2014 is going to be the year our brand and profession take the spotlight. The new APP’s coupled with daily media on privacy make this inevitable. Our aim is to be recognised by all the organisations responsible for the management of personal information, and to create greater awareness of what the iappANZ is and to make the membership more valuable.

The new Board continues to build on achievements of its predecessors over the last 5 years. By mid-year iappANZ will have a new website and completed its first set of ten stand-alone training workshops. Find full details of our credit reporting event in Brisbane, security event in Melbourne and health event in Sydney towards the end of the Bulletin. More in depth sessions will follow. We have also reintroduced our popular member networking sessions – Director Kate Reynolds kicks these off in Sydney on 12th March. For those of you who don’t like social media, our iappANZ linked in group does have its place – even if just to let you know about when the next social event is in your city. We invite you all to ‘link in’ and make these sessions stronger. If you want to lead an event, get in touch with us and we would be delighted to help you organise it.

Privacy Unbound, our newly branded Bulletin aims to provide you with practical advice and insights from all sides - our regulators, security experts, lawyers, privacy practitioners and academia. This month we have the popular Q+A section with Australia’s Privacy Commissioner Timothy Pilgrim facilitated by our
Treasurer Melanie Marks. Rob Sherman, the privacy and policy manager for Facebook in Washington D.C explains his company’s commitment to privacy, and our Vice President Anna Kuperman provides a timely series of take home lessons on the APP Guidelines.

New Zealand punches above its weight in more than rugby - in Australia we have much to learn from New Zealand in the area of privacy. And this is the year we want to do it. This month we have a viewpoint from the Assistant Privacy Commissioner NZ, Katrine Evans. We also have viewpoints from academia – Professor Gehan Gunasekara from University of Auckland, and business - Souella Cummings, partner KPMG Auckland. Souella was a part of the now famous team who provided the report on the ACC which has now become a gold standard in privacy.

Our other focus for 2014 will be security. We all know that great security is possible without privacy, but privacy on the other hand depends on security. We

kick off the focus with a piece on 10 of the most significant cyber threats from Michael Sentonas, Vice President and Global Chief of Technology for Security Connected at McAfee.

We are delighted this month to introduce you to one of our new partner associations, Australian Corporate Lawyers Association (ACLA). Through these collaborations we aim to extend our knowledge network and benefits.

iappANZ membership provides you with up to date information on all your areas of privacy practice as well as a place in an internationally recognised privacy community. We hope that you find this first issue for 2014 a good read.

Warm regards

Emma Hossack, President

---

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

---

Introducing your new iappANZ Board for 2014

Each month we will be introducing some of our Board directors for 2014. We are very pleased to kick off with our Vice-President Anna Kuperman and our President Emma Hossack, who are working together as a dynamite team for the second year…
President Emma Hossack

(Ed's note: you can see the lovely Emma's picture above so we wont show you again!)

Emma Hossack is iappANZ’s very energetic President! When she’s not wearing her iappANZ hat, Emma is the CEO of Extensia, a leading Australian supplier of software solutions and technologies for the health care sector. She is also CEO of Edocx, used for information sharing and storage. This makes Emma the iappANZ board’s resident expert on health privacy and shared electronic health record systems (and that’s just for starters …).

Before joining Extensia, Emma practised as a commercial lawyer and completed a Masters of Law with a focus on medico/legal and privacy/ethical issues in 2007. Now based in Brisbane, Emma’s other interests and positions include:

- Vice President- Medical Software Industry Association
- Secretary CIRCA
- Member of CEO Institute, HISA and Brisbane Institute.

Emma lives in Brisbane with her family which includes a set of triplet teenage daughters and their many pets. Emma relaxes by training for marathons and enjoying the thriving Arts scene in Brisbane.

Emma is about to head off to the IAPP Global Privacy Summit in Washington DC – and we can’t wait to hear her report.

Emma holds a Bachelor of Laws & Bachelor of Arts (Hons) from the University of Melbourne, LLM

Vice President Anna Kuperman

We could call our Vice-President Anna Kuperman ‘Robin’ (alongside President Emma Hossack’s ‘Batman’), but ‘Wonder Woman’ works too! Having spent over 12 years in private practice at a top tier law firm, Anna has been Legal Counsel at Serco Asia Pacific since January 2013 and advises across all its Asia Pacific operations including IT & BPO outsourcing, justice, defence, science, health, transport and consulting. Anna has a depth of experience in intellectual property and commercial law and specialist expertise in privacy law. She has counselled large organisations on privacy compliance, mitigating risks of data security breaches and managing offshore data disclosure.

Anna has served on the Board since 2012, as Vice President in 2013 and continues in that role in 2014. Anna lives in Sydney and is married with 2 children, Danny aged 7 and Alana aged 4. In rare moments of calm, Anna enjoys watching National Geographic channel (finding animals wrangling in the wild strangely soothing) and listening to uplifting music that is not The Wiggles … sometimes simultaneously!

Anna has a Bachelor of Laws (Hons) & Bachelor of Arts (Hons), Macquarie University; Master of Laws from the University of Technology
Australia legislates for 'privacy by design'
by Veronica Scott and Tarryn Ryan

In March this year, Australia will be overhauling its privacy laws. One of the key features of the new regime means Australia will become one of the first jurisdictions to effectively legislate for the concept of 'privacy by design'.

Australia's system of privacy regulation is a principles based regime. The new Australian Privacy Principles (APPs) are structured to reflect the information lifecycle – from privacy planning to collection of personal information, use and disclosure, quality and security, and access and correction.

For the first time there will be a stand alone provision that requires organisations to manage personal information in an open and transparent way. Organisations will also be required to take reasonable steps to implement practices, procedures and systems relating to their functions or activities that will ensure that they comply with the APPs and are able to deal with any privacy inquiries or complaints. A failure to meet either of these obligations will mean that the organisation has breached the Privacy Act and could be liable for penalties.

The APP Guidelines issued by Australia's privacy regulator which will underpin the APPs explain that organisations will be better placed to meet their privacy obligations if they embed privacy protections in the design of their information handling practices. While there is no doubt about the truth of this statement, legislating for it is a big leap from the current position where in reality many organisations' approach to privacy is still largely reactive.

Australian privacy professionals are waiting to see how the 'privacy by design' requirements will be enforced. The privacy regulator will have a significantly broader set of powers as part of the overhaul. Come March, he will be able to walk into any organisation that is subject to the APPs and audit their compliance. A failure to have documented policies and procedures in place could theoretically mean a breach of these new provisions and an exercise of the regulator's new enforcement powers. He will be able to require enforceable undertakings and to pursue civil penalties of up to AUD$1.7 million (approximately US$1.5 million) for serious or repeated privacy breaches.

Of course these changes only strengthen the business case for privacy in Australia. A recent survey conducted by the Australian privacy regulator found that 60% of Australians had chosen not to deal with a company because of concerns about how it would use their personal information. Transparency is also a primary concern with 95% of people believing that organisations should tell them how their information is stored and protected, and 96% believing that they should be informed if a company has a data breach which affects their personal information.

