In March the iappANZ has offered its membership some fascinating insights into the public, private and secret thresholds we all treasure with two free member events, namely:

- Kaliya Hamlin "The Identity Woman" in Sydney 22 March, and
- The international Law Firm Bird&Bird Webinar on the EU Data protection Regime on 28 March.

Members of the Executive and Board have been at the Global Privacy Summit in Washington where our Former and Founding President Malcolm Crompton was awarded the prestigious IAPP Privacy Leadership Award for his leadership in the field of privacy and ongoing promotion of privacy issues and the growth and visibility of the privacy profession. We are delighted that Malcolm has been recognised with this honour.

Privacy Week is in the first week of May, and we have 3 events scheduled, with more details coming. Hold these dates:

- Brisbane Tuesday 1 May “Doing Business in 2012 & Privacy” – Breakfast to be held at Corrs Chambers Westgarth;
- Melbourne Wednesday 2 May – Panel Discussions with Information Integrity Solutions, McAfee and the Australian Office of the Information Commissioner at Norton Rose; and
- Sydney Friday 4 May – Panel Discussions with Information Integrity Solutions, McAfee and the Australian Office of the Information Commissioner at Norton Rose.

This month our President, Annelies Moens provides us with a concise summary of the rapidly growing global data protection laws for the private sector, and our Secretary, David Templeton gives us a detailed description of the ePayments Code released by ASIC September 2011, along with other thought provoking articles on facial recognition and the new draft European data protection regulation.

Please also note that from 1 April 2012 the new Credit Reporting Privacy Code in New Zealand takes effect. For more information please visit: http://privacy.org.nz/credit-reporting-privacy-code/

Warm Regards
Emma Hossack
Vice President
iappANZ
Enactment of data protection laws affecting the private sector are accelerating at an ever increasing pace. In the 1970’s eight data protection law were enacted commencing with Sweden’s Data Act of 1973. In the 1980’s thirteen data protection laws were enacted, in the 1990’s twenty-one data protection laws were enacted, in 2000’s (till 2010) thirty-five data protection laws were enacted. In the current decade from the beginning of 2011 there have already been twelve data protection laws enacted. At this rate, by 2020 it is likely that every country in the world will have data protection laws in place.

A recent study by Professor Graham Greenleaf comprehensively puts together in one table the list of separate legal jurisdictions (generally countries) that have data protection laws in place that meet the following criteria, they:

- Cover most of the private sector;
- Include privacy principles meeting or exceeding the minimum standards of international data protection, based on the OECD guidelines; and
- Have methods of legislation-based enforcement (ie: not self-regulation).

The table can be found online at: [http://www2.austlii.edu.au/~graham/DP_Table/DP_TABLE.html](http://www2.austlii.edu.au/~graham/DP_Table/DP_TABLE.html). The countries listed in the table meeting the above criteria also have data protection laws for the public sector, except India, Malaysia and Vietnam which only have data protection laws in place for the private sector.

The most recent data protection laws to be enacted based on the above criteria are in Costa Rica, Trinidad & Tobago, St Lucia, Faroe Islands, Mexico, Peru, India, Malaysia, Vietnam, Ukraine, Gabon and Angola. The most economically significant countries that currently do not have data protection laws in place for the private sector (based on the above criteria) are the USA, China and Brazil, though a data protection Bill has been submitted for public comment in Brazil. It is also useful to note that the USA (at federal level) and Thailand have data protection laws in place for the public sector only, though a bill has been introduced into Parliament in Thailand to also cover the private sector. South Africa, Ghana, Kenya, Niger, Mali, Georgia, Cayman Islands and the Philippines have data protection bills before Parliament. Legislation is also expected in Singapore and Qatar.

All 27 member states of the European Union have data protection laws in place (based on the above criteria), along with all other European states, except Vatican, Georgia and Belarus. Israel was the first non-European state to enact data protection laws in 1981. New Zealand led the way in Asia Pacific in 1993 and Chile led the way in South America in 1999.

