Many exciting initiatives have happened this year as iappANZ grows. Indeed, since 1 January 2012, member numbers have increased over 20%. iappANZ has held a number of events to date, including with Kaliya Hamlin, known as the “identity woman”, on user centric identity and data sharing in the digital age in March, and recently events in Melbourne, Sydney and Brisbane during Privacy Awareness Week (PAW). Highlights of PAW are outlined in this Member Bulletin.

It was during PAW, that Nicola Roxon, Australian Attorney-General announced, in addition to the introduction of the Australian Privacy Principles and positive credit reporting, changes to the Privacy Commissioner’s powers would be introduced in the Winter sittings of Parliament. On 23 May, these changes were introduced before Parliament. New Zealand already has positive credit reporting provisions in effect from 1 April 2012.

Privacy is gaining wider appreciation and observation in the community. Just over a week ago, the Sydney Writers’ Festival (SWF) presented multiple talks on privacy – with the theme for SWF being “on the focus on the line between the public and private. The question of the limits of what is personal is one of the hottest subjects around”: Chip Rolley, Artistic director SWF.

As guests of IAPP, Judith Cantor, iappANZ’s General Manager and I attended the IAPP Global Privacy Summit and met with key staff at IAPP Headquarters in the United States in March. Whilst iappANZ operates independently, it is affiliated with IAPP. As a result of discussions, iappANZ members will see increased benefits, including the ability to access not only the members-only area of iappANZ’s website, but also the members-only area of IAPP’s website, including the Knowledge Centre containing data privacy resources. Information about how to access this will be sent shortly to members.

You may have also noticed that it is now easier to obtain privacy certifications, with online testing available in testing centres located throughout Australia and New Zealand. Information about certification can be found at the end of this Member Bulletin.

Coming up, we have a couple of events slated for July and September, with our annual Privacy Summit set in Sydney on 23 November 2012. We will have a practical and engaging day of speakers, so make sure you save the date. Should you wish to sponsor the conference, or otherwise be involved, please contact Judith Cantor, iappANZ’s General Manager on Judith.Cantor@iappanz.org.

Annelies Moens
President, iappANZ
CIPP/IT
annelies@iappanz.org
May has been a sparkling month for Privacy in Australia. Privacy Awareness Week (PAW) ran from 30 April - 4 May and iappANZ was proud to present events in Brisbane at Corrs Chambers Westgarth as well as at Norton Rose in Sydney and Melbourne with McAfee, iappANZ’s principal sponsor. Highlights of the events are covered inside this Bulletin. To celebrate PAW, iappANZ jointly with Information Integrity Solutions P/L, iappANZ’s consulting partner, released a global update on changes that have happened in the last 18 months in privacy from a regulatory and technology point of view. It is accessible on iappANZ’s website at: www.iappanz.org/images/stories/2012_PAW_IIS_and_iappANZ_Background_Paper_v2.pdf


It is great news that 4 years after the Australia Law Reform Commission’s most comprehensive Report on Privacy in 2008, that the reform is beginning. The Government introduced legislation to reform the Privacy Act on 23 May including a unified set of Privacy principles, updated credit reporting arrangements and enhanced powers for the Australian Privacy Commissioner. The ability of the Commissioner to seek civil penalties for privacy breaches where they are serious or repeated reflects the growing public desire to see individual’s private data treated appropriately by private and public entities.

In this month’s Bulletin you can read our Editorial about the proposed amendments to the Privacy Act and the likely effects for Australian consumers interacting with offshore sites, in terms of enforcing their privacy rights in this jurisdiction.

Planning for the iappANZ Privacy Summit in Sydney is underway, so make sure you keep 23 November 2012 free.

Warm Regards
Emma Hossack
Vice President

The eXtra-territorial factor

Imagine this … you are a website user accessing an Internet site from your living room in Bondi. You’re looking for a random shopping site that sells customised beach towels and you find a great US website that is offering big discounts on bulk purchases … just what you had in mind for this year’s Christmas gifts. You make a purchase, providing your name, address, email address, credit card information and expressly opt-out of receiving any future marketing communications from the website operator or any third parties associated with the operator. You’ve been down that road before and simply wish to confirm the purchase with no strings attached.

Your towels arrive and you are impressed with the quality of the product and the speed of delivery … Aunty Sue is going to love the caricature of her on a camel in the desert. The following week you start receiving emails from various marketing offshore outlets promoting various services and products … the senders are unknown to you but you suspect they have received your personal information as a result of your recent purchase. So, what? Do you have privacy rights against the website operator of the original site with which you transacted?
The extra-territorial reach of the Privacy Act 1988 (Cth) (Privacy Act) is regulated in section 5B. This section extends the application of the Privacy Act to acts done, or practices engaged in, outside Australia, by an organisation provided that certain requirements are met. Those requirements are as follows.

