surfers use of social media and device usage and found that just over half (53 per cent) have a social media account, with 48 per cent using Facebook and 39 per cent using Google+. Photo sharing was the least common social tool amongst this age group.

Of those with social media accounts, 72 per cent said that social media puts them at greater risk of scams and identity theft and a third said they do not know all the people in their network. President of the Australian Seniors Computer Clubs Association (ASCCA), Nan Bosler, who was also involved with the launch of the Silver Surfers research, echoes the important role the internet plays in connection. She says that older Australians are isolated from loved ones, or they have lost family members, so the internet is a wonderful place to help fill this loneliness. However, she went on to say that as the research highlights, there are risks, so ASCCA drives the same message as us here at McAfee in ensuring education is in place for our members so they can enjoy the benefits of technology safely.

Our new partnership with ASCCA will see us roll-out a module designed to equip older Australians with the tools they need to learn how to navigate the internet safely. McAfee has a number of cyber education initiatives in place including a free e-guide which offers practical advice about safety online, our volunteer program and our cyber education website, which is just the start of driving the cyber safety message and greater awareness of the risks among our senior citizens.

*Joel Camissar is the Data Loss Prevention and Privacy Lead with McAfee Asia Pacific*
The Role and Function of a Data Protection Officer in Practice and in the European Commissioners Proposed General Data Protection Regulation Workshop on the DPO Role Project, Brussels

By Malcolm Crompton

Privacy (or Data Protection) Officers (DPOs) have been around in some organisations for some time. Indeed companies have been required to have them under German data protection law for many years. If passed in its current format, the draft EU Data Protection Regulation would spread this requirement across Europe.

This proposal has spread some consternation across companies in Europe and also to non-European companies with presence in Europe.

In response, the Centre for Information Policy Leadership (CIPL) conducted a survey as part of its project on “Addressing the Challenges of a Changing Role: An exploration of the dynamics impacting on the role of the Chief Privacy or Data Protection Officer” (see www.informationpolicycentre.com/DPO_Project/ for more background). The Centre is funded by businesses that wish to provide leadership on privacy and data protection and are predominantly US headquartered.

The survey had two themes. The first focussed on current practices in those surveyed as well as seeking desired practice. The second theme was to seek views of respondents on aspects of the draft EU Regulations. The survey was conducted in mid-2013. The results of the survey were released at the Workshop in Brussels and discussed by expert panels of DPOs and of Data Protection Authorities (DPAs). At a late stage in the project, iappANZ sought to ensure some ANZ input to the survey. We didn’t have time to publicise it widely so we contacted some members directly and got a wonderful response: many thanks to those who contributed!

The report of the survey is based on the responses of 43 practicing DPOs/CPOs/global privacy leads worldwide, mostly from the US and UK as well as 5 from Australia and one from Canada. About 70% of respondents had 10,000 staff or more worldwide. The survey report will be online at www.informationpolicycentre.com but wasn’t available at the time of writing.

The most relevant part of the survey for privacy officers in our region comprises the results on current and desired practices. Headline results include:

- The major reasons for appointing a DPO were based on a desired good practice imperative and a pro-active management of data privacy. Results suggested that compliance by itself has not been a strong driver.
- The role of the DPO is evolving. The great majority oversee the organisation’s privacy program and advise on compliance with privacy law as well as provide advice following a data breach. A smaller proportion, just over half, perform very operational tasks such as deal with complaints or conduct compliance assessments. The drift towards the higher level activities appears to have been underway for some time.
- The DPO role requires a diverse skill set, which should not surprise any of us. Skills required include technical and commercial awareness and a deep understanding of the business and strong communication and public relations skills. All this often requires a team approach rather than just one person. That said, just over half reported a privacy team with 5 or less supporting members.
- The DPO is almost exclusively located in Legal or Compliance. Fewer are located in Risk, HR, Marketing or IT Security.

During the panel discussion on the report, the most fascinating discussion centred on the independence of the DPO – structurally and how they conducted themselves. The DPOs on the panels and also the participating DPAs (from Ireland, France, Poland, UK) all agree the DPO was not the mouthpiece of the DPA in the company. Nor did they see the DPO simply as an internal privacy advocate or simply
there to help the company find a way to avoid or get around the law. They all saw the DPO as needing to understand the business imperative, ensure good practice was enunciated and instilled into the organisation and in the end to have the right level of independence.