Clearly even the law makers in Australia now realise that privacy is not simply a matter of regulatory compliance that can be bolted on to an organisation's usual functions or activities. By introducing the new 'privacy by design' provisions, they are pushing Australian organisations to adopt a holistic and proactive approach to privacy planning. If they don't, the regulator will have a much bigger stick to strike them with.

Veronica Scott (Special Counsel) and Tarryn Ryan (lawyer) are in the Media and Communications Group at Minter Ellison specialising in media and privacy. Veronica is also a Board Director of iappANZ.
iappANZ Profile of Garth Luke
CEO, ANZ/SVP Corporate Development

Questions by Veronica Scott, iappANZ

1. How did you come to your current role with AvePoint?

I began my IT walk working for Microsoft in 1996 before moving on to a consulting role with Siemens Business Services. From there, I've had many diverse experiences in the IT world from back office consulting and implementation, to development, to SQL programming and infrastructure implementations. This journey landed me at AvePoint in 2008, where I've had a great experience leading sales and marketing activities in Australia, New Zealand, and the United States. In my current role, I oversee our business strategies, Microsoft alliances, and channel partners across Australasia and Africa – which of course includes leading our Australasian team in helping our customers balance compliance and privacy with latest IT technologies in enterprise collaboration, social networking and mobility. I also head up our global business development efforts which include OEM and integration relationships with companies such as NetApp, IBM, HDS, and HP.

2. How is AvePoint helping clients prepare for the changes to the Privacy Act 1988 (Cth)?

The biggest step is fact finding. We first assess the current state of privacy compliance with our clients. This involves identifying sensitive data for further action, understanding who accessed it, and how it got there in the first place. We then have our clients assess their existing sensitive data and evaluate in-place privacy protection programs – it’s only then that we’re able to better understand the current risk levels of their enterprise content and the management systems in place. By overlaying this information with an understanding of how frequently sensitive data is being accessed and by whom, we can further prioritise the steps necessary to then use our compliance solutions to secure their sensitive data and abide by the changes to the Privacy Act.

3. How does security interact with privacy?

A recent Forrester study on data privacy and security found that last year the security group is fully responsible for privacy and regulations in 30% of firms, contrary to 2012 when responsibility was shifting toward a Privacy Officer. With all of the recent data breaches that have been so prevalent in the news, organisations realise that they don't want to end up on the front page of The Australian for losing people's sensitive data. So security comes into play, to put some teeth behind the need to keep private data, well, private by finding the right strategies and technologies to do so. The intersection comes in the execution and responsibility.

4. Looking into your crystal ball, what do you see as the short and long term issues facing privacy professionals?

The shortest term issue is figuring out how they, being the privacy professionals in charge, ensure that their respective organisations are living up to the Privacy Principles and changes to the Privacy Act. That’s the biggest priority. The change is coming in mid-March. The longer term issues include changing a history of lack of education and understanding on behalf of end users. Studies find that half of all data breaches are accidental in nature. Most have not received security
awareness and training, or understand data use policies. To complicate matters, employees use so many technological devices now to access company information that many don’t even know where to begin. Changing that culture is going to be a longer term issue. Last, ensuring that you have a proactive – not just reactive approach – to privacy compliance. How do you implement an effective risk management lifecycle to ensure all the data being created and flowing in and out of organisations are abiding by the proper privacy regulations? Those are the issues privacy professionals face today and long into the future.

5. How can privacy professionals best convey the business case for privacy?

I think that you can point to any number of incidences of privacy breaches that have happened in the last year. Privacy was the word of the year in 2013, and you don’t even need to reference Edward Snowden, Target, or Adobe. Recently the Immigration Department in Australia accidentally published the personal information of 10,000 asylum seekers. Terrible press, instant investigations from the Privacy Commission, loss of credibility and trust from your constituents or customers – you don’t want to be on the front page of The Guardian for this reason.

6. Do you think privacy is a real game changer for organisations?

Absolutely. Trust reigns supreme with your customers and employees – and as an organisation, it is your duty to ensure that you uphold that trust. Whether it’s delivering high quality products or services, or keeping information that is sensitive in nature from seeing the light of day, ensuring that you uphold that trust is paramount. Private information in the wrong hands exposes organisations to significant financial risk through regulator fines or through severely damaging a company’s reputation and brand equity. Especially now with these very highly discussed changes to the Privacy Act, this is going to fundamentally change the way organisations think about and execute any communication or information gathering with the public at large. It is going to change the way we all do business – and that, to me, is the very definition of a game changer.

Garth has been in the IT business for 17 years. Since joining AvePoint in 2008, he has advised some of Microsoft’s biggest customers worldwide on strategic implementation of social enterprise and collaborative platforms such as Microsoft SharePoint, Yammer and Jive. Garth has helped many Australian and international CIOs – including Fortune 500 and public sector organisations – realize their visions of a truly social and collaborative enterprise with forward-thinking investments in people, processes and technologies. Working often in partnership with Microsoft and many of AvePoint’s top partners around the world, Garth has proven expertise in helping CIOs align social enterprise and collaborative platforms, such as Microsoft SharePoint with business, while balancing collaboration with compliance and Governance. In his current role, Garth oversees AvePoint’s business strategies, Microsoft alliances and channel partners across Australasia, Africa and US South West. Garth also heads up AvePoint’s global business development efforts which include OEM and integration relationships with companies such as NetApp, IBM, HDS, and HP.
Hong Kong Update: International Conference on Privacy Protection in Corporate Governance and the Privacy Management Program

by Malcolm Compton

On 11 February, the Privacy Commissioner for Personal Data of Hong Kong, Allan Chiang, hosted the International Conference on Privacy Protection in Corporate Governance.

Like the International Conference on Privacy by Design convened by the Commissioner in 2012, this was a conference of the first order.

Many of the conference presentations are available on the Conference Programme page, http://www.pcpd.org.hk/privacyconference2014/programme.html. They are well worth a visit.

Speakers included Trevor Hughes, President and CEO of IAPP, Bojana Bellamy, President of the Centre for Information Policy Leadership, Scott Taylor from HP, JoAnn Stonier from MasterCard and Mikko Niva from Nokia, who we remember at Privacy Unbound in Sydney last November.

There were excellent speakers from Hong Kong, including Sunny Cheung the CEO of Octopus Holdings who has rebuilt the company into a privacy best practice company after the misuse of personal information that cost the previous CEO her job. Others included Elaine Chong Senior Group Legal Adviser, HKT Group a major energy company in Hong Kong.

I was there as moderator, including for the two panel sessions.

The dominant theme of the conference was that compliance is no longer enough. The public expects more. We heard global leaders in privacy practice give us their views on how they had strived to achieve this objective. In almost all cases, they had built strong privacy practices brick by brick as the opportunities in their organisation came to hand. They also reinforced the importance of top management buy in complemented by strong governance structures.

The Conference also set the backdrop for the launch a week later by the Commissioner of his Privacy Management Programme: A Best Practice Guide. The launch was complete with pledges from many of the largest companies in HK that they will apply the plan to their own operations.

At a ceremony convened by the Commissioner, the Hong Kong Special Administrative Region Government, together with twenty five companies from the insurance sector, nine companies from the telecommunications sector and five organisations from other sectors, all pledged to implement the Privacy Management Programme. Details of the launch and copies of the Guide are all online at http://www.pcpd.org.hk/english/infocentre/press_20140218.htm.