- **The legality of the Act or practice** under the law of the country in which it took place ("The Act or practice overseas will not breach a National Privacy Principle or approved privacy code or be an interference with the privacy of an individual if the act or practice is required by an applicable foreign law.").

- **The nature of the data subject** (The Privacy Act only has extraterritorial effect where the act or practice relates to personal information about an Australian citizen or another person whose continued presence in Australia is not subject to a limitation as to time imposed by law (section 5B(1)(a))).

- **The nature of the organisation transferring the data.**

Where a dispute comes before the Privacy Commissioner, this section determines jurisdiction.

The requirement as to the nature of the organisation transferring the data is met where, among other things, the following two conditions are satisfied.

- The organisation **carries on business in Australia** (s5B(3)(b)).
- The personal information was **collected or held** by the organisation in Australia or an external Territory, either before or at the time of the act or practice (s5B(3)(c)).

**Meaning of “carries on business in Australia” and “collected or held”**

There are no legal precedents as to the meaning of the phrase "carries on business in Australia" in the context of privacy law. However, the Privacy Commissioner’s website on Frequently Asked Questions seems to indicate that section 5B has a narrow application:

“If the social networking site is based in another country, then there may be no privacy rights under Australian law.”

There are some analogous uses of the phrase “carries on business” in the Corporations Act 2001 (Cth) and Competition and Consumer Act 2010 (Cth). Without doing a comparative analysis, the phrase can have a wide or a narrow meaning depending on how much emphasis is given by the interpreter to the connecting factors between the organisation and Australia.

Personal information can presumably be regarded as being ‘held’ at the location at which it is physically stored (e.g. where a foreign corporation stores information on a server in Australia). The meaning of ‘held’ can potentially be extended to the place a particular organisation has its main place of business even if the information is not physically stored there. Focusing on the location of a server is difficult because content is easily moved from one server to another and servers may be moveable and organisations may be tempted to choose to store information on servers in so-called ‘data-havens’. Further, there is the classic dilemma of where Internet communications ‘take place’ i.e. does a website visitor ‘go’ to the server hosting the website, or does the operator of the website ‘go’ to the website visitor?

According to a Fact Sheet issued by the Attorney-General’s Department in the context of the Privacy Amendment (Private Sector) Bill 2000, in order to regulate the behaviour of foreign organisations operating outside Australia, it is necessary to establish a strong link with Australian jurisdiction. In the Bill, the foreign organisation must carry on business in Australia and deal with information about Australians. The information must have been collected or held at some time in Australia.
In short, whether or not an offshore operator is likely to meet the extraterritorial criteria will largely depend on the underlying policy considerations for characterising the purpose of that section of the Privacy Act.

Policy Considerations ii

Should it be preferable to give the Privacy Act a wide extraterritorial scope, we may conclude that an organisation is carrying on business in Australia whenever it interacts with an Australian citizen or another person whose continued presence in Australia is not subject to a limitation as to time imposed by law. So, back to the customised towel saga, the fact that you accessed the offshore site and transacted with that site would constitute a sufficient link.

The problem with a wide interpretation is that where external applicability cannot be backed up by effective enforcement, the making of the extraterritorial claims may have a negative effect. It might contribute to a situation where the server hosting the particular website can decide whether or not to grant a particular visitor access to their website based on their location, so that visitors in countries with strict privacy regulatory regimes may be excluded.

Arguably, evidence of a narrow policy view can be seen in a recent own motion investigation by the Australian Privacy Commissioner into acts done by Reverse Australia under section 40(2) Privacy Act. Reverse Australia operates a reverse phone look up directory. The focus here was to establish whether Reverse Australia fell under the Privacy Act’s jurisdiction. A letter from the Office of the Australian Privacy Commissioner to the organisation was posted on its website. The key take-outs are as follows:

- The Privacy Act has limited extraterritorial application. An organisation is required to comply with the Privacy Act if it has an organisational link with Australia or the personal information is collected, used, stored and disclosed in Australia.

- Relevant factors include that the organisation in question carries on business in Australia or an external Territory, and the degree of control that overseas organisation is entitled to exercise, and does exercise, over the running of the business conducted by any subsidiary or representative in Australia.

- Reverse Australia was not found to carry on business in Australia as it does not have any physical presence in Australia, and its employees and infrastructure reside in the US. It does not conduct any functions or activities in Australia and therefore does not meet the requirements under section 5B.

