iappANZ is delighted to welcome the Commonwealth Bank of Australia as our newest Platinum Sponsor. iappANZ relies on the generosity of organisations which value privacy to support its training Programmes, Annual Summit, Bulletins and industry participation in other formal and informal events. The commitment of the Commonwealth Bank of Australia to the promotion of privacy in Australia has been notable in its support of the OAICs recent “Community Attitudes to Privacy Survey”. The bank has previously highlighted that the highest standards of privacy and security underpin its world-leading solutions across a range of platforms, including mobile. “Trust is vital to deepen our customer relationship value in mobile banking” says Michael Harte, Group Executive Enterprise services and Chief Information Officer Commonwealth Bank. “Our strong platforms and security layers are at the heart of all our technology, and have spearheaded the growth in consumer confidence in mobile banking services”, he adds, which is a theme which will be expanded in our Summit on 25th November which has the theme of “privacy unbounded” and the CIO of Nokia, and Danny Weitzner in particular will be discussing how privacy can be used to enhance organisations business.

Nominations for the iappANZ Board are coming in record numbers which is marvellous, and we look forward to the election at the AGM which will immediately follow the Summit. Please make sure that you send a brief Bio for circulation amongst the membership before the Annual General Meeting, which will take place immediately following the last session at the Summit and before the Cocktail party. Stay in touch at LinkedIn: http://www.linkedin.com/groups?gid=1128247&trk=anetsrch_name&qoback=gdr_1281574752237_1 and follow us on Twitter at: https://twitter.com/iappANZ
It has been a tremendously busy and exciting month for our association with some excellent opportunities to engage with our first class membership in events held in Sydney on 30 September (Data In Flight) and in Melbourne on 21 October (Credit Reporting Workshop). We continue to be grateful to our especially generous members and Board who dedicate their time and efforts to knowledge share and provide specialist insights on management of privacy compliance.

In this month's bulletin, David Kreltzheim (Special Counsel, Clayton Utz) sheds light on how the credit reporting reforms will affect credit providers outside the finance sector such as retailers, utilities and other suppliers which provide seven or more days' of credit for payment for their goods or services. It is an overlooked point that credit reporting reforms are of significance not only to finance and credit industry and those working in compliance in other industries need to know how their organisation may be captured.

In a sharp contrast, Vanessa Hoban (Privacy Advisor, nehta - National E-Health Transition Authority) provides a great piece on changes to laws affecting tattoo parlours and nightclubs in Kings Cross with serious privacy ramifications. Helen Davidson has recently written an article (see: http://www.theguardian.com/world/2013/sep/19/privacy-scan-nightclub-patrons-sydney) on the enduring tension between public safety and privacy. Public sentiment on this issue seems to shift in parallel with media articles on drug and alcohol induced violence which fuels outcries for tougher measures on curbing the hooligans while glossing over some fundamental privacy issues. Helaine Leggat (Information Legal) shares her unique insights into the power of the digital economy and all that goes with it. And for those of you that found the first part of our interview with Privacy Commissioner intriguing in last months' bulletin part two follows in this bulletin.

Finally, regular contributor Joel Camissar from McAfee provides a useful snapshot of the trends reported in 2013 Community Attitudes to Privacy report, released in October. Can you believe 97 per cent of Australians believe it is a misuse of their personal information when it is collected by an organisation for one reason and then used for another. The importance of trust and can privacy never be overstated.

As always, we welcome contributions from all of our members and encourage debate and alternate opinions on any articles published. Please send in your views!

iappANZ Credit Reporting Workshop

By Veronica Scott
iapANZ Director and Special Counsel, Minter Ellison

The new comprehensive credit reporting regime is both an opportunity and a challenge. The evening of Monday, 21 October saw iappANZ run its first workshop on the new provisions in Part IIIA of the Privacy Act 1988 hosted by Minter Ellison in Melbourne. We were very lucky to have as our guest speakers Damian Paull, CEO of the Australasian Retail Credit Association (ARCA), and Ian Lockhart, partner at Minter Ellison (Brisbane). Key highlights from the workshop and takeaways are:

- the proposition of the key role credit reporting bodies (CRBs) will play in the new credit reporting system (arguably acting almost as a quasi regulator) in terms of the requirements they have for the information that will be disclosed to them by credit providers (CPs). CPs should therefore be getting to know their CRBs;
- how the system will deal with pre-commencement information;
CP collection notice obligations;
- the complexity of the requirements for sending default notices to consumers before defaults can be listed with a credit reporting body;
- the new industry standard for the exchange of positive data;
- the reciprocity of the system - CPs will get the information out that they put into the system, for example, negative information in: negative information out;
- there will be many CPs who, whilst not collecting the new sets of positive credit reporting data (eg repayment history), will nevertheless have additional obligations under Part IIIA if they participate in the system; and
- the importance of the role external dispute resolution bodies will play.