Malcolm Crompton, CIPP, is Managing Director, Information Integrity Solutions Pty Ltd and Founding President and now Director, iappANZ, mcrompton@iispartners.com. He was Privacy Commissioner of Australia 1999-2004.
Will the Tide Turn in 2014? New Zealand Update

by Professor Gehan Gunasekara

Last year was not a good one for New Zealand privacy-wise. While Australia forged ahead enacting legislation covering issues such as cross-border controls for personal data and proposing measures to implement breach notification, the Government in New Zealand, by contrast, has been dragging its feet and instead adopted a raft of measures diminishing existing privacy protections. This article briefly reviews developments in New Zealand in 2013 and ventures some predictions as to what may lie in store in 2014.

The New Zealand Law Commission completed an exhaustive review of privacy law in four stages culminating in its final stage 4 report (on the Privacy Act 1993) in 2011. This report contained numerous recommendations addressing current issues such as breach notification, cross-border controls and misuse of the personal affairs exception, especially in relation to the use of social media. The Minister of Justice the Hon Judith Collins, promised a bill would be introduced in 2013 repealing the 1993 Act and implementing most of the Law Commission recommendations but this did not eventuate. This year, 2014 is an election year in New Zealand and it remains to be seen if the long-promised legislation will materialise. The Government did, however, announce the appointment of Wellington privacy lawyer John Edwards as the new Privacy Commissioner, replacing the long-serving Marie Shroff who has completed two five-year terms in the role. A bill to address ‘Harmful Digital Communications’ is also in the pipeline addressing social media in particular.

In the meantime the other side of the ledger has seen an alarming erosion of existing privacy protections in New Zealand. One recommendation of the Law Commission that has been speedily implemented has been for better mechanisms for information sharing between public sector agencies to enable efficiency in the provision of services and the detection of fraud. The Privacy (Information Sharing) Amendment Bill was enacted in 2013 inserting a new Part 9A into the Privacy Act 1993. The measures allow information sharing agreements between public sector agencies and even between public and private sector ones to be approved by order in council. On the other hand compensating safeguards, such as mandatory breach notification requirement have not yet been enacted.

This comes against the backdrop of a continuing succession of privacy breaches by public sector agencies such by ACC (Accident Compensation Corporation), IRD and the Earthquake Commission. An earlier detailed audit of ACC and the
appointment of a single information officer to oversee privacy policy across all government agencies have not yet led to fewer privacy breaches.

By far the most contentious intrusion on citizens’ privacy though has been the Government’s enactment of changes to the Government Communications Security Bureau (GCSB) Act 2003 which enables the collection and processing of metadata by the spy agency. Section 8B of the GCSB Act extends its role beyond ‘intelligence gathering and analysis’ about foreign persons and organisations to ‘information infrastructure’ in New Zealand. Information gathered under this category may be provided to the Minister and ‘any person or office holder (whether in New Zealand or overseas) authorised by the Minister to receive the intelligence’. The interception of the private communications of New Zealand citizens and residents is not permitted under the Act but intelligence gathering and analysis of information infrastructure in New Zealand is permitted.

The definition of information infrastructure ‘includes electromagnetic emissions, communications systems and networks, information technology systems and networks, and any communications carried on, contained in, or relating to those emissions, systems or networks.’ The use of an inclusive definition is technology-neutral and permits access to, for example, the ‘Internet of things.’ What led to these legislative changes, however, is more startling.

In addition to the Snowden revelations, public concern regarding surveillance in New Zealand has stemmed largely from a local source. These are the disclosures made in the course of legal proceedings involving Internet tycoon and New Zealand resident Kim Dotcom who has been resisting extradition to the United States for alleged copyright and money laundering violations. It emerged that New Zealand’s secretive intelligence agencies had been illegally monitoring Dotcom’s communications. A subsequent inquiry found many other unnamed residents and citizens had also been targeted leading to the abovementioned measures that essentially legitimise future surveillance. The Bill was enacted despite intense opposition from privacy advocates and large public demonstrations.

Kim Dotcom has become something of a folk-hero in New Zealand. He has announced his intention to launch a political party which, under New Zealand’s strictly proportional electoral system, may end up controlling the balance of power. Privacy will be a major election issue this year. There is still time for the Government to redeem itself by introducing the long-promised Privacy Act replacement but time is running out.

Professor Gehan Gunasekara is an associate professor in commercial law at the University of Auckland Business School. His privacy research has been cited by the Australian and New Zealand Law Commissions and by the Canadian Privacy Commissioner.

---

**Code Red! Key facts about the Credit Reporting Privacy Code**

by David Kreltszheim

From 12 March 2014, the existing credit reporting provisions in the Privacy Act will be replaced by entirely new provisions. Those provisions will be supplemented by a new Credit Reporting Privacy Code (CR Code) that was registered on 22 January 2014 to take effect from 12 March 2014.

**Coverage of the CR Code**

The CR Code binds all credit reporting bodies (CRBs) as well as all credit providers (CPs).
CPs include:

- conventional lenders; and
- retailers, utilities and other suppliers which provide seven or more days' of credit for payment for their goods or services,

which hold credit-related personal information, undertake credit checks on consumer credit information and provide consumer credit default information to CRBs.

The CR Code should be distinguished from the voluntary code that a CP will be required to adopt if the CP wishes to access and report on the more comprehensive data sets that will be available on and after 12 March. CPs that wish to handle 'consumer credit liability information' and (if they are licensees under the National Consumer Credit Protection Act (2009)) 'repayment history information' will need to comply with the voluntary code. The documents that comprise the voluntary code are published by the Australian Retail Credit Association (ARCA) and include the Australian Credit Data Reporting Industry Requirements and Technical Standards and the Principles of Reciprocity and Data Exchange.

*How does the CR Code affect credit providers?*

From a CPs perspective, key features of the CR Code include:

- a requirement to have reasonable practices, procedures and systems, given the size and complexity of its business, that are designed to cover its reporting obligations under the Privacy Act, the Regulations and the CR Code
- additional disclosures to be made by CPs when collecting personal information from an individual that they are likely to disclose to a CRB
- a 'safe harbour' for CP disclosures to be made on a credit provider's website if certain conditions are satisfied
- restrictions on a CP reporting default information to a CRB in certain circumstances where the defaulting individual has made a financial hardship assistance request to the credit provider
- detailed preconditions to be satisfied before default listing an individual with a CRB, including that:
  - the notice informing the individual of an overdue payment and requesting payment (*Section 6Q Notice*) must be separate from the notice of intention to default list the individual with a CRB (*Section 21D Notice*)
  - the Section 6Q Notice must be issued before the Section 21D Notice
  - the Section 21D Notice must not be issued less than 30 days after the issue of the Section 6Q Notice
- details of what a credit provider must include in a notice of refusal of credit
- detailed rules about individuals' rights to access and correct their credit reporting information or credit eligibility information
- complaints handling mechanisms and escalation to the recognised external dispute resolution scheme of which the credit provider is a member
- additional definitions to supplement, amplify and clarify new definitions to be included in the Privacy Act of terms like 'consumer credit liability information' and 'payment information'
- additional details on what a CP must do to assist a CRB regarding the integrity of consumer credit-related information
- clarification of the tests to be satisfied before a CP is able to disclose a serious credit infringement to a CRB on the basis of fraud or because the individual cannot be contacted
- additional restrictions on a CP's ability to use information that is sourced from a CRB, to ensure the information is not used for marketing purposes
- requirements for reasonable systems for secure electronic transmission of credit reporting data
External dispute resolution schemes

A CP which intends to disclose credit information to a CRB must be a member of an external dispute resolution scheme that is recognised by the Office of the Australian Information Commissioner (OAIC). Many CPs would already be members of existing industry-based external dispute resolution (EDR) schemes, such as the Financial Ombudsman Service, Credit Ombudsman Service Limited and the Telecommunications Industry Ombudsman. All of these EDR schemes have now been recognised by the OAIC. As a result, CPs which are members of these schemes do not need to join any other EDR scheme in order to be able to disclose credit information to a CRB.