Currently, there are 89 countries with data protection laws in place for the private sector, with many more countries with pending legislation. With fewer than 200 countries in the world, it won’t be long before data protection is completely globalised. As remaining countries enact data protection laws, existing data protection laws are being reviewed.


Whilst the current data protection framework in the European Union remains sound, according to the Explanatory Memorandum (page 2), “it has not prevented fragmentation in the way personal data protection is implemented across the Union, legal uncertainty and a widespread public perception that there are significant risks associated notably with online activity”.

Data protection for the private sector accelerates globally
The changes, if enacted, will have significant impact on global companies, notably the power of data protection authorities to impose fines of up to 2% of a company’s annual worldwide turnover (i.e., revenue) or fixed fines [see proposed Article 79]. Such developments, suggest that not only will data protection laws around the world be further accelerated, but will become core business issues at the most senior levels of business operations.

By Annelies Moens, President iappANZ
annelies@iappanz.org

This article is largely based on research conducted by Professor Graham Greenleaf, University of New South Wales on data protection laws around the world, and a lengthy version of an article published by Professor Graham Greenleaf in Privacy Laws & Business in September 2011, entitled “76 global data privacy laws” and a follow up paper in Privacy Laws & Business entitled, “Global Data Privacy Laws: 89 Countries and Accelerating”, Issue 115, Special Supplement, February 2012 also available for free access at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000034

Note: At the time this article went to press - the Philippines Senate passed the Data Privacy Act, thus adding another country with data protection laws in place.

An Overview of the Draft European Commission Data Protection Regulation & the Implications for Australian Businesses

Introduction

On 25 January 2012, after the completion of a review process lasting more than 2 years, the European Commission (the Commission) published its proposal for a new regulation (the Draft Regulation) on the protection of individuals in the processing of personal data and free movement of same.

The Draft Regulation will inevitably be amended during the forthcoming legislative process and is likely to become law within 2-3 years. The following provides an overview of the measures currently proposed by the Commission and some insight into the potential implications for Australian based companies, including the current proposal to allow national Data Protection Agencies (DPAs) the power to directly impose sanctions up to a maximum of 2% of a company’s annual worldwide turnover. Given the relevance of data protection of recent times, the article also includes some practical steps on how companies can update their business practices more generally to keep up with shifting expectations relating to data security.

Harmonisation of EU Data Protection Frameworks

The Draft Regulation aims to harmonise the 27 data protection regimes in operation across the European Union since the current regime known as the Data Protection Directive (DPD) came into effect in 1995. The Commission hopes that the announced proposal will be the first step in adopting a uniform approach to data protection across European Union (EU) member states, and provide greater legal certainty for EU and non-EU member states alike.

The Draft Regulation introduces a “consistency mechanism” which seeks to ensure a high level of cooperation among the DPAs, the Commission and a newly formed body known as the European Data Protection Board (EDB). The main features of the consistency mechanism are:
ensuring the consistency of national measures across EU states;
• increased cooperation among DPAs. If several DPAs operate in a Member State (as is the case in Germany), a single DPA must be designated as a “contact point”; and
• a "one-stop shop" approach where data processing takes place in several EU jurisdictions. This would require the DPA in the relevant EU Member State where the controller or processor is located to oversee processing (identifying where the relevant controller or processor is located will be determined objectively according to where an entity’s main administrative functions are located).

**Scope of Application**

While considerable uncertainty prevails as to the extraterritorial application of the DPD, the Draft Regulation clarifies that non-EU based service providers will be required to comply with EU data protection standards if they market their services to EU customers.

Article 3(2) of the Draft Regulation states that the processing of personal data of EU data subjects by a service provider not established in the EU will be subject to EU law where the processing activities are related to:

• the offering of goods or services in the EU; or
• the monitoring of behaviour of data subjects in the EU.