In this month’s bulletin, we have an article from David Kreltszheim, special counsel, of Clayton Utz which carries on the theme and highlights some of the key issues of where things stand today. We also have some comments from the Privacy Commissioner on the new system in his answers to our five questions. As David says, it is crunch time.

Credit Crunch Time: Less Than Five Months to go

By David Kreltszheim,
Special Counsel,
Clayton Utz

David 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 center procedures and the drug/alcohol testing of employees.

From 12 March 2014 the existing credit reporting provisions in the Privacy Act will be replaced by entirely new provisions. Credit providers and other affected organizations need to ensure that their practices, procedures and systems for handling credit-related personal information comply with the new credit reporting provisions by that date.

Many of the major players in the financial services industry have had substantial credit reporting compliance projects on foot for a considerable period of time. However, there are numerous credit providers outside the finance sector which will need to focus on the new provisions if they have not already done so. In particular, retailers, utilities and other suppliers which provide seven or more days’ of credit for payment for their goods or services need to comply if they hold credit-related personal information and if they wish to continue to undertake credit checks on consumer credit information and provide default information to credit reporting bodies (CRBs).

Actions being taken to ensure readiness by 12 March 2014 include:
- affected organisations undertaking a “gap analysis” to identify where existing practices, procedures and systems need to be changed to comply with the new provisions and then implementing the necessary changes; and
- credit providers considering the scope for improved credit decision-making in the light of the additional data sets of credit-related personal information that are potentially available to them (and implementing any additional procedures that may be necessary if they elect to obtain additional data sets).

The new obligations of credit providers and other affected organizations will ultimately be set out in:
- the new Part IIIA of the Privacy Act: this was enacted last year;
- the new mandatory Credit Reporting Code: a draft Code prepared by the Australian Retail Credit Association (ARCA) as the designated Credit Reporting Code Developer was submitted to the Office of the Australian Information Commissioner (OAIC) in July 2013, but this has yet to be approved; and
the Privacy Regulations: as at 21 October 2013 these have yet to be released.

In addition, ARCA is developing a voluntary Industry Code and a supporting Data Standard. These documents are relevant to credit providers wishing to access additional data sets of more comprehensive credit-related personal information (these are described below). A final version of the Data Standard is not expected to be available for release until November 2013 and at least 30 days after the OAIC approves the new mandatory Credit Reporting Code.

Undertaking a "gap analysis" is not a straightforward task. Although many of the substantive features of the existing credit reporting provisions are essentially unchanged, it is only possible to discern this by working carefully through numerous new definitions in the (very differently structured) new Part IIIA of the Privacy Act. This task of undertaking a "gap analysis" is compounded by the fact that the mandatory Credit Reporting Code has not yet been approved and the Privacy Regulations have not yet been released.

Overview of changes

The existing credit reporting provisions were introduced in 1991 and pre-dated the significant changes in privacy law and practice that have occurred in the last 15 years, including the inclusion of the National Privacy Principles and associated private sector provisions in the Privacy Act in 2001.

In contrast, the new provisions mesh with the broader regulation of how organizations handle personal information more generally by mimicking the order and structure of the new Australian Privacy Principles (APPs) that will also come into effect on 12 March 2014.

The new provisions replace the existing provisions that control the content and handling of "credit information files", "credit reports" and "reports" with new provisions that regulate the handling of various types of credit-related personal information at different stages in the information life-cycle. To do this, the new provisions deploy a series of new concepts that take account of the flows of information to and from CRBs as well as how that information is augmented as it flows from a credit provider (CP) to a CRB and then back to the CP and then potentially on to other CPs and other "affected information recipients" like related bodies corporate of a CP, as well as credit managers and credit processors.