As of the end of February 2014, three of the State and Territory-based Energy/Water Ombudsman Schemes have lodged applications for recognition with the OAIC but none of these applications have been approved. In addition, there are other Energy/Water Ombudsman Schemes that have not lodged applications with OAIC. It is understood that an amendment is being made to the Privacy Regulations that will have the effect of permitting an energy/water retailer to disclose credit information to a CRB for 12 months without having to be a member of an OAIC-recognised EDR scheme.

***

In summary, CPs need to pay close attention to the CR Code as it supplements and amplifies key obligations under the new credit reporting provisions.

David Kreltszheim is Special Counsel, Clayton Utz and has extensive experience in advising both private and public sector clients on privacy, spam and surveillance device laws. This includes conducting privacy impact assessments and advising on a wide range of privacy issues, including credit reporting, breach notification, offshoring, the handling of health information in clinical trials and in Internet-based patient-support systems, online marketing, call centre procedures and the drug/alcohol testing of employees.
Five Questions for the Australian Privacy Commissioner, Timothy Pilgrim

by Melanie Marks

Amendments to the Privacy Act 1988 introduced under the Privacy Amendment (Enhancing Privacy Protection) Act 2012 will commence on 12 March 2014. The Australian Information Commissioner has the power to make 'guidelines for the avoidance of acts or practices that may or might be interferences with the privacy of individuals, or which may otherwise have any adverse effects on the privacy of individuals'. This includes guidelines in relation to the Australian Privacy Principles (APPs).

The APP guidelines outline how the Information Commissioner will interpret and apply the APPs when exercising functions and powers under the Privacy Act relating to the APPs. The APP guidelines were the subject of public consultation run by the OAIC during the second half of 2013. Whilst primarily aimed at agencies and organisations, all interested stakeholders were invited to make submissions. On 21 February 2014, the OAIC released the APP guidelines. A number of changes have clarified key concepts. A summary of the key changes is available on the OAIC website here.

Australian Privacy Commissioner Timothy Pilgrim has shared these insights with us.

1. How has the relationship between APP1 and APP5 been clarified? Has the OAIC issued new guidance on privacy policies?

The guidelines on APP 5 include new examples of reasonable steps to notify or ensure awareness of the collection of personal information — such as a new example of where it may be reasonable to comply with APP 5 by alerting the individual to specific sections of an APP entity’s APP Privacy Policy. The APP guidelines also include new guidance on a layered approach to notification, new examples of where it may be appropriate to take no steps to notify and refinements to the guidance on the kinds of information to be included in the notification.

APP 1 requires organisations and agencies to have a clearly expressed and up-to-date privacy policy outlining their management of personal information.

An APP 1 privacy policy is required to include information about: the kinds of personal information usually collected and held; how such information is collected and held; the purposes for which the entity collects, holds, uses and discloses personal information; access and correction procedures; complaint-handling procedures; and information about any cross-border disclosure of personal information that is likely to occur, including where practicable, the countries where recipients are likely to be located.

We have been meeting with business and government over the last year, and one of the messages we have received is that entities across the public and private sectors would be keen to see some more guidance on writing effective privacy policies.

We will shortly be releasing an APP privacy policy tool to assist organisations ensure that their privacy policy is as clear and accessible as possible. I know that many organisations will have their new policy well under way by now, which is encouraging. However, it will still be worth assessing a privacy policy against the tool to check that it achieves compliance with the APPs or if it needs more work. The tool will be ready in March.
As you know, the OAIC participated in the OECD Global Privacy Enforcement Network internet sweep last year. The OAIC used the sweep to assess a number of website privacy policies against APP 1. The results showed that some organisations websites had quite a way to go to bring their privacy policies up to best practice.

This was confirmed in our Community Attitudes survey which shows that 51% of Australians don’t read privacy policies on websites, although this number is decreasing. Among people who don’t read privacy policies, the biggest reason by far is that they are too long (52%) or too complex (20%).

2. How frequently and in what circumstances do APP entities need to provide notice?
APP 5 says that an APP entity must take reasonable steps to notify or ensure an individual is aware of certain matters at or before the time the entity collects the individual’s personal information, or if that is not practicable, as soon as practicable after the collection occurs.

This requirement recognises that it is preferable that an individual can make an informed choice about whether to provide personal information to an APP entity. The guidelines give examples of when it may not be practicable to take reasonable steps at or before the time of collection including where urgent collection of the personal information is required and giving a notice or ensuring awareness would unreasonably delay the collection, for example, where there is a serious threat to an individual’s life or health or to public safety.

It may also not be practicable to take reasonable steps at or before the time of collection where the medium through which personal information is collected makes it impracticable to notify or ensure the individual is aware of the relevant matters at or before the time of collection. The test of practicability is an objective test. It is the responsibility of the APP entity to be able to justify that it is not practicable to give notification or ensure awareness before or at the time of collection.

Options for providing early notification or ensuring awareness should, so far as practicable, be built into information collection processes and systems — for example, by including relevant information in standard forms and online collection mechanisms. If notification does not occur before or at the time of collection, the APP entity must take reasonable steps to provide notification, or ensure the individual is aware, of the required matters as soon as practicable after the collection. In adopting a timetable that is ‘practicable’, an entity can take technical and resource considerations into account. However, it is the responsibility of the entity to be able to justify any delay in notification.

3. What has been clarified in relation to the extra-territoriality provisions?
The APP guidelines include further clarification of when an entity, with no physical presence in Australia, is taken to be covered by the Privacy Act because, among other things, it carries on business in Australia.

The phrase ‘carries on business in Australia’ is not defined in the Privacy Act but is further explained in the APP guidelines. The phrase arises in other areas of law that provide guidance on when a business is carried on in Australia. An entity may carry on business in Australia despite the bulk of its business being conducted outside Australia, or the entity not having a place of business in Australia, provided there is some activity in Australia that forms part of the entity’s business.

Activities that may indicate that an entity with no physical presence in Australia carries on business in Australia include: the entity collects personal information from individuals who are physically in Australia; the entity has a website which offers goods or services to countries including Australia; Australia is one of the counties on the drop down menu appearing on the entity’s website; and the entity is the registered proprietor of trade marks in Australia. Where an entity merely has a website that can be accessed from Australia, this is generally not sufficient to establish that the website operator is ‘carrying on business’ in Australia.