**International Data Transfers**

The Draft Regulation proposes a more flexible regime for international data transfers. International data transfers would be permitted on the following grounds:

• binding corporate rules (BCRs) approved by a DPA (automatically accepted across the entire EU);
• standard contractual clauses approved by the Commission for transfers to non-EU countries (i.e., the Model Clauses);
• data protection clauses adopted by a DPA in accordance with the consistency mechanism;
• on the basis of one of the derogations contained in Article 44 (this includes exceptions such as data transfers required and necessary for the protection of important grounds of public interest i.e. between competition authorities, tax or social security administration); or
• an "adequacy decision" under Article 41 where the Commission will assess the level of protection based on an assessment of the rule of law, judicial redress and independent supervision.

Further flexibility can be seen by the fact that the Draft Regulation contains a new derogation (not contained in the DPD) for the transfer of data to recipients outside the EU on the basis of a "legitimate interest" of the data controller or processor, as long as the transfer is not "frequent" or "massive".

**Compliance Implications**

The Draft Regulation has been hailed by the Commission as a means of “cutting red tape” and creating “a more business-friendly regulatory environment”. While this is true in respect of adopting a uniform regulatory framework across the EU community, some of the provisions proposed are, in fact, more prescriptive.

The Draft Regulation will apply to “data controllers” (the people or bodies that collect and manage personal data) as well as “data processors” (the people or bodies who process personal data on behalf of the controller). Both are subject to EU law when handling data.

The following is an overview of the compliance implications of the Draft Regulation for business:
• **Removal of general notification obligation** - The general requirement to notify (GRTN) processing operations to the relevant DPA under Articles 18(1) and 19 of the DPD (which has been widely criticised as an unnecessary administrative burden) is proposed to be abolished under the Draft Regulation. It will be replaced by a "prior consultation" and/or "prior authorisation" system. This would operate in a situation where a privacy impact assessment indicates that the processing operations are high risk, or if a DPA determines a consultation is necessary. Authorisation would also be required where non-model contractual clauses are adopted for a transfer.

• **Express obligations for data controllers** - The Draft Regulation is much more prescriptive in comparison to the DPD for data controllers. Under the Draft Regulation data controllers are required to:
  - maintain documentation regarding data processing;
  - implement specific data security requirements;
  - perform data protection impact assessments;
  - seek prior authorisations and/or prior consultations for certain processing activities;
  - designate a data protection officer (DPO) (a DPO must be appointed in public bodies, in large private enterprises with more than 250 employees and where the core activities of the data controller or the processor consist of processing operations which, by virtue of their nature, scope and/or purposes, require regular and systematic monitoring of data subjects); and
  - notify personal data breaches to the national DPA (in certain instances, the data subject must also be notified).

• **Express obligations for processors** - Article 26 of the Draft Regulation sets out requirements for controller-processor contracts. Article 26 states that a processor must:
  - ensure staff are either under a statutory obligation of confidentiality or are otherwise committed to maintaining confidentiality;
  - only employ a sub-processor with the prior permission of the data controller;
  - ensure security measures are implemented;
  - maintain documentation of all processing operations; and
  - assist with the fulfilment of data controller obligations (such as notification of breaches, carrying out risk assessments, seeking prior authorisations and consultations).

**Strengthening Individuals Rights**

There is a strong emphasis on enhanced individual protection, control and transparency in respect of data use, storage and deletion.

• **Elements of transparency** - Article 11 of the Draft Regulation requires that the data controller must have transparent and easily accessible policies. Data controllers must use plain language that is adapted to the data subjects level of comprehension (for instance a child under the age of 18).

• **Elements of control** – the Draft regulation sets out a number of provisions for users to consent to the use of their data, where consent is defined as "explicit" control. For example, in order for a user to give consent he or she must "have awareness as to what he or she gives consent." In addition Article 7 states that consent does not provide a legal basis for processing where a significant power imbalance exists between the data subject and the data controller (such as in the public or employment sector).