The new provisions still regulate the handling of consumer credit information only. However, that concept has been expanded to include credit for residential investment property purposes, in line with changes made to the scope of regulated credit in the National Credit Code in 2010.

The 5 new data sets

The current system permits the handling of very limited categories of "negative" default information. In contrast, the new provisions allow for the handling of additional data sets of more comprehensive credit information, namely:

- 4 items of "consumer credit liability information" (CCLI), broadly the type of consumer credit plus details of the provider and whether the provider is a credit licensee under the National Consumer Credit Protection Act, the commencement and end date of that credit, certain details of repayment terms and the maximum amount of credit available; and
- "repayment history information" (RHI), broadly information about whether an individual has met an obligation to make a monthly payment that is due and payable in relation to consumer credit, the day on which that payment is due and payable and (if paid after the due date), the date on which the individual makes the payment.

Broadly, only credit providers which are credit licensees will be permitted to handle RHI.

Credit providers wishing to have access to CCLI or RHI need to observe the principle of reciprocity to be embodied in ARCA’s voluntary Industry Code and supporting Data Standard. That is, a credit provider will only be able to take out of the system the level of data that corresponds with the level of data that it contributes to the system (i.e. negative only, negative plus CCLI or comprehensive).

Other changes - a snapshot

A credit provider needs to focus on several matters in the lead-up to March 2014, including:

- the need for new documents: these include a written policy setting out how it manages credit-related personal information and a collection statement notifying individuals about a range of notifiable matters
- the need to develop and implement new practices, procedures and systems to comply with the new
requirements: these could include system changes that have a significant lead time

- that it will be required to be a member of an OAIC-recognised external dispute resolution scheme before it will be permitted to disclose credit information to a CRB
- that the amount of the minimum default payment reporting threshold has been increased from $100 to $150
- that there are significant changes to the way in which it must deal with individuals' requests for access and correction of credit-related personal information

- That there are opportunities for CRBs to assist it by pre-screening individuals to determine their eligibility to receive direct marketing from it.

---

**Bikies and Tattoos and Clubs! Oh, my!**

By Vanessa Hoban
Privacy Advisor
nehta - National E-Health Transition Authority

The 2012 Underbelly spinoff, *Bikie Wars: Brothers in Arms*, was a glorification of Australia's bikie culture neatly condensed into a six-part miniseries. Packed full of montages of violence and nudity, it dramatized the event of the Milperra Massacre, when the Bandidos and the Comanchero bikie clubs went to war on Father's Day in 1984.

One year later and bikie gangs are back on Australian television, albeit without an overlayed rock 'n' roll soundtrack. If you believe the news, there is currently a war on the streets of Sydney between rival bikie gangs disagreeing over turf, guns and illegal imports. Although, in the last few months, the New South Wales Police Commissioner, Andrew Scipione, publicly commented that he disagreed with the idea that Sydney's bikie gangs are at war.¹

Whether or not a bikie war endures, one thing is for certain, and that is the recent introduction of bikie related laws aimed at cracking down on Australian organised crime. One of these laws has been a reform to the tattoo industry, which is designed to break the

‘stranglehold that outlaw motorcycle gangs have over the tattoo industry in New South Wales’. Police have estimated that one in four tattoo parlours are bikie affiliated.\(^3\)

From October this year, all tattoo parlor owners are required to have an operator license. The alternative is an $11,000 fine, plus another $11,000 per day until the owner complies.\(^4\) An individual tattoo artist must also have a license or face an initial $5,500 fine and an $11,000 fine for any subsequent offence.\(^5\) The new law also gives powers of entry to police officers without warrant to enforce compliance.\(^6\)

Each application for a tattoo parlor license must be accompanied with the name and residential address of each staff member employed to work at the tattoo parlor.\(^7\) The requirement for an organization to supply the personal information of its employees to a government agency would not be an issue for the vast majority of organizations. But, the tattoo industry is unique.

If tattoo artists believe the conservative estimate of the New South Wales police that one in four tattoo parlors are bikie affiliated, then the likelihood that artists would want to supply their personal information, including their address, to a parlor owner is very low, to say the least. This leaves tattoo artists in a bit of a bind over whether job security is more important than home security.