4. When should an organisation complete a privacy impact assessment (PIA)?
The OAIC is in the process of updating the Privacy Impact Assessment (PIA) guide. This will be available soon. I
strongly encourage you to re-familiarise yourself with it, even if you have read it before.

A PIA should be an integral part of the project planning process, not an afterthought. A PIA works most effectively when it evolves with and shapes a project’s development, ensuring that privacy is considered throughout the planning process.

A PIA should be undertaken early enough in the development of a project that it is still possible to influence the project design or, if there are significant negative privacy impacts, reconsider proceeding with the project.

Undertaking a PIA should be seen as a process that does not end with the publication of the PIA report. A PIA may be useful more than once during the project’s development and implementation. It should be revisited and updated when changes to the project are considered. If there are substantial changes to how personal information will be handled, it may be necessary to undertake another PIA.

5. Is there going to be a ‘big bang’ on 12 March 2014?

The OAIC recognises that Australian Government agencies and businesses are working hard to implement the new requirements. Our compliance focus in the months following 12 March 2014 will be on working with entities to ensure that they understand the new requirements and have the systems in place to meet them. In resolving matters brought to the attention of the OAIC we will take into account the steps taken by entities to genuinely prepare for the changes and to comply with the new legal requirements. Individuals will continue to have the right to make a complaint to the OAIC and we will deal with these according to our usual processes. In the case of individual complaints we would expect to see a person try to resolve a matter with the organisation or agency first. If the respondent is a member of a recognised External Dispute Resolution scheme, we would also expect the individual to have first accessed that scheme. If a matter is accepted by us, we will always attempt to resolve issues through conciliation. In relation to Commissioner initiated investigations the OAIC will work with respondent organisation and agencies to resolve the matter.

However, where conciliation or working with entities in not effective, we may use our other tools, including determinations, enforceable undertakings or in the case of serious or repeated breaches, initiating court proceedings for civil penalties. This is consistent with our current practices and the approach of the OAIC for some time.

It’s important to remember that while 12 March might be the deadline for the implementation of these changes, there’s no deadline for compliance and continuous improvement. We don’t want to see organisations quickly making the absolute minimum changes, and then sitting back in the knowledge that you have just met compliance requirements.

Organisations should be striving for continual improvement in the privacy space. Don’t just read the law reform guidance on our website, familiarise yourself with our data breach notification guide, our guide to information security, and the information that we have available on issues such as de-identification. These resources will help you to rise above the minimum expectation, to stand out in the increasingly competitive field of customer service.

As we know, community understanding and expectations in regard to privacy are fluid and every changing. Continuous self-assessment is one way you can strive to meet those expectations. This is one of the reasons we have included so much detail in the APP guidelines. You need to know the ‘musts’ and ‘shoulds’ of compliance, but you also need to know the ‘could’s, so that you have the tools available to help you meet best practice
The title of this article is not a cause for alarm but it does capture a mood that I have increasingly felt permeate (and more recently crescendo!) around various privacy related conferences both formally and informally. In the first few months of 2014, I have attended at least half a dozen privacy related training sessions and whilst the audience is always a captive one filled with highly knowledgeable professionals whose remit clearly crosses over into the privacy or data protection arena, I sense a nervous and anxious energy beneath the surface.

Of course, those of us working in this space are all aware of the long path to privacy reform and countless discussions, debates, and pontificating around strengthening and advancing our privacy standards for the new digital age. Yet, somehow with the deadline of 12 March fast approaching I sense many of us feel that more could’ve been done, should’ve been done, will definitely need to be done ... And not to sound blasé but I think that’s OK! It is clear that privacy compliance, like most compliance areas, is not a fixed quantity which is locked and secured in the steam room of an organisation and then left to tick over until a maintenance issue arises!

Privacy compliance is and should be a matter for continual and dynamic dialogue and review. It should in a few words be an inherent part of organisational culture and systems i.e. privacy by design.

Recently many of us have been involved in some rigorous data flow reviews and reformulation of compliance guides and policies. Others may have barely pierced through the surface of the intertwining and complex layers of data flows within business units, within divisions, within local organisations, within global enterprises. Many have eagerly been awaiting the resources and tools from the regulator to assist with finalising and implementing privacy practices.

In the hurried pace to get all ducks in order, I, myself feel a calm before the storm and an awareness that while we all aspire to the Rolls Royce model of privacy compliance platforms, dare I say that the sky will not collapse on 12 March if we are behind the wheel of a Lexus rather than a Rolls! It will, however, put a spotlight on organisations that have fundamentally failed to make appropriate preparations for compliance with the new laws (or in some cases, may be failing to comply with the former laws) – to continue the car analogy, the lemons. That is a certain fact and Privacy Commissioner Timothy Pilgrim has reinforced that whilst his approach will continue to be based on conciliation, there will be no hall passes for organisations who fail to take reasonable steps to adequately address the new requirements. Remembering that what is reasonable will differ for each organisation depending on size, resources etc.

Last week on Friday 21 February 2014 the Office of the Australian Information Commissioner (OAIC) released the final version of the Australian Privacy Principles (APPs) guidelines following public consultation. The guidelines will be a key resource for entities covered by the Privacy Act in implementing and managing compliance with the new laws as they outline minimum compliance requirements and provide practical examples of best practice.

Many readers of this bulletin will probably be well informed on the draft guidelines and used them as a yardstick for advising on the Privacy Commissioner’s likely approach to enforcing the APPs. Some many also have responded during the public consultation period to feed into the finalised version.
Hand on heart I have not completed a line by line read through of the final APP guidelines (though a delta view has proved very useful to note some significant additions or deletions though this is not an exhaustive list by any means!). Key themes and issues that drew my attention are briefly set out below.

Many of the changes relate to clarifying the key concepts that form the basis for the APPs and strategies for implementing a compliance program.

[A.21] An act done or practice engaged in by a person in one of the following categories will be deemed an act done or practice engaged in by the APP entity:

- a person employed by, or in the service of an APP entity, in performing the duties of the person’s employment;
- a person on behalf of an unincorporated body or other body that is established by or under a Commonwealth (or Norfolk Island) enactment, for the purpose of assisting or performing functions in connection with an APP entity; and
- a member, staff member or special member of the Australian Federal Police in performing duties as such a member (s 8(1)).

Information disclosed to a person or member in one of the preceding categories is also taken to be information disclosed to the APP entity.

**Key takeout is that APP entities should ensure all members of staff are included in awareness and compliance training and not only ‘employees’ – should include interns, secondees, contractors etc.**

[B.14] It is reinforced that an overseas based entity may carry on business in Australia despite the bulk of its business being conducted outside Australia, or the entity not having a place of business in Australia, provided there is some activity in Australia that forms part of the entity’s business.

Examples used are the entity has a website which offers goods or services to countries including Australia or Australia is one of the countries on the drop down menu appearing on the entity’s website or the entity is the registered proprietor of trade marks in Australia. Where an entity merely has a website that can be accessed from Australia, this is generally not sufficient to establish that the website operator is ‘carrying on a business’ in Australia.