All up, the survey is a useful snapshot on current practices with useful insights for us all. And for those with an interest in the potential impact of the EU Data Protection Regulation, this is an interesting view on one of the practical impacts it could have.

By Malcolm Crompton, CIPP/US, is managing director of Information Integrity Solutions Pty Ltd, a global consultancy that works with public and private sector organisations wishing to embed trust and privacy as core value propositions in their products and services. Malcolm was Privacy Commissioner of Australia from 1999-2004 and helped to found iappANZ in 2008. He received the 2012 Privacy Leadership Award from IAPP in recognition of his global reputation and expertise in privacy.

---

**Recent Exiting Things**

*by David Templeton*

October saw some compelling reading issue from the OAIC. In this month’s editorial I’d like to cover some of this material (at the risk of repetition). I’ll also reflect on the forward agenda for privacy, speculating on the future of data breach reporting offering further thoughts on how to survive the Australian Privacy Principles.

**AAPT**

The OAIC recently published its Own Motion Investigation (OMI) findings concerning the July 2012 hack perpetrated by Anonymous of AAPT data. The OMI found that AAPT breached NPP4.1, the obligation to take reasonable steps to protect personal information “from misuse and loss and from unauthorised access, modification or disclosure”, but did not breach of NPP2.1 (the obligation not to disclose personal information improperly) as AAPT was the victim of a hack or cyber-attack.

In this case, in failing to update its Cold Fusion hosting platform, and leaving in place a version that was known to be vulnerable, AAPT failed to take such steps.

AAPT’s data was held on third party servers subject to a contract that allocated responsibility or patching applications, but not updating applications, to the third party. The third party had complied with its obligations to implement security patches. The problem was the application itself. As the contract was clear, the third party was held not to be in breach.

While this OMI demonstrates the benefits of clear contractual provisions dealing with security related responsibilities, it contains no surprises when compared to OMIs of similar instances in recent years involving Sony, Telstra, Dell Australia, First State Super and MedVet in terms of applying the NPPs.

In short, preventable hacks will be found to involve breaches of NPP4.1, but probably not NPP2.1, while preventable leakages of information into accessible domains will generally breach NPP2.1.

Hacks that could not reasonably have been prevented will breach neither, but the standard of reasonableness is high, at least that of a competent information security professional.

From March next year, when the Australian Privacy Principles take effect, serious or repeat data security failures are clear candidates for civil penalties.

In a further twist, it emerged in the course of investigation that not all of the data that was lost was actually in use. The OAIC also found AAPT to be in breach of its NPP 4.2 obligation to destroy or permanently de-identify obsolete data.

**Attitudes to Privacy**

**Community Attitudes to Privacy Survey**

The OAIC released the fourth Community Attitudes to Privacy Survey on 9 October and Joel Camissar, McAfee’s Data Loss Prevention and Privacy Lead for the Asia Pacific, gave an excellent summary in our last edition. This is a rich document offering riveting insights into attitudes across segments of the community distinguished by age, income, geography, gender and other key factors. Together with previous surveys, it reveals important trends in community priorities and expectations from 2001 to the present.
The survey involved 1,000 respondents, 90% of which use the internet. In other words, the findings are highly relevant. I’ve picked on some that I think will be highlights for you – but I strongly recommend the OAIC report for your reading list and note that the full survey results are available for your own analysis via the OAIC’s site.

The survey indicates that privacy concern is increasing (consistently with complaints being up 10%, according to the OAIC’s Annual Report also released in October). Commensurately, privacy policies are becoming more, not less important to individuals and as a result, more important to organisations who want to differentiate themselves from competitors or simply build deeper and more trusting customer relationships.

To illustrate, 44% of respondents reported that they read online privacy policies at least “often” in order to use them to make decisions about whether to deal with a website. Conversely, only 13% reported never doing so, despite the tendency for them to be long, dry and complex. This is underscored by the increasing rate at which Australians exercise choice to not do business online on the basis of a privacy concern. Around 60% of respondents report making such a decision (clearly some without having read the privacy policy), up from 36% in 2007, 33% in 2004 and 42% in 2001.