Unfortunately, current privacy law cannot alleviate tattoo artists’ concerns. While the Australian Law Reform Commissioner’s report into privacy recommended the removal of the employee record exemption,\(^8\) the current Privacy Act reforms do not touch on this removal, nor does the Privacy Act provide for compensation measures for those whose privacy has been breached. Even if those bikie affiliated parlor owners were subject to the Privacy Act with regard to their employee records, it’s a slim chance that this would deter bikies from misusing the personal information of their employees. If the Crimes Act doesn’t deter bikies, the Privacy Act certainly won’t.

Since the New South Wales government has rolled out the new bikie laws, it is now turning its attention to alcohol-fuelled violence on the streets of Sydney. The government, in its latest sitting, passed law which requires ‘high-risk’ venues in Kings Cross to scan the identity of customers to prevent customers who are thrown out of a venue from entering another.\(^9\) The recent reforms originate from the Kings Cross Plan of Management 2012 which ensued from a series of violent incidents, including the death of teenager Thomas Kelly in Kings Cross in July last year.

Pursuant to the new law, a person can be issued a 48 hour precinct ban prohibiting entry to ‘high risk’ venues to a person who is drunk, violent or disorderly.\(^10\) A person may also be subject to a 12 month precinct ban where that person has been charged with, or found...
guilty of, a serious criminal offence involving alcohol related violence. Those subject to a banning order who enter, or attempt to enter, a Kings Cross licensed premises could face a fine of up to $5,500.\textsuperscript{11}

To complement the banning order provisions, the new law requires ‘high risk’ venues in Kings Cross to undertake ID scanning from 7pm on Fridays until 7am on Mondays.\textsuperscript{12} A ‘high risk’ venue is one that admits 120 or more patrons and is open past midnight. There are approximately 35 ‘high risk’ venues in Kings Cross. Each individual scanner will be linked to a central identification scanning system. This will ensure that those who have been issued with a banning order ‘can be stopped at the door and not jeopardize the safety of patrons and staff’.\textsuperscript{13}

The NSW Council for Civil Liberties has criticized the new law, stating that patrons will be forced to hand over their personal information to ‘colorful Kings Cross identities’.\textsuperscript{14} These types of identities include bikie gangs and associates of some of the more notorious figures in Kings Cross, such as John Ibrahim. Concerns have also been raised that the personal information collected by the clubs could be disclosed for direct marketing or customer profiling, or be misused for financial, credit card or identity fraud.

Pubs and clubs are subject to the Privacy Act and must collect, use and disclose the personal information they collect in accordance with the National Privacy Principles. In addition, the new law requires licensees and staff operating ID scanners to undergo privacy training and licensees will also be required to adopt an approved privacy management plan and policy.\textsuperscript{15}

However, it is questionable as to how these privacy ‘safeguards’ will ensure the integrity of the Kings Cross ID scanning system and protect the personal information captured by the linked scanners. The authority of the Privacy Act has not prevented inappropriate use of personal information by clubs before. In 2010, the federal Privacy Commissioner published guidance to licensed venues over their privacy obligations following complaints that staff at venues were using scans of female patrons’ driver licenses to get their names and addresses.\textsuperscript{16}

The new tattoo industry regulations and the linked ID scanners initiative highlight the difficulties in balancing the broader interests of society. On the face of it, these areas of regulation appear contradictory. There are now robust licensing restrictions around the tattoo industry to stop the bikie ‘stranglehold’, which seem to be in the public interest. But individual tattoo artists’ privacy and safety is potentially put at risk by necessitating artists to disclose personal information to parlor owners. The government initiative to scan driver licenses in Kings Cross is designed to protect innocent victims from alcohol-fuelled violence. However, the unintended upshot is this increases the risk of club patrons’ personal information being in the hands of those associated with ‘colorful identities’, including bikies. As privacy professionals, we are often afflicted with tunnel vision. We get caught up in the interpretation of a privacy principle, the fine-tuning of a privacy policy or construing the differences between state and federal legislation. We seldom stop to think of the guiding principles behind privacy law or the significance of balancing the value of privacy with other interests.

It would be remiss for us as privacy professionals to neglect the bigger picture. You may have thought that bikies, tattoos and Kings Cross nightclubs, having been glorified in Underbelly style mini-series, form part of a separate sub-culture and affect different types of people. But bikies, tattoos and Kings Cross nightclubs are more relevant to you, as a privacy professional, than you may think.