On this reading, section 5B has limited application and information is collected in Australia only where the data collector is located in Australia at the time of collection, and that information is held in Australia only where it is physically stored in Australia.

Proposed Reforms

In April 2011, the Senate Environment and Communications References Committee published a report with recommendations titled “The adequacy of protections for Australians online. This report arose from a specific enquiry referred by the Senate regarding online privacy protections (separate but related to the Exposure Drafts on Privacy Amendment Legislation). The Office of the Australian Information Commissioner made a submission to the Committee enquiry that there is uncertainty as to how section 5B operates with respect to personal information submitted over the internet by an individual in Australia to an organisation based overseas and suggested that the requirement for information to have been collected in Australia is ambiguous because in a situation where an Australian submits information to an organisation based overseas, it is unclear whether the overseas organisation has collected information at the point of upload (i.e. Australia), or wherever the recipient organisation is based.
The Committee recommended that item 19(3)(g)(ii) of the exposure draft of amendments to the Privacy Act be amended to provide that an organisation has an Australian link if it collects information from Australia, thereby ensuring that information collected from Australia in the online context is protected by the Privacy Act. The policy intent here appears to favour a wide interpretation.

In May 2012, the Government published its response to the Senate Finance and Public Administration Legislation Committee Reports on the Exposure Drafts of Australian Privacy Amendment Legislation. A similar theme emerged to the April 2011 report (see above) calling for more clarity on the extra-territorial reach of the Privacy Act. Recommendation 19 in Part 1 of the report recommends that section 19, relating to the extraterritorial application of the Privacy Act, be reconsidered to provide clarity as to the policy intent of the provision. This is accepted in principle and the Government will develop appropriate amendments to the draft legislation to provide clarity as to the operation of proposed section 19 (extraterritorial operation).

So, there are some indications that the Australian Privacy Commissioner and the Government is favouring a more flexible approach when dealing with offshore operators. This combined with other proposed reforms to allow the Australian Privacy Commissioner to accept written undertakings from an organisation that they will take or refrain from a specified action which will be enforceable in the Courts; and make a determination following an own motion investigation as well as seek civil penalties in the case of serious or repeated interferences with privacy – may mean that the question of extraterritorial enforcement could gain more weight in the future.

This article is written by Anna Kuperman, iappANZ Board Director.

Postscript

Since this article was written, the Government introduced the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 into the House of Representatives on 23 May 2012. The Bill had a first reading (http://aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r4813). The Explanatory Memorandum states that in relation to Section 5B(3), there will be a reference to the new term ‘Australian link’ to clarify that the subsection lists additional connections with Australia which would be a sufficient link for the Privacy Act to operate extra-territorially in relation to organisations and small business operators.

The collection of personal information ‘in Australia’ under paragraph 5B(3)(c) includes the collection of personal information from an individual who is physically within the borders of Australia or an external territory, by an overseas entity. The Explanatory Memorandum states at Item 6 in Schedule 4 that: “For example, a collection is taken to have occurred ‘in Australia’ where an individual is physically located in Australia or an external Territory, and information is collected from that individual via a website, and the website is hosted outside of Australia, and owned by a foreign company that is based outside of Australia and that is not incorporated in Australia. It is intended that, for the operation of paragraphs 5B(3)(b) and (c) of the Privacy Act, entities such as those described above who have an online presence (but no physical presence in Australia), and collect personal information from people who are physically in Australia, carry on a ‘business in Australia or an external Territory’.
After six long years and much waiting, we have finally rounded the final stages of the review of the Privacy Act with the Attorney General, Nicola Roxon, tabling the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (the Bill) into the House of Representatives on Wednesday 23 May.

The legislation represents the most significant overhaul of privacy legislation since the introduction of the National Privacy Principles in 2001.

As many of the readers of this Member Bulletin will be aware the main elements of the Bill are:

a) The introduction of Australian Privacy Principles which will unite the National Privacy Principles (private sector) and the Information Privacy Principles (public sector)
b) Major reform of the credit reporting provisions
c) Provision of additional powers to the Office of the Australian Information Commissioner including the ability to apply to court for civil penalties and apply sanctions for issues found as part of an own motion investigation
d) New provisions for privacy codes and credit reporting codes

Since its introduction to parliament the Bill has been referred to the Standing Committee on Social Policy and Legislative Affairs which has been instructed to examine:

a) The adequacy of the proposed Australian Privacy Principles
b) The efficacy of the proposed measures relating to credit reporting
c) Whether defences to contraventions should extend to inadvertent disclosures where systems incorporate appropriate protections
d) Whether provisions in relation to the use of depersonalised data are appropriate.