**Key takeout - The regulator is not shying away from extraterritorial enforcement.**

[B.33] An APP entity cannot infer consent simply because it provided an individual with notice of a proposed collection, use or disclosure of personal information.

**Key takeout - There will be a high bar for showing implied consent. The content and display of collection statements or notices are vital.**

[B.40] If a bundled consent is contemplated, an APP entity could consider whether:

- it is practicable and reasonable to give the individual the opportunity to refuse consent to one or more proposed collections, uses and/or disclosures;
the individual will be sufficiently informed about each of the proposed collections, uses and/or disclosures;

the individual will be advised of the consequences (if any) of failing to consent to one or more of the proposed collections, uses and/or disclosures.

**Key takeout – Take great care in drafting bundled consents, clarity of scope and simplicity for opt outs are vital.**

[B.58] An APP entity will generally disclose personal information when it makes it accessible to others outside the entity and releases the subsequent handling of the personal information from its effective control. Where an APP entity engages a contractor to perform services on its behalf, the provision of personal information to that contractor will in most circumstances be a disclosure (only limited circumstances where it will be a ‘use’).  

**Key takeout – The concept of disclosure is critical for the obligations under APP 8 and whether the entity is accountable for overseas disclosures. This seems to suggest that there may not be a disclosure where the data is accessible to others BUT the entity still retains effective control. Tread carefully on relying on limited exceptions to the term ‘disclosure’ in unchartered waters.**

[B.75] The term ‘holds’ extends beyond physical possession of a record to include a record that an APP entity has the right or power to deal with.

**Key takeout – Stop! Did my data holdings just get bigger? The examples point to an outsourcing arrangement where the data is moved onto a device that is not owned by the data owner. But what about where the entity has the power or right to deal with data not owned by it but by a third party it has some business association with e.g. a joint venture? APP 11.1 provides that an APP entity must take reasonable steps to protect the personal information it holds, including from interference, loss and unauthorised modification. Take caution with the data that your entity may be ‘holding’ and therefore triggering obligations which can be very difficult to manage.**

[Chapter 5] An individual may be notified or made aware of APP 5 matters through a variety of formats, provided the matters are expressed clearly. A notice may be prepared in advance (paper, online, telephone script) and staff should be trained to understand their obligation to take reasonable steps to notify or ensure awareness under APP 5. A notice may also be provided in layers, from a full explanation to a brief refresher as individuals become more familiar with how the APP entity operates and how personal information is handled. Brief privacy notices on forms or signs may be supplemented by longer notices made available online or in brochures.

**Key takeout – The new red herring of APP 5 and the collection statement. Beware of mediums used for collecting personal information and compliance with APP 5. Note that notification can be provided in layers with shorter notifications being supplemented by longer notifications in more suitable mediums i.e. online brochure or by reference to the privacy policy published online.**

[Chapter 8] Many organisations with complicated global network exchanges and offshoring of data will be pleased to see some guidance on listing each of the countries where data is being disclosed. The guidelines now recognise that it may not be practical to list each and every country and allow an entity to list regions where appropriate such as the European Union. Of course, this does not relieve an entity from keeping the notification up to date.

**Key takeout – Stop, revise and survive!**
And remember - the APP guidelines are not legally binding and do not constitute legal advice about how an entity should comply with the APPs in particular circumstances.

Anna Kuperman is Vice President iappANZ

---

Introducing ACLA

The Australian Corporate Lawyers Association (ACLA) is the peak national association representing the interests of in-house lawyers working for corporations and government in Australia.

We cater for all in-house lawyers including those new to in-house through to general counsel working in ASX 200 companies and government departments.

ACLA supports our members by:

- Developing the **knowledge** base about and for the in-house profession;
- Fostering member **collaboration** in forums, networks and think tanks;
- Championing the professional **recognition** of in-house lawyers publicly and recognising personal standing;
- **Advocating** on matters of interest to the in-house profession to shape our nation’s corporate legal environment and promote the understanding of the law within the business and legal communities and by the public;
- Providing cutting-edge in-house specific and developed **education**; and
- **Supporting** members with the tools and services they need to excel personally and professionally in their careers and to be able to give back to the community as a whole.

---

Privacy reflections/predictions for 2014

by Souella Cumming

The high profile privacy breaches of 2012/13 have shed an unprecedented light on personal information in New Zealand. The outgoing Privacy Commissioner, Marie Shroff, is leaving the role at a time when protecting personal information, a cause she has actively championed over the past 10 years, is at the forefront of public awareness and is top of mind for policy analysts, legislators and businesses alike.

*It's not just a public sector issue*

While it’s been the public sector that has made the headlines in New Zealand over the past two years (Accident Compensation Corporation, Ministry of Social Development and the Earthquake Commission, to name just a few), local and international events show that the corporate sector is not immune. Continued technology developments, cost reduction initiatives and changes to business operating models place pressure on traditional/business as usual approaches to protecting personal information for both public and private sector entities. All organisations need to find new, smarter ways of working with customer information that keeps it safe while minimising the compliance burden.
Legislative change required but running hard to keep pace

The recent (information sharing) and pending changes to privacy legislation in New Zealand aim to address some of these issues (compulsory privacy breach notification, and greater powers for the Office of the Privacy Commissioner to audit and require compliance). But will the change come quickly enough? And will it keep pace with the challenges of big data, global information sharing, unauthorised disclosures (Snowden, Assange).

Is education the key?

In a time when the boundaries between public and person information is increasingly blurred organisations and individuals still have a limited understanding of privacy requirements (both the principles of protecting information and the impact on trust and reputation in business and government). Attitudes to accessing and sharing information also vary markedly, and ethical dilemmas abound. Over the past 15 years there has been an increased emphasis on financial literacy in education – is the time right to focus on privacy education in schools and business? Will a more informed public demand more of the organisations they entrust with their personal information?

Expectations of enhanced compliance and greater assurance?

One of the benefits of the high profile breaches is the increased public awareness about the safety of the information they entrust to public and private sector organisations. Public awareness is helping to fuel the call for international standards, better understanding about the risks posed in collecting, using, storing and disclosing information, and assurance that information is protected from inappropriate use/disclosure. Public and private sector organisations need to respond to these expectations and find enhanced ways of providing confidence to their customers and stakeholders.

We know the problems......but finding the right solution(s) is an increasing challenge. It’s not just about legislation, or business systems, accessibility of big data, security, attitudes to information sharing, or ethics or culture – it’s the combination of these things that make solutions complex.

So, no shortage of opportunities for individuals, private sector businesses and public sector agencies to tackle – welcome to 2014!

Souella Cumming is a partner in KPMG’s Advisory practice. She leads KPMG New Zealand’s Government Services and Privacy Advisory Services. Contact Souella on +64 4 816 4519 or +64 27452 1278 or smcumming@kpmg.co.nz
Living in interesting times
by Katrine Evans

One of the dubious delights of being a privacy regulator is the unexpected things that crop up during every working week. It doesn't matter how I plan and prioritise work - some headline-grabbing issue or urgent demand for time and attention will come across the desk and force a rethink. It can be a challenge, but it certainly keeps the job interesting.