\textsuperscript{11} Section 116AE, Liquor Amendment (Kings Cross Plan of Management) Bill 2013
\textsuperscript{13} Second Reading Speech of the Liquor Amendment (Kings Cross Plan of Management) Bill 2013
\textsuperscript{14} http://www.abc.net.au/pm/content/2012/53692926.htm
\textsuperscript{15} Section 116AC(4), Liquor Amendment (Kings Cross Plan of Management) Bill 2013.
\textsuperscript{16} Privacy Commissioner Inforantion Sheet (Private Sector) 30 – 2010: ID scanning in clubs and pubs.
More than the Bottom Line

By Helaine Leggat
| Bachelor of Law | CISSP | CISM | CIPP/US | CIPP/IT

Helaine Leggat is one of a few people in the world to hold a bachelor of law degree together with information security, governance and privacy qualifications from global leaders in these fields. An executive director with over 20 years of experience, she is currently involved in providing strategic advice to government Entities and global organisations. Her client engagements and Professional affiliations include the following jurisdictions: European Union, United Kingdom, United States of America, Africa, Australia, New Zealand and Singapore.

I recently watched and highly recommend a video of J. Trevor Hughes the President and CEO of the IAPP on Data Privacy available at www.youtube.com/watch?v=3eniaZVpX8c.

Mr. Hughes speaks of the importance of data privacy to “organizations worldwide”, highlighting the complexity of the privacy risk matrix and stating that data privacy has “......emerged as perhaps the most significant consumer protection issue - if not citizen protection issue (my emphasis) - in the information economy”.

According to Mr. Hughes, data privacy has become an enterprise-wide concern affecting the bottom line because of its impact on competitiveness, brand loyalty and customer trust. Mr. Hughes does not elaborate on the issue of “citizen protection issue”. I would like to pick up on this thread. It is an area that needs far more attention and one where I believe there are both governance and ethical obligations that demand more than concern for the bottom line. There is also a moral obligation to assist in the protection of the societies in which we live because individuals and societies are threatened by increasing levels of state and corporate surveillance nearly all of which concern personal information.

If law (simply put) is about norms within a particular society at a particular time, then law at this time is about information. ‘Privacy’, ‘data subject’, ‘personal information’ and so on, are mere nomenclature. What we are really talking about is, people. Organizations, as custodians of personal information, have in a very real way become guardians of people and their ideas.

Countless recent articles refer to personal information as the ‘new gold’ of organizational assets. If this means that personal information has value, including financial value, I agree. My contention is that the value and concomitant risk are not properly appreciated. People are the new currency in the tug of massive change. Change, which is connected to wealth and power.


While the focus of the lecture is Intellectual Property, Gurry, like Niall Ferguson, in his book titled “Civilization, the West and the Rest”, tells the story of shifting powers. The shifts arise from the one thing common to all societies – people – their individualism and talent for innovation in combination with the digital renaissance.

Ferguson, speaks of “5 Killer Apps” - competition, science, property, medicine, consumption (consumerism) and work (ethic), which are tilting the balance of power from the West after more than 500 years of Western supremacy. Interestingly, Australia and New Zealand are positioned at the heart of the shift in more ways than one.

Gurry, speaks of economic, geo-political (geographic) and political shifts. An examination of which supports the shift in dominance from West to East. Based on the Standard and Poor’s top 500 index rating in the US, Gurry quotes the value of intangible assets in 1978 at 5% as against tangible assets, increased to 95% in 2010 – a reflection of the growing importance of knowledge based capital and which demonstrates that investment follows innovation.

Gurry references evidence of a massive geo-political shift in the center of gravity brought about by technology the likes of which has not been seen in hundreds of years. He cites investment in research and development, with China now the 2nd largest
investor in research and development after the US and followed by Japan. Together, China, Japan and Korea now file 38% of all Intellectual Property applications worldwide. China alone files 25% of the world’s patents. China has the largest patent (brains trust) office in the world.

In terms of the political shift, Gurry speaks of the diffusion of power from state to society (people), brought about by the Internet and Social Media that inter alia “busted” the state monopoly on policy (‘Arab Spring’).