• **Right to be forgotten and obtain erasure** - Article 17 sets out a particular provision for a data subject to request the data controller to erase personal data relating to him or her and abstain from further dissemination. The data subject would also have the right to obtain a copy of any data used that is personal
to them from the data controller. Finally, the data subject would have the right to transmit his or her data from one application such as a social network to another (data portability).

Sanctions and Enforcement

Under the Draft Regulations each DPA should have the power to sanction administrative offences, with a purpose to be "effective, proportionate and dissuasive." The risks of non-compliance under the Draft Regulation are substantially greater than under the current legal framework. The current proposal is to allow national DPAs the power to directly impose administrative sanctions, and where the most serious breaches could have a fine imposed of up to 2% of a company's annual turnover worldwide.

Conclusion

The Draft Regulation will likely come into force in 2-3 three years time and although the final form is likely to change, some practical steps for businesses to consider and/or implement include:

- assess current mechanisms in place for validating transfers of data to countries outside the EU;
- establish to what extent your business relies on consent as a basis for processing;
- review data protection notices;
- review and revise controller-to-processor contracts;
- maintain a close eye on the legislative changes in Europe to ensure all business and legal frameworks are indentified and implemented on time;
- establish at senior levels a management team that is aware of and responsive to issues relating to data security;
- appointment of a data protection officer (independent, sufficiently resourced who reports directly to management);
- the need for a data protection audit to obtain a profile of where your business may be at 'risk' in relation to the handling of personal data; and
- education and training for all employees handling data.

The extent to which companies and organisations will need to have regard to the proposed changes will depend on whether they are established or operate in the EU or otherwise deal with EU based organisations from whom they receive data. For organisations operating in the EU, full compliance with all its implications will be required whilst for organisations external to the EU, the compliance requirements will be imposed by contract in controller-to-processor contractual arrangements. EU based organisations are likely to seek indemnities and/or uncapped or greater liability limitations for breaches that expose the controller to the fines noted above.

In conclusion, whilst the Draft Regulations would be beneficial to business and data subjects in terms of legal certainty, it comes at a cost. For example, while international data transfers would be more flexible, a mandatory requirement to seek authorisation for transfers of data requested by a non-EU country's court, tribunal or administrative authority would present a significant administrative burden for globally active businesses.

This paper was adapted from an article by Baker & McKenzie's London, Paris and German offices dated February 2012 which has been edited by Robert Walker and Laura Ballantyne-Brodie for the iappANZ. The original article was by Christoph Rittweger, Matthias Scholz, Christina Demetriades and Denise Lebeau-Marianna. If you would like a copy of the original article please contact Robert Walker at robert.walker@bakermckenzie.com.

© Baker & McKenzie 2012
I recently returned from the annual IAPP Global Privacy Summit in Washington DC and a visit to IAPP in Portsmouth to negotiate increased benefits for members of IAPPANZ and Australian and New Zealand members of IAPP (to be announced in upcoming communications to members).

The annual IAPP Global Privacy Summit is attracting an increasingly international audience, with 20% of its delegates now coming from outside of the USA. There were numerous presentations and workshops over three days, including diverse topics such as mobile phones and privacy, data breach, social media and privacy, facial recognition, cybercrime, cloud computing, information security and APEC cross-border privacy.

One largely unregulated application, but with the potential to substantially impact everyday lives, is facial recognition technology. Below I provide a perspective of a presentation at the IAPP Global Privacy Summit entitled, “Privacy Implications of Facial Recognition, Facial Detection and Digital Signage’ and accompanying paper prepared by the Center for Democracy & Technology in Washington DC, also available online.

Facial recognition technology has the potential for a myriad of uses. Some apparent uses today, include photo tagging on social networking sites, targeted advertisements in stores or public spaces, security and authentication. Mobile phones and other handheld devices are ubiquitous platforms in which the technology is being deployed. Apple’s iOS 5, Windows Mango, and Google’s Android 4.0 mobile operating systems include face detection and recognition APIs. Facial recognition technology has the potential to significantly alter the ways in which individuals are marketed to, identified, tracked and assessed for health risks and emotions.