For instance in 2013, Edward Snowden’s revelations over government surveillance exploded onto our news feeds at the very time we were making submissions on the government’s plans to revise intelligence agency statutes. Wearable technology and unmanned aerial vehicles raised urgent questions (and not just along the lines of ‘can I have one for Christmas?’). Continuing major data breaches, for example by the Earthquake Commission, challenged public confidence in government and business institutions alike, and some required urgent input from our office. With this backdrop, we expect our upcoming public opinion poll is likely to show an upward trend in people’s concerns about privacy and security – overseas polls certainly suggest that concerns are increasing.

Leaving space to deal with the unexpected isn’t easy when even the ‘known knowns’ (or should that be ‘known unknowns’?) occupy us full time. These include the government’s intention to reform the 20-year-old Privacy Act. The exact shape of the changes is still ‘to be announced’, but we’re hoping for announcements reasonably soon. Proposed changes by the Law Commission, if accepted, would include putting a few more items in our enforcement toolbox, to enable us to deal better with modern information practices and to speed up our current investigations processes. Fingers crossed.

Another challenge is that we believe biometrics is an emerging area that will get more media and public attention. Facial recognition, finger printing and other physiological signature technologies are increasingly being explored as solutions, or options, to deal with a variety of problems. The earlier focus has been on biometric applications in situations such as border control, but applications of biometric technologies are now cropping up in many other domestic and commercial settings.

New applications of technology, will continue to challenge us, such as the much heralded ‘Internet of Things’ and various types of ‘smart’ systems. The different types of wearable technology are only going to grow. Also, younger and younger children are interacting with others online and publishing information about themselves. On the latter issue, we launched our ‘OWLS’ teaching resources for primary schools on 11 February – teaching kids to be wise about privacy online.

Privacy breach notifications are on the rise, and there’s no reason to think that this trend will change in the near future. Breaches are going to continue, particularly in those entities where information management systems are still relatively immature. We were (voluntarily) notified of 107 breaches in the 2012/13 year, compared with 46 for the previous 12 months. This is not necessarily an indication of rising breach numbers (most of which we still wouldn’t know about), but, we optimistically think, shows an increase in awareness about breaches from agencies. Growing breach reporting, though, also ups the pressure on us to provide useful advice and to follow up with investigations into agencies that have had major lapses.

Some of our recent data breach notifications have involved lost or stolen portable devices, including ones supplied by employees. Managing BYOD successfully is becoming a real issue for organisations, particularly with ubiquitous smart phones and the need for more flexible work practices. There’s a growing need for organisations to get their heads around the topic, and to establish or adapt their policies and practices, to get work done efficiently and safely.
It is also poised to be a big year for developments in healthcare information management, with shared care services being introduced by some major health agencies. We’ll continue moving towards new online portals, to enable patients to self-manage their medical records, book doctor appointments, receive results and contact their GPs. Information security and other privacy issues will be closely watched (by us and others) because trust and confidence is so integral to getting people to use the new systems.

Late in 2013, the government announced that it would establish the new role of Government Chief Privacy Officer. This all-of-government position will place privacy at the highest levels of public administration and bring it into line with how many large businesses operate. This is a good investment in helping to improve how people’s personal information is handled.

Last but far from least, we’re kicking off this year with a new Privacy Commissioner. Marie Shroff is stepping down after ten years (two terms) in the role, and John Edwards commenced in the job on 17 February. We’re sure he’ll enjoy it, challenging though being a privacy watchdog can be in these interesting times.

Katrine Evans is Assistant Privacy Commissioner (Legal and Policy), New Zealand. Katrine joined the Office in August 2004, after a ten-year career as a law lecturer at Victoria University of Wellington. She is legal counsel to the Privacy Commissioner, leads and manages litigation and gives advice in the area of investigations. She also manages the Office’s policy, technology and data matching work.

---

Top 10 cyber threats Australian privacy professionals face in 2014

By Michael Sentonas

As businesses reap the benefits of increasing digital connectivity over the next 12 months, they also need to be aware of the growing trends in cyber crime to ensure they can make smarter, more informed decisions on how to best protect their data. The cyber threat landscape in 2014 will feature more sophisticated ransomware, malware, hacktivism and targeted attacks, as cyber criminals move further into the local lucrative business market.

We also expect to see an increase in new and complex attacks on business PCs and mobiles, but it is clear that traditional tactics which have been around for years will also continue to impact businesses. Over the next 12 months, we foresee that ransomware attacks, such as CryptoLocker - which usually target consumers – will move further into the business space where they have the potential to severely affects operations and cost companies a lot of money.

An increase in mobile malware is a certainty and will start to have an impact on businesses via increasingly mobile workforces. Hacktivism attacks which usually target governments are anticipated to spill over into business and enterprise...
markets. Understanding cyber threats and areas of vulnerability in the year ahead is vitally important as more businesses move operations into the cloud and embrace mobile technologies, providing cyber criminals with more entry points into company networks and data. Unfortunately, the poor cyber security foundations of many companies will continue to create an environment of high motivation, high opportunity for the attacker in 2014. In 2013, we saw a number of successful high profile attacks that occurred due to poor patching, misconfigurations, out of date security, and a lack of enterprise wide security visibility. Businesses need to understand that lax cyber security could have significant implications on their company data, operations and financial viability.

For privacy professionals in particular, understanding the risk from 2014’s cyber threats pose is important as they prepare for how upcoming changes to the privacy laws in Australia will impact their organisation.

Over the next 12 months we foresee the following cyber security threats becoming more prevalent:

1. Ransomware – Expect ransomware samples to increase given the financial success the cyber criminals have had with this type of malicious software. Ransomware such as CryptoLocker has typically targeted consumers, but now also targets enterprises.

2. Mobile Malware – The increasing volume and complexity of malware designed to capture identity and financial information will continue to crossover from desktops to mobile devices; a significant issue for an increasingly mobile workforce.

3. Destructive Malware – Cyber attackers are leveraging more destructive functions within their attack code. Cyber criminals will continue to drive the unprecedented rise in destructive malware, some of which are designed to damage the victim’s master boot record resulting in complete computer systems being rendered inoperable.

4. Hacktivism – Hacktivist groups based in Singapore, Malaysia, Indonesia and Australia will continue to target governments in 2014, and are expected to also spill over and target private enterprise.

5. ‘Next Generation’ security tools will come under attack – Attackers will continue to develop exploits that will be ‘sandbox aware’ aiming to bypass security systems, demonstrating that sandboxing is a feature and not a complete security solution.

6. The Internet of Things comes alive – All devices that connect to the corporate network and the internet should be considered endpoints that come with a level of risk as they typically have less security, both by design and through poor security practices, and will be a target for attackers.

7. Bypassing Digital Signatures – More than 1.5 million samples of malware signed with digital signatures already exist and attackers will continue to circumvent the trust mechanisms upon which our digital ecosystems rely.

8. Security vs Privacy debate will continue – In 2014, expect to see some government and corporate organisations go dark in response to privacy issues. Consumer privacy demands will impact security architectures, the cloud, and information sharing. This will be exacerbated in Australia where the new Privacy Act legislation will be enforced from March 2014 with heavy fines for business and consumers.