People create individual and state wealth. People, acting together, can overpower state authority. While neither of these consequences is new, the effect of each is massively propelled by technology and innovation. The increase in the ‘value’ of people in respect of economic success and the stability of states has resulted in increased levels of surveillance – surveillance carried out largely on/through the personal information of people that is in the care and custody of public and private sector organizations.

Anyone who reads widely will be aware of news relating to information warfare, espionage and surveillance. Espionage is occurring at a state and organization level, for reasons of state power and economic advantage. Hyperbole aside, we have what Keith Alexander, Director of the National Security Agency, US Cyber Command, has called “the greatest transfer of wealth in history”. The ‘IP Commission Report’ available at www.ipcommission.org/report/IP_Commission_Report_052213.pdf, quotes sums of stolen Intellectual Property in excess of US$300B per annum, in excess of the value of real asset exports from the US to Asia.

In April 2013, Mark Zuckerberg founded a lobby group called FWD.us (pronounced Forward US), which seeks to promote the equivalent of the Australian 457 visa in the US, the H-1B visa. FWD.us seeks to attract the most talented and hard-working people to the US as part of the effort to stem losses to Western supremacy.

So, what has all this got to do with privacy and personal information? For me, personal information is the stuff of power and wealth. The currency of the digital economy.

Australia and New Zealand are tied through history and tradition to the West. Geographically they are remote from the West. Close to China, Japan and Korea. Economically, even culturally, ANZAC countries have symbiotic and inter-dependent relationships with their Asia Pacific neighbors.

I believe that Australia and New Zealand play a critical role in the changing balance of world power and that personal information is part of the change. It will be interesting to see how things develop.

Organizations here should not think of the changing Australian privacy regime as just another compliance requirement. They should look further and wider to see the greater good, embrace the future, and do more.

---

**Five questions for the Commissioner on Guidelines to the Australian Privacy Principles**

The Australian Privacy Principles (APPs) will come into force on 12 March 2014. The Office of the Australian Information Commissioner (OAIC) has released a set of draft privacy guidelines to assist organizations and agencies understand their obligations and how the OAIC will administer the changes under the APPs (APP Guidelines). Public consultation has been conducted in tranches with the second stage of consultation (covering APPs 6-11) concluding on 21 October 2013. The third and final part of the guidelines will be released for public comment at the end of October.

The APP Guidelines will be issued by the Information Commissioner (the Commissioner) under the guidance of the Commissioner, Timothy Pilgrim.
related functions set out in the Privacy Act 1988. While the APP Guidelines are not binding, the draft APP Guidelines outline how the Information Commissioner interprets and applies the APPs when exercising functions and powers under the Privacy Act relating to the APPs. Privacy professionals should therefore be familiarizing themselves with the APP Guidelines in the lead up to March 2014.

The iappANZ took the opportunity to speak with Privacy Commissioner Pilgrim about the APP Guidelines and what can be expected in the final stage of the consultation.

1. **Can you give us a sense of the types of issues that stakeholders commonly raised in relation to the consultation on the second part of the draft APP Guidelines?**

   Stakeholders have raised a number of issues that we will consider before finalising the guidelines. These issues include:
   - the scope and operation of the new ‘permitted general situation’ exceptions under APP 6 (Use or disclosure of personal information) which outlines situations where the collection, use or disclosure by an APP entity of personal information about an individual, or of a government related identifier, will not be a breach of the APPs
   - in relation to APP 7 (Direct marketing), the need to ensure there is an appropriate balance in the APP Guidelines between facilitating legitimate direct marketing practices and addressing community concern that some aspects of these practices raise privacy concerns
   - when APP 8 (Cross-border disclosure of personal information) applies, including whether it applies to personal information shared with an overseas contractor such as a cloud service provider
   - how the exception in APP 8.2 (a) applies to a particular law or binding scheme. This exception permits an entity to disclose personal information to an overseas recipient where the entity reasonably believes that the recipient is subject to a law or binding scheme that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the APPs protect the information
   - when personal information would be considered ‘de-identified’ under APP 11 (security of personal information), for example the potential for personal information to be re-identified through analytics.

   We will be publishing all the submissions we received to the second stage of consultation.

2. **The amendments to the Privacy Act extend the operation of the Act to organisations or small business operators that have an “Australian link”. What approach will your Office be taking to regulate the activities of foreign organisations that have an “Australian link”?**

   The Privacy Act applies to acts or practices engaged in outside Australia, by an organization or small business operator that has an ‘Australian link.’