What this means is that we still have a little way to go before we can expect the legislation to be passed and even then entities will have nine months to ready themselves to comply with the new requirements before the law takes effect.

The Bill introduces a very significant number of changes. Whilst its not possible to capture all the changes here a brief summary of the some of the key changes in relation to the Australian Privacy Principles and the Powers of the Australian Privacy Commissioner are included here. We are sure that more detailed articles will be available on other key aspects of the Privacy Amendment Bill in subsequent Member Bulletins.

Changes to the Australian Privacy Principles

At the end of this review process Australia will have 13 Australian Privacy Principles.

Importantly the first privacy principle deals with openness and transparency and is designed to prompt organisations and entities alike to consider the personal information cycle of collection, notification, use, disclosure, security and destruction before setting about collecting information.

There are also additional Privacy Principles that have never existed before including two that contemplate what entities should do when dealing with solicited and unsolicited information.
There is also an additional Privacy Principle dealing with Direct Marketing. Direct marketing is marketing that relies on personal information and is channel agnostic. It allows more relevant advertising to reach audiences that are the most likely to be interested and prevents the wastage of ill-directed advertising to uninterested audiences. The Bill has laid out the privacy framework around Direct Marketing including differentiating between the different consumer protection regimes that apply dependent on whether an organisation has obtained information about an individual from an individual or from another source.

There are many new provisions that recognise the transnational nature of data, especially in the online world. Consistent with one of the fundamental elements of privacy, entities will be required to include in their notice to individuals and their privacy policies information about whether the entity discloses personal information to overseas recipients and the countries to which that the personal information will be disclosed.

There have also been significant changes to the provisions that apply to the transfer of information overseas. National Privacy Principle 9 has been reshaped to only apply to cross-border disclosure of personal information rather than situations where information is transferred overseas but still remains under the control of the same entity.

The new regime will place a strict liability on an organisation for the actions of an overseas recipient if that overseas recipient acts inconsistently with the Australian privacy regime.

**Powers of the Australian Privacy Commissioner**

The Australian Privacy Commissioner will be able to make determinations to direct organisations to take specific actions. In addition, the Commissioner will also be able to obtain enforceable undertakings from an organisation.

The amended Act will also allow the Australian Privacy Commissioner to apply to a court for civil penalties against an organisation where serious and repeated breaches have occurred. The civil penalties that may apply are $220,000 per contravention for an individual and $1.1m per contravention for organisations.

The Privacy Commissioner will also be given the power to direct agencies to perform a Privacy Impact Assessment. The Australian Privacy Commissioner will also be able to conduct a Privacy Performance Assessment.

*This article is written by Melina Rohan, iappANZ Board Director.*

### iappANZ PAW Highlights

During Privacy Awareness Week 2012, iappANZ held three free member seminars: in Brisbane (held jointly with Corrs Chamber Westgarth), Melbourne and Sydney (both held jointly with Norton Rose and McAfee). The Melbourne and Sydney events were well attended with around 40 guests each, and participants heard from privacy luminaries such as Australian Privacy Commissioner Timothy Pilgrim, former Australian Privacy Commissioner and iappANZ board member Malcolm Crompton, Victorian Privacy Commissioner Dr Anthony Bendall, iappANZ president Annelies Moens, and McAfee’s Dr Ratinder Paul Singh Ahuja. We received favourable coverage of the Sydney event from ZDNet: [http://bit.ly/J1Lzkl](http://bit.ly/J1Lzkl)
Brisbane Event
As part of Privacy Awareness Week earlier this month, iappANZ and Corrs Chambers Westgarth co-hosted a breakfast briefing to discuss ‘Privacy in the Private Sector’. Felicity Cooper, Executive Director of IT Risk and Assurance at Ernst & Young, led the briefing with a presentation which examined the methods organisations can implement to address the management and control of information and data, and measures organisations can take to prevent data loss. A key message from Felicity’s presentation was that although many organisations have developed procedures for handling data, it is also important that organisations implement effective data loss prevention programs and tools, and train their people to be aware of and comply with them.

The briefing also included a panel discussion facilitated by MC and iappANZ Vice-President Emma Hossack, with panellists Helen Clarke (Technology & IP Partner at Corrs Chambers Westgarth), Adrian Panozzo (Executive Manager, Group Risk & Compliance at Suncorp) and James Kelaher (Director of SmartNet). The panel discussion focused on the legal and commercial issues faced by organisations if a data breach event occurs, and all panellists agreed that one of the key risks in this area (that is often underestimated) is the scope for reputational damage to the organisation. Helen Clarke also discussed the release of updated Data Breach Notification Guidelines by the Office of the Australian Information Commissioner during Privacy Awareness Week. While there are currently no data breach obligations under the Privacy Act 1988 (Cth), they are under consideration as part of the second phase of Australian privacy Reforms and the Guidelines represent a good indication of the type of regime that the Government may seek to introduce as a mandatory obligation under the Privacy Act in the future.