9. Threat cycles will be recycled – A significant percentage of successful cyber intrusions do not rely on sophisticated techniques, rather the attackers aim to exploit lax security architecture, policy and skills shortages using tried and true methods.
10. Targeted attacks to continue – An increase in targeted attacks on government, large enterprise organisations and small businesses is expected as cyber criminals focus their attempts to financially exploit targets. This does not necessarily mean a correlating increase in advanced malware and advanced persistent threat samples as attackers may use sophisticated or traditional techniques to achieve their ends.

Businesses need to understand the cyber security risks to their operations, and take steps towards mitigating the opportunities for attackers, because while there is financial gain to be made and easy opportunities to steal intellectual property, cyber attacks will continue.

In particular, organisations need to determine how quickly they can restore their critical data and bring systems back on line if attacked by malware designed to freeze or destroy their network.

Michael Sentonas, Vice President and Global Chief Technology for Security Connected at McAfee. He has been with the company for 15 years, in various roles championing for driving the integrated security architectures and platforms that have propelled McAfee into a leadership position as the largest dedicated security provider in the world. Michael is an active public speaker on security issues and provides advice to both governments and business on global and local cyber security threats through various media platforms and at a range of conferences worldwide as well as contributing to various government and industry association’s initiatives on security. He has over 18 years experience in the IT industry, focusing on internet security solutions. Michael holds a B.Sc degree in Computer Science from Edith Cowan University, WA and has an Australian Government security clearance.

Facebook's commitment to privacy
by Rob Sherman

Facebook was founded to give people the power to share and connect, in the ways that they want, with the audiences that they want. As our founder and CEO, Mark Zuckerberg, has explained, trust is the foundation of the social web: we can only fulfill our goal of helping people to share and connect if those people are empowered to control who will see the information they choose to share (https://blog.facebook.com/blog.php?post=10150378701937131)

We're proud that Facebook is rapidly becoming an everyday part of life for the majority of online Australians. It is a global communications platform that is embraced by over 12 million Australians each month. Each day, on average, 4.5 billion pieces of content are shared on the site and there are 4.1 billion likes, which suggests that people find a value and enjoy connecting and sharing with the people, places and things that matter to them each day.

At Facebook, we seek to develop innovative products and services that facilitate sharing, self-expression, and connectivity while putting people in control over their Facebook experience. For example, people who post on Facebook can decide who will see what they share using an inline control that appears at the time they are making a post. More recently, we launched an enhanced Activity Log, which makes it easy for people to see and control the things they’ve posted on Facebook – all in one place.

These tools reflect a meaningful step forward in people’s ability to control their online experience, but they are not the end of the story. Facebook’s global privacy team – like everyone at Facebook – works each day to offer a service that honors the trust that people have placed in us. We do this through a comprehensive ‘Privacy by Design’ process that incorporates...
privacy into our product development, and through external verification – including through comprehensive audits by the Irish Data Protection Commissioner of Facebook Ireland, the company that provides service to Australians, which ‘found a positive approach and commitment on the part of [Facebook Ireland] to respect the privacy rights of its users' (http://dataprotection.ie/viewdoc.asp?DocID=1182).

Most importantly, though, the best way for us to maintain a high standard of privacy on Facebook is to communicate with the people who use Facebook to share with their friends, communities, and customers every day. We do this in many ways, including soliciting feedback when we make changes to the policies that govern Facebook, and by engaging in an ongoing dialogue on our Facebook Pages. Please join the conversation by liking the Facebook Page for Australia: https://www.facebook.com/FacebookAU and the Facebook and Privacy Page: https://www.facebook.com/fbprivacy

Rob Sherman is Facebook’s Privacy & Policy Manager in Washington D.C.
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.

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 profile 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 enough not to be at our Summit.
- There will (sadly) be one prize only. Its value is AUS$250, so that’s pretty good really.
- We may need to verify the winner’s identity so we don’t give the prize to the wrong person.
- If the prize is not claimed for any reason (and we hope this won’t happen) the author of the runner-up article as judged by the Editorial team will receive the prize.

To make sure things go smoothly and fairly (and we are sure they will) we just have to say that our decision in relation to any aspect of the award of the prize, including the content and publication of submitted articles, is final and binding and not up for discussion.
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>Time, Date &amp; Location</th>
<th>Information</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Thursday 13 March 2014</strong>&lt;br&gt;5.30pm – 7.30pm&lt;br&gt;Minter Ellison Lawyers&lt;br&gt;1 Eagle Street&lt;br&gt;Brisbane QLD 4000</td>
<td>Credit Reporting workshop&lt;br&gt;<strong>Speakers:</strong>&lt;br&gt;Ian Lockhart - Partner, Minter Ellison&lt;br&gt;Damian Paull - CEO, ARCA&lt;br&gt;Andrew Rice - National Security Resilience Policy Division, Attorney-General’s Department&lt;br&gt;Emma Hossack - Chair/MC, President, iappANZ</td>
<td>Free for iappANZ members&lt;br&gt;$99 for non-members&lt;br&gt;Costs deductible from joining fee&lt;br&gt;ACLA members - 15% discount workshop fee&lt;br&gt;<a href="#">Information and register here</a></td>
</tr>
<tr>
<td><strong>Wednesday 19 March 2014</strong>&lt;br&gt;5.00 – 7.30pm&lt;br&gt;Pricewaterhouse Coopers&lt;br&gt;L19, 2 Southbank Boulevard&lt;br&gt;Melbourne</td>
<td>Data Security workshop&lt;br&gt;<strong>Speakers:</strong>&lt;br&gt;David Shaw - Shaw information, security consultant&lt;br&gt;Mike Burnett - Lawyer, Gilbert + Tobin&lt;br&gt;Kerryn O’Brien - Kerryn O’Brien Management Consultant&lt;br&gt;Ben Carr - CPO, Telstra</td>
<td>Free for iappANZ members&lt;br&gt;$99 for non-members&lt;br&gt;Costs deductible from joining fee&lt;br&gt;ACLA members - 15% discount workshop fee&lt;br&gt;<a href="#">Information and register here</a></td>
</tr>
<tr>
<td><strong>Tuesday 25 March 2014</strong>&lt;br&gt;2.45pm – 5.30pm&lt;br&gt;Corrs Lawyers&lt;br&gt;L17, 8 Chifley Square&lt;br&gt;Sydney</td>
<td>Privacy Health Check workshop&lt;br&gt;<strong>Speakers:</strong>&lt;br&gt;Helen Clarke – Partner, Corrs Chambers Westgarth&lt;br&gt;James Kelaher – Director, SmartNet&lt;br&gt;Dr Richard Kidd, Specialist VR General Practitioner&lt;br&gt;Dr Patricia Williams – Author, RACGP Computer + Information Security Standards</td>
<td>Free for iappANZ members&lt;br&gt;$99 for non-members&lt;br&gt;Costs deductible from joining fee&lt;br&gt;ACLA members - 15% discount workshop fee&lt;br&gt;<a href="#">Information and register here</a></td>
</tr>
<tr>
<td><strong>November 2014</strong></td>
<td>iappANZ annual Privacy Summit</td>
<td>TBC</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.