   A range of organizations and small business operators will have an ‘Australian link,’ including for example, a body corporate incorporated in Australia. An entity that ‘carries on a business in Australia’ will also be covered where the personal information was collected or held by the entity in Australia either before or at the time of the overseas act or practice.

   The OAIC will assess, on a case by case basis, whether an entity has the requisite Australian link before considering whether to investigate a privacy complaint. The OAIC will also consider a range of other matters before taking regulatory action against a foreign entity. These matters will be addressed in the OAIC’s privacy regulation strategy that we aim to release before the amendments commence.

3. **APP 8 and a new section 16C of the Privacy Act introduce an accountability approach to organisations disclosing personal information across borders. Specifically, before disclosing the information, an entity must take reasonable...**
steps to ensure that the overseas recipient does not breach the APPs (other than APP1) in relation to that information.

What are the types of actions that might constitute “reasonable steps”?

The draft APP Guidelines state that the appropriate steps for an entity will depend upon a range of circumstances, including: the nature of the personal information, the entity's relationship with the overseas recipient, the risk of harm to an individual if the information is mishandled by the overseas recipient, any existing technical and operational safeguards implemented by the overseas recipient to protect the privacy of the personal information and the practicability of taking particular steps.

The draft APP Guidelines also indicate that it is generally expected that an APP entity should enter into an enforceable contractual arrangement with the overseas recipient that requires the recipient to handle the personal information in accordance with the APPs (other than APP 1). These contractual arrangements may, for example, cover the types of personal information to be disclosed and the purpose of the disclosure; a requirement that the overseas recipient complies with the APPs in relation to the collection, use, disclosure, storage and destruction or de-identification of personal information; the process for handling privacy complaints; and a requirement that the recipient implement a data breach response plan.

4. **Under APP 10**, an organisation must take reasonable steps to ensure that the information it uses or discloses is accurate, up-to-date, complete and “relevant”. How would an APP entity determine if information it uses or discloses is “relevant”?

‘Relevance’ is assessed by considering the purpose of the use or disclosure.

Generally, an entity should first consider the purpose of the use or disclosure, and then assess whether the information is relevant to that purpose. It must take reasonable steps to ensure it only uses or discloses personal information it holds about an individual that is relevant to the purpose of a particular use or disclosure.

The following example is included in the draft APP Guidelines: an organization holds personal information about a client (including the client’s name, address, job description, financial position, physical disabilities and marital status), that was collected for the purpose of providing the client with financial advice. The organization is later instructed to buy shares on the client's behalf. In this case, the organization must take reasonable steps to ensure that when doing so, it only uses and discloses parts of the information relevant to purchasing the shares, such as the client's name.

5. **The credit reporting laws have also been subject to significant change**, including the introduction of a new division dedicated to recipients of credit information other than credit reporting bodies and credit providers (‘affected information recipients’). What advice do you have for these persons or entities that will be required to comply with credit reporting laws?

The term ‘affected information recipients’ (AIRs) is used to refer to various third parties to whom credit-related personal information is disclosed by credit reporting bodies and credit providers, such as mortgage and trade insurers, related body corporates, credit managers and advisors.

Certain rules apply to AIRs in relation to their handling of a set of regulated information within the credit reporting system. These rules include requirements to:

- have a clear and up-to-date policy for the management of the regulated information,
- take reasonable steps to comply with relevant Privacy Act provisions and the Credit Reporting Code, and
- notify the individual about information on access, correction and complaint rights.

I would advise any entity that believes it may be an AIR to review the relevant provisions in the Privacy Act to ensure they understand the obligations that apply to them. The OAIC has developed a Privacy business resource entitled “Credit reporting — what has changed” which provides information on the major changes to Australia’s credit reporting framework, which will be a useful resource for AIRs to consider. Furthermore, the draft Credit Reporting Code has been submitted to the OAIC for registration and is currently being assessed. This Code will outline obligations relevant to AIRs.
Australians’ growing online privacy concern is a wakeup call for businesses.

By Joel Camissar,
Data Loss Prevention and Privacy Lead with

McAfee
An Intel Company

Trust and privacy are becoming increasingly important to Australians in our connected world, and recent research by the Office of the Australian Information Commissioner (OAIC), in conjunction with McAfee, has found that as consumers we are becoming more privacy savvy and aware, and are placing more value on our digital footprint.