Helen Clarke also brought the group up-to-date with the latest developments in the Australian Privacy Law reforms. The panellists discussed the slow pace of the Privacy Law reforms, lamenting that it was not clear when the draft legislation and new Australian Privacy Principles which were released some time ago as exposure drafts, and which will amend the Privacy Act 1988 (Cth), would be introduced to Parliament.

However, a mere two days later there was a significant development with the Government announcing it would introduce this major legislative reform of the Privacy Act in this year’s winter sittings of Parliament. You can read more about these developments in the Corrs In Brief at (http://www.corrs.com.au/publications/corrs-in-brief/privacy-law-reform-gaining-momentum).

Helen Clarke, Partner and Melissa Burrill, Lawyer at Corrs Chambers Westgarth specialise in technology procurement and related privacy and data security issues.

Upcoming Privacy Events

Thursday, 19 July 2012, Sydney

iappANZ in conjunction with UNSW and Privacy Laws & Business is pleased to present “A comprehensive survey of privacy and data protection in the region”.

Data privacy legislation is accelerating in Asia, but the form it takes differs dramatically between countries. This day long seminar provides you with the updates on what's happening in China, South Korea, Taiwan, Japan, Hong Kong, SAR, Macau SR, India, Malaysia, Singapore, Vietnam, Thailand, the Phillipines and Indonesia. The proposed changes in the EU and USA and APEC cross-border privacy rules will also be discussed.

Join your fellow iappANZ members at a discounted rate to this event. Further information on registration will be made available soon.
In the interim, if you would like to express your interest to reserve a place, please email Judith Cantor, iappANZ's General Manager on judith.cantor@iappanz.org.

Save the Date
Annual Privacy Summit 23 NOVEMBER 2012 (SYDNEY)

ANNUAL PRIVACY SUMMIT
23 NOVEMBER 2012 SYDNEY
The SMC Conference & Function Centre

Missed the iappANZ 2011 Conference? - Speaker presentations online

For those of you who missed out on the 2011 Privacy Summit, we have made the presentations available for members, in the members-only section of the iappANZ website. Many member delegates who attended the Summit have also been keen to listen to the presentations again. Login to the members only area, and view the presentations under the 2011 Privacy Summit. You will find the password to access the presentations in the members only area.

Each Member Bulletin will highlight one of those speakers. This month we highlight Timothy Pilgrim, Australian Privacy Commissioner. **Topic: International Data Breaches - a perspective from the Office of the Australian Information Commissioner**

Timothy Pilgrim, Australian Privacy Commissioner made a compelling case that the take up of social media does not mean that privacy is dead citing the increasing media coverage of privacy issues, the recent settlement between Facebook and the Federal Trade Commission, increasing number of privacy complaints and growing awareness that the increasing amount of data being held can lead to data breaches. The Commissioner called for increased powers to give the Commissioner additional crediability pointing specifically to the limited powers the Commissioner has when conducting own motion investigations.

The Commissioner also foreshadowed an increased willingness to use existing powers noting that he was prepared to use all the powers available to his office including determinations. Finally Mr Pilgrim opined that any statutory cause of action should require the courts to take into account public interest matters including freedom of speech and that due consideration should be given to including a dispute resolution step that would be overseen by the Office of the Australian Information Commissioner to facilitate resolution of matters prior to full court proceedings needing to be commissioned by an individual. Timothy’s speech is available on the Commissioner’s website at: www.oaic.gov.au/news/speeches/timothy_pilgrim/timothy_pilgrim_iappANZ_summit_Nov_11.html
Privacy is a growing concern across organisations in the ANZ region and, increasingly, privacy-related roles are being made available only to those who can demonstrate expertise. Similar to certifications achieved by accountants and auditors, privacy certification provides you with internationally recognised evidence of your knowledge, and it may be the edge you need to secure meaningful work in your field.

The International Association of Privacy Professionals (IAPP) says:

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

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

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

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

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

What about testing?

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

iappANZ is happy to offer its members computer-based testing for all IAPP certification programs at ten venues across Australian and New Zealand via IAPP technology partner Kryterion.

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

FIND OUT MORE at:
Articles featured within this bulletin are not legal advice and are provided as general information and comment only, the authors do not accept responsibility. and the opinions are of the authors not that of iappANZ