Facial recognition technology can enable government, business and individuals to collect – openly or in secret – and share the identities and associated personal information of any individual whose face is recognised. Unlike other tracking methods, such as GPS or RFID, facial recognition does not require the tracked individual to carry any special device or tag, thereby reducing an individual’s ability to prevent unwanted tracking. Some facial recognition systems can recognise individuals at a distance of 15- 20 meters and track an individual from a distance of 25-50 meters. Visual sensors can also estimate an individual’s emotional state by measuring minutely shifting facial features. MIT researchers indicate that the technology can also be used to measure heart rate, blood oxygen levels, and blood pressure – potentially exposing medical conditions of individuals.

Now that companies such as Facebook, Google, Apple, Polar Rose, Riya, PhotoTagger and others enable the easy upload of photos, there is a prolific private and public data source of faces. These companies employ facial recognition technology and quite often by default. Polar Rose and Riya were purchased by Apple and Google, respectively, in 2010. Prior to this, both companies offered services akin to “visual search engines” whereby users could label photos of individuals or objects and then find other photos of the same individual or object – i.e., tagging a photo of an individual taken with a mobile phone and locating more photos of the individual on the Internet.

Facial recognition technology deployment is not limited to the online world, but increasingly, applications are found in the off-line world, for example digital signage advertising. The digital signage industry is building an offline version of the behavioural advertising that currently occurs online. Currently, a passerby’s gender and age can be determined to enable certain advertisements to be shown to that demographic, based on assumptions made by the advertiser. It is conceivable that in the not too distant future individuals could be identified.

Do you want to lead the life of a celebrity? Facial recognition technologies and the impact on everyday life and public spaces
In its accompanying paper, the Center for Democracy & Technology conceptualises facial recognition’s impact on privacy on three general levels:

- **Individual counting.** Individuals facial information is gathered on an aggregate basis and not used for tailoring advertisements or messages to the individuals. No information is retained. For example: facial detection systems that track gazes or record passerby’s demographics, but do not store facial images or contextualise ads. This is the least privacy-intrusive form of facial recognition.

- **Individual targeting.** Individuals facial information is collected on an aggregate basis and is used for tailoring contextual advertisements. No information is retained. For example: systems that record passerby’s demographics and contextualise ads accordingly.

- **Individual identification.** Individuals facial information is collected and may be used for tailoring advertisements or other messages to the individual. Facial information is linked to individual identity or property. For example: facial recognition systems that record the unique biometric data points of an individual’s face in order to pinpoint images of the individual on the web or log that individual’s physical location. This is the most privacy-intrusive form of facial recognition.

The question arises is there an expectation of privacy in relation to information voluntarily revealed in public places (in this case – faces)? Celebrities generally have less expectation of privacy, they are known faces. However, with the potential of facial recognition to identify a vast proportion of the population, does this mean the population can only expect the same level of privacy as a celebrity?

Many businesses are already mindful of privacy issues associated with facial recognition and have taken steps to reduce the impact the technology has on individuals’ privacy. Privacy considerations persuaded Google to withhold a facial recognition enhancement it had created for its Google Goggles mobile app. The Digital Signage Federation has Digital Signage Privacy Standards. Many digital signage companies use the less privacy-intrusive facial detection, rather than facial recognition. For example, Intel’s Anonymous Video Analytics (AVA) uses facial detection software to record the age and gender of passersby to contextualise advertising in real time based on those factors. The Digital Signage Privacy Standards, Intel’s AVA, and Google’s decision to require user approval for photo tags of the user are all examples of privacy being considered in early product development.

How companies handle facial recognition privacy issues today will affect the way the public, regulators, and advertisers perceive the businesses that use the technology, as well as the technology’s direction in the future. Privacy by Design is clearly needed with respect to facial recognition, and there is some cause for optimism insofar as prominent trade associations and companies proactively adopt privacy standards for facial recognition, doing so in the absence of serious public scandal or government pressure. In contrast, the major online behavioural advertising trade associations only issued self-regulatory guidelines under pressure from government regulators and after widespread public controversy over their business practices.