The OAIC also recently published “Mobile privacy: A better practice guide for mobile app developers”, a good practice guide for mobile app developers during October. The quality of privacy disclosure, as one means to build competitive advantage, features prominently in the Guide. Statistics cited by the OAIC from the US and UK indicate that consumers in those countries will vote with their fingertips against apps that seem to be privacy unfriendly at a similar rate.

This reveals a significant opportunity for business to fix something that probably sends around half of their potential customer pool to competitors. It should be borne in mind that not all website/mobile privacy policies fit the annoying bucket. According to the Global Privacy Enforcement Network (GPEN) Internet Privacy Sweep findings (another also published on the OAIC’s website), many organisations offer accessible, simple and relevant privacy policies, presented in reader-friendly formats. GPEN was a truly global survey of websites conducted by information privacy regulators across 12 countries including the United States, the UK, Canada, Hong Kong, France and Germany as well as Australia and New Zealand.

The Community Attitudes survey also reveals increasing concern about the link between disclosure of personal information and risk of crime/financial loss, and belief that individuals should be informed of data breaches, a matter that may well impact the new Government’s policy on data breach notification. Media has reported early signals from the new Government that the Privacy Amendment (Privacy Alerts) Bill 2013 might be seen as over-regulation and further delayed. The survey results, and the behavior of many of the organisations involved in the data breaches mentioned above, suggest that data breach reporting will remain on the policy agenda.

Across those five instances, only one clearly involved a malicious hacker likely to have customer identity takeover as an end goal. The others involved inadvertence or hacktivism. For example, in the case of First State Super, the hacker was himself a customer of First State who contacted FSS advising them of the hack and who “[promoted] himself as a ‘white hat’ hacker intending to improve their computer security”. He even made a statutory declaration that he had destroyed the information.

In these instances it could be argued (in varying degrees) that harm was unlikely to eventuate. Nevertheless, the organizations concerned promptly notified customers. Real risk of serious harm is the main criteria for a breach notification proposed in the Privacy Amendment (Privacy Alerts) Bill 2013 and the question of its definition is a significant point of objection to the Bill. Definitional concern about whether these instances resulted in such a risk does not seem to have been difficult for any of these organisations.

The Survey shows that overall concern about data going offshore has not materially changed since 2007 and remains significant, 62% of respondents expressing strong concern. Even more tellingly, 79% of respondents, when asked if they thought that their data being sent to an “overseas processing centre” was a misuse of privacy, agreed with that proposition. This presents an interesting inconsistency in consumer behavior when the increase in offshore internet shopping is considered. It seems safe to speculate that a significant proportion of these respondents are not so concerned that they are not prepared to send their name, address and credit card details overseas in the interests of price and convenience.

It would be useful for organisations, when this survey is next conducted, to gather a deeper level of insight into what specific matters respondents are “concerned” about. Specific anxieties can be dealt with by specific measures but amorphous anxiety is difficult to address. Business process offshoring is widely...
practiced by Australian business and there is almost certainly an appetite to allay consumer concern.

Concern about biometrics is another area in which it would be useful for future surveys to analyse more specifically what concerns individuals harbor. Biometric identification is likely to become more important, and more frequent, as reliance on a customer’s life history as evidence of identity is increasingly exploited by criminals.

Are you APP ready?

Differences between the current privacy principles and the Australian Privacy Principles (APPs) will affect different organisations in different ways, but all organisations should be reviewing the APPs carefully to identify gaps between their current practices and those required after 14 March, but you are reading the iappANZ editorial and you already know that.

An area that will require care and attention – and may occasion organizational headaches as you work to influence your procurement and contract management areas, is the impact that the APPs will have on what organisations’ arrangements with business partners will need to achieve, particularly in the areas of direct marketing and cross border data movements. Varying existing contracts requires agreement and sometimes comes at a price, but notwithstanding that, variations that deserve consideration include:

- rights to trace the provenance of personal information used for direct marketing, if an individual makes a request under APP 7.6(e).
- rights to be kept informed about transborder data movements, and obligations on the part of suppliers to ensure that they have similar rights against their contractors, and so on. This will support the new disclosure obligations, in particular, and will go to the reasonableness of beliefs as to local privacy regulation and the adequacy of local protection.
- indemnities in relation to the APPs that clearly operate where an Australian based organization is deemed to be responsible for the acts or omissions of an offshore counterparty, and (to the extent possible) that operate in relation to civil penalties.