According to the 2013 Community Attitudes to Privacy report, released in October, and co-sponsored by Commonwealth Bank of Australia and Henry Davis York, an overwhelming 97 per cent of Australians believe it is a misuse of their personal information when it is collected by an organisation for one reason and then used for another.

In addition, the research found that one in three Australians have had an issue with the way their personal information was handled in the last year, and a significant portion of Australians (29 per cent) would go straight to the business responsible for a suspected data breach – an increase from 13 per cent in 2007.

The longitudinal study, last conducted in 2007, explored the changing attitudes of Australians on the use of their personal information and what came through very clearly is that changing attitudes are a timely wakeup call for businesses and government agencies in the lead up to the enforcement of changes to the Australian Privacy Act in March next year.

The findings have significant ramifications for Australian businesses and government agencies keen to build trust and secure customer loyalty, and suggest the need for organisations to effectively communicate the measures they take to protect their customers’ valuable personal information.

The research was launched at an event hosted by Australian Privacy Commissioner Timothy Pilgrim to business leaders, media and privacy experts. According to the Australian Privacy Commissioner, data breaches most often occur due to poor or inadequate security measures.

The Commissioner goes on to say that with only five months to go until the changes to the Privacy Act take effect, businesses need to reinforce to their employees the company’s responsibility for protecting customer details and also ensure that their security technology is robust – a sentiment with which McAfee entirely concurs.

Trust around privacy has become such a key element in the customer service relationship, and there is a real competitive advantage for businesses that take the lead in being transparent in how they handle and protect their customers’ personal information. Those that take consumer privacy seriously moving forward will also benefit by aligning their business processes to customer expectations around privacy.

There are five key steps Australian businesses can take to improve their management of customer privacy:

1. Develop and implement a comprehensive and easy to understand privacy policy and ensure strong policies for managing data
2. Perform a Privacy Impact Assessment (PIA) on how customer information is handled
3. Review technology controls to prevent data breaches
4. Thoroughly educate employees and create a culture of privacy protection
5. Create a dedicated privacy role within the company and review the amendments to the Privacy Act (found at oaic.gov.au) and determine the impact to the organisation

For more information on protecting customer privacy, visit mcafee.com.au/business.
Win a Cash Prize: iappANZ’s writing prize 2013

iappANZ is very excited to announce the launch of a new [$250 cash] writing prize for an article that is published in our monthly Bulletin between February and October 2013. 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 [kate.johnstone@suncorp.com.au or an iappANZ email] by 20 October 2013. 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, Kate Johnstone, Veronica Scott 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>
</table>
| **Wednesday 20 - Friday 22 November 2013**<br>Fairmont Resort, Blue Mountains | ARCA National Conference 2013  
the aim of the conference is to combine international best practice with local challenges and opportunities – in line with the principles of the ARCRC conference held in April 2011.<br>[http://www.arcaconference.com.au/ARCAC/index](http://www.arcaconference.com.au/ARCAC/index) |       |
| **Monday 25 November 2013**<br>All day event<br>Westin Hotel, 1 Martin Place<br>Sydney | iappANZ Privacy Summit<br>For more information on our World Class Speakers and networking event, and to catch the Early Bird prices, follow the link<br>[http://pams.com.au/iapp/StaticContent/Images/iappANZ_Summit2013_eflash.htm](http://pams.com.au/iapp/StaticContent/Images/iappANZ_Summit2013_eflash.htm) | Members $595<br>Non Members (including iappANZ membership) $756 |
| **Wednesday 12 February 2014**<br>OAIC<br>Room1 Level 3<br>175 Pitt Street (nr crnr King St)<br>Sydney | The Big Wrap up on the Privacy Act | TBC |
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.


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=112847&trk=anetsrch_name&qoback=.qdr_1281574752237_3

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

Platinum Sponsors

Commonwealth Bank
McAfee

Gold Sponsors

AvePoint
Facebook
Google

Silver Sponsors

eBay
Gilbert Tobin
Microsoft
Palantir
ShredX

LAWYERS
International Association of Privacy Professionals - Australia/New Zealand Chapter Inc.
Registered Association No. A0371238