Most individuals in public spaces would expect that few businesses and passersby would recognise their face, fewer would affix a name to their face, and fewer still would be able to associate their face with internet behaviour, travel patterns, or other profiles. Will changing that with widespread deployment of facial recognition lead to lower expectations of privacy, as celebrities deal with on a day to day basis, or will individuals and businesses retain their current expectation that in a public space you can still be relatively anonymous?

By Annelies Moens, President iappANZ
annelies@iappanz.org
Aspects of this article have been extracted from a presentation and paper by the Center for Democracy & Technology based in Washington DC and which was presented at the IAPP Global Privacy Summit, 7-9 March 2012. The paper is available at: https://www.cdt.org/files/pdfs/Facial_Recognition_and_Privacy-Center_for_Democracy_and_Technology-January_2012.pdf


Much of the EFT Code is retained. Loss allocation is largely unchanged and the ePayments Code continues to regulate the issue of ATM receipts and statements of account on electronic payment facilities. Relief is given concerning some areas of the code for low value products, particularly gift cards.

As expected, the separate concept of stored value facilities disappears and the new code moves toward plain English, principles based wording. Subscription to the code continues to be voluntary and limited to consumer transactions, unless the subscriber wishes to apply it to business transactions. Intending subscribers should note that ASIC’s general power to modify the ePayments Code (following suitable consultation), and the absence of any mechanism to withdraw from the Code for subscribers who find such modifications unpalatable.

Subscribers to the existing EFT Code must re-subscribe to the ePayments Code, and those choosing to do so will need to be compliant by 20 March 2013. The ePayments Code must be reviewed again, 5 years after the last review. On this basis, it will be reviewed again after only two years of full operation.

The ePayments Code does make some changes. It will have a broader application than the EFT Code, and will be open to a wide range of subscribers including ATM operators, and several aspects of the ePayments Code are of interest to privacy professionals.

• Loss allocation

Loss allocation remains focussed on the authority of subscriber to debit a consumer’s account for a challenged transaction, rather than the payment of compensation, and it remains the case that unauthorised transactions caused or permitted through the negligence of other participants in the payment process cannot be debited to the consumer’s account.

The ePayments Code clarifies that a consumers’ use or security of information that the subscriber does not expressly require them to keep secret cannot be taken into account in determining whether the consumer contributed to a loss. This will include the number and expiry date of a credit or debit card.

Overall, consumers will be grateful that Australia has not adopted the New Zealand position, where a bank can resist liability for a fraudulent internet payment if the consumer used a device with outdated or insufficient security software. ¹

• Mistaken payments

---

¹ Source: IappANZ Member Bulletin 31 | March 2012
The ePayments Code takes a tentative step toward solving the difficult issue of mistaken electronic payments between ADIs. This has been problematic because Australia’s interbank electronic clearing system operates solely on account and BSB (Bank State Branch) numbers, rather than payee names.

When a payer mis-keys a payee’s BSB and account number in the course of an internet banking instruction, the funds go to an account whose holder is entirely unknown to the payee. To pursue a return of the funds, the payer is dependent on the payee’s bank either:

• agreeing to debit the payee, or
• disclosing the payee’s identity to enable the payer to take legal proceedings for recovery.

The privacy challenge for the payee’s bank lies in balancing its own potential liability to the payer, and its obligations to protect the payee’s rights to privacy, including their identity and contact details.

While there is a strong body of opinion that the payee’s bank can disclose the payee’s identity in order to sort out a mistaken payment claim (see Alan Tyree http://austlii.edu.au/~alan/mistaken-epayments-2.html#tyree03: mistak_inter_payment and the Financial Ombudsman Service’s Supplementary Bulletin), some financial institutions adopt a more conservative view and refuse disclosure of the payee’s identity. This requires mistaken consumers to take costly legal action against the payee’s bank simply to identify the party who received their money.