The data protection and privacy aspects of contracts are much more likely to be relied upon after March 2014 and warrant a careful review, both of whether the terms and conditions are adequate and of the extent to which more active ongoing contract management is warranted, particularly in relation to audit and assurance rights.

Organisations may also wish to consider whether supplier contracts should anticipate data breach reporting laws and deal with responsibility for identifying, escalating and notifying incidents.

The earlier you start on this, the more likely it is that a contract renewal, or some other event in the contract lifecycle, might present an opportunity to introduce provisions dealing with these matters at a more affordable price.

David Templeton is an iappANZ Board Director and Senior Manager, Retail Division, ANZ

Win a Cash Prize: iappANZ’s writing prize 2014

iappANZ is very excited to announce the launch of its [$250 cash] writing prize for a second year running for an article that is published in our monthly Bulletin between December 2013 and October 2014. Anyone can enter (you don't have to be an iappANZ member), simply by writing and submitting an article between 500-1500 words that tells us something interesting, new and relevant about privacy. Opinions are most welcome but nothing too extreme.

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

The winner will be announced at our Privacy Summit on 25 November 2013 and their name and details will be published on our website. [We also hope to publish profile of the winner in our Bulletin]. So alert your network and get writing!

More details about the writing prize if you are interested:
Our Editorial team, Veronica Scott, Carolyn Lidgerwood plus President Emma Hossack and Past President Malcolm Crompton, will decide on the winner whose article they judge to be the most interesting, original and relevant to our members.

Articles submitted and published in the February, March and April Bulletins will also be eligible for the prize – we don’t want anyone who has already made a valuable contribution to miss out.

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

After the winner is announced we will notify them and arrange for the prize to be delivered to them if they are unlucky 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.
Recruitment

Watch this space for new positions with the OAIC
The OAIC brings together in one agency the functions of information policy advice and independent oversight of privacy protection and freedom of information. Its vision is a community in which government information is managed as a national resource and personal information is respected and protected. If you would like to work with the OAIC or to find out what positions are currently available, how to apply for jobs and conditions of employment at the OAIC keep an eye on our recruitment section here. The OAIC welcomes applications from the diverse Australian community including Aboriginal and Torres Strait Islander people and people with disability, people of all ages and those from culturally and linguistically diverse backgrounds.

For more information go to the OAIC website.

Up coming Privacy Events

<table>
<thead>
<tr>
<th>Date &amp; Details</th>
<th>Information</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Wednesday 12 February 2014</strong></td>
<td><strong>The Big Wrap up on the Privacy Act</strong></td>
<td>Free for iappANZ members $99 for non-members Costs deductible from joining fee</td>
</tr>
<tr>
<td>OAIC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Room1 Level 3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>175 Pitt Street (nr crnr King St)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sydney</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Late February 2014 in Melbourne</strong></td>
<td><strong>Data in flight</strong></td>
<td>TBC</td>
</tr>
<tr>
<td>Day, time and venue TBC</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Late February 2014 in Brisbane</strong></td>
<td><strong>Credit reporting workshop</strong></td>
<td>TBC</td>
</tr>
<tr>
<td>Day, time and venue TBC</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Early March 2014 in Melbourne</strong></td>
<td><strong>Health check</strong></td>
<td>TBC</td>
</tr>
<tr>
<td>Day, time and venue TBC</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
IAPP Certification

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

The International Association of Privacy Professionals (IAPP) says:

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

What certifications are available? Are they relevant to my work here?
The IAPP offers four credentials, one of which is particularly relevant to iappANZ members, namely the Certified Information Privacy Professional/ Information Technology (CIPP/IT).

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

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

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

FIND OUT MORE at:

Join us on LinkedIn or follow us on Twitter

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

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

Follow us on Twitter at: https://twitter.com/iappANZ