The ePayments Code provides a detailed mechanism to deal with the issue of mistake, placing the onus on the payer’s bank to resolve matters with the payee’s bank. EDR as between the consumer their account provider is the backstop.

In determining whether the payment was mistaken, the mechanism relies on the cooperation of the banks. While they will be subject to the scrutiny of the Financial Ombudsman’s service, the mechanism does not directly address the privacy issues confronting the payee’s bank.

In fairness, the most effective way to relieve a payee’s bank of any concern about providing the payee’s identity and contact details to a payer, short of fixing the clearing system, would most likely lie in legislation. ASIC states that it intends to monitor the operation of these provisions and it is likely that clear data both on their efficacy, and the scale of the issue, will accumulate over the near future. That may, of course, lead to revised measures.

- **Statements and receipts**

The ePayments Code preserves the requirements relating to receipts for higher value facilities but now imposes a positive obligation (clause 5.3) to ensure that paper receipts don’t include information that would increase the risk of unauthorised transactions.

- **Book up**

The practice of book up, whereby retailers supply goods on credit and take possession of the customer’s ATM card (and in many cases, their PINs) as security is addressed in the ePayments Code. Book up is practiced in regional and remote areas.

The ePayments Code requires subscribers to include prohibitions in merchant agreements on collecting consumer PINs.
The review outcomes represent adjustment and refinement of what has become an accepted norm for electronic payments in Australia. For those interested, a detailed explanation of the review findings and how they are addressed by the ePayments Code is set out in ASIC’s Report No 218, available at: http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/rep218.pdf/$file/rep218.pdf.

By David Templeton, Secretary, iappANZ

References


2012 IAPP Privacy Leadership Award – Malcolm Crompton

Washington, DC—March 8, 2012—Malcolm Crompton, managing director of Information Integrity Solutions Pty Ltd. and former privacy commissioner of Australia, received the International Association of Privacy Professionals’ (IAPP) 2012 Privacy Leadership Award for his significant achievements and forward thinking on the handling and governance of personal information. The award recognizes a leader in the field of privacy and data protection who demonstrates an ongoing commitment to furthering privacy policy, promoting recognition of privacy issues and advancing the growth and visibility of the privacy profession.

It is great to have an iappANZ Board member (and founding President) receive such recognition. Congratulations Malcolm.

Upcoming Events

• Privacy Awareness Week, 30 April – 5 May 2012 http://www.privacyawarenessweek.org/
iappANZ events as follows:
  • Brisbane: Tuesday, 1 May Doing Business in 2012 & Privacy, to be held at Corrs Chambers Westgarth
  • Melbourne: Wednesday, 2 May Panel discussion with Information Integrity Solutions, McAfee and the Office of the Australian Information Commissioner, to be held at Norton Rose
  • Sydney: Friday, 4 May Panel discussion with Information Integrity Solutions, McAfee and the Office of the Australian Information Commissioner, to be held at Norton Rose

• Identity Conference, Wellington, New Zealand 30 April-1 May 2012 www.identityconference.victoria.ac.nz
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 Brendon Lynch

Brendon Lynch, Chief Privacy Officer, Microsoft USA

Mr Lynch has responsibilities for all aspects of Microsoft Corporation’s privacy program, including privacy creation and implementation across the company, influencing the creation of privacy and data protection technologies for customers and overseeing communication and engagement with external stakeholders.

Topic: Looking into the Future – Trends and Implications of Data Privacy, Technology and Policy

IAPP Certification

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? Will I have to travel to Baltimore?

Although the IAPP website refers to US-based certification testing only, testing is available to iappANZ members locally, with details of testing dates and times made known via the iappANZ website and the Member Bulletin. Online testing will be available soon. Further information will be available in April.

FIND OUT MORE at www.iappANZ.org

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 opinions are of the authors not that of iappANZ.