Welcome to the first Member Bulletin of 2012. 2012 is expected to be a year of change in the privacy landscape as Parliament, in its autumn sittings, is scheduled to consider amendments to the Privacy Act. These changes include draft Australian Privacy Principals (merging the Information Privacy Principles and the National Privacy Principles) along with positive credit reporting provisions.

This had been foreshadowed by the then Minister of Privacy, Brendan O’Connor at iappANZ’s annual conference, held in Melbourne 2011. This year the Privacy Summit will be in Sydney on 23 November 2012 and will introduce practical privacy parallel sessions to compliment plenary keynote sessions, as a result of conference feedback.

Feedback responses indicated that more than half of the attendees at the 2011 Privacy Summit are keen to attend this highlight event in 2012.

This year, iappANZ’s new p/t General Manager, Judith Cantor will continue to ensure member benefits are delivered and grow the Association, thereby increasing the network of privacy professionals in the region who can share best practice privacy solutions and opportunities with each other.

As part of delivering valued educational and professional development opportunities to privacy professionals, iappANZ kicks off the year with an exciting opportunity for members to engage with Kaliya Hamlin – known as the “identity woman”, on user centric identity and data sharing in the digital age, on 22 March in Sydney. This half day interactive workshop valued at $150 will be free to members. Details will be on our website soon. We are also busy preparing for Privacy Awareness Week commencing on 29 April with events scheduled in major capital cities.

Annelies Moens
President, iappANZ
annelies@iappanz.org

As Annelies Moens, our new President outlined, delivering member benefits and growing the Association are key goals for 2012. We are working towards this through the voluntary efforts of our enthusiastic new and old Board Members, together with our p/t General Manager, Judith Cantor whom many of you met at our November 2011 Privacy Summit. We welcome new memberships and alliances, so please let Judith know if you have colleagues interested in joining the Association.
We were delighted to read your positive Summit feedback, suggested conference topics and have noted that in future you would also like:

- More advance notice of the Summit and the programme line up;
- Better registration processes;
- More case studies on the practical privacy issues which affect your organisations.

We agree with your comments which are being addressed and would be pleased if you could let either, Judith, our General Manager or any of our Board Members know if you have further ideas for topics or speakers you would like us to consider for the year ahead. Judith can be contacted on Judith.Cantor@iappanz.org

From this month onwards we are offering members links to the audio presentations from the 2011 Privacy Summit. These will be available on our website for those of you who were unable to attend, or for those of you who wish to replay some of the highlights.

We hope you enjoy this month’s edition of the Bulletin which provides a New Zealand perspective on the privacy approach to patient care. We also provide you with a summary on the status of the Personally Controlled Electronic Health Records Bill 2011 and the Personally Controlled Electronic Health Records (Consequential Amendments) Bill 2011 which has been the subject of an Inquiry this month by the Senate Standing Committee on Community Affairs Legislation Committee.

Warm Regards,

Emma Hossack
Vice President, iappANZ

Privacy and Personal Health Information – A perspective on Australia’s introduction of the Personally Controlled Health Record (“PCeHR”)

“I can confirm that the Government is not going to build a massive data repository. We don’t believe it would deliver any additional benefits to clinicians or patients – and it creates unnecessary risks.”
(Minister’s own bold type).


The benefits of eHealth have been articulated often both here in Australia and overseas.¹ In essence, the ageing population, the high incidence of chronic disease and the shrinking resources to respond to this challenge, mean that more effective and efficient methods of health care delivery are essential. The Federal Government has allocated $467M to the Project, which has a “Go Live” date of July 2012². Privacy issues arise


² Government sources have indicated that original 1 July timeframe may be extended to 31 July 2012.
wherever “big data” is collected, and particularly where personal health data is involved. Consequently there have been a number of privacy (and practical) concerns raised throughout the various consultation processes starting from the draft Concept of Operations for the Personally Controlled Electronic Health Record, through to the legislation which was read in Parliament last year and is currently the subject of a Senate Inquiry. The following is a commentary on some of the issues that have been raised in respect of the need for a PCeHR and the protection of patient privacy.

To fully appreciate the privacy issues, it is important to appreciate what a PCeHR is, or is likely to be. The most reliable place to find this is “The Con Ops” which is the diagrammatic representation of how the PCEHR should work and a copy of which appears below, see Figure 10. Health informaticians and experienced Architects have found this complex, but this is the layman’s version which is the basis for many of the specifications still subject to finalisation. There are of course many views on exactly what a PCeHR should be, and how it should be implemented.

Figure 10: PCEHR System components, Concept of Operations: Relating to the Introduction of a Personally Controlled Electronic Health Record System p.76.

---

3 http://en.wikipedia.org/wiki/Big_data
4 April 2011 see: www.health.gov.au
5 The Personally Controlled Electronic Health Records Bill 2011 and Personally Controlled Electronic Health Records (Consequential Amendments) Bill 2011 were introduced into Parliament on 23 November 2011.
6 On 25 November 2011 submissions were requested from any interested parties from Senate Community Affairs Committee with the first hearing on 6 February 2012 and possible reporting date of 29 February 2012 subject to Questions on Notice.
7 As at the time of writing 49 public submissions were loaded onto the to the Senate Standing Committee http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=clac_ctte/pers_cont_elect_health_rec_11/submissions.htm
9 Concept of Operations: Relating to the Introduction of a Personally Controlled Electronic Health Record System p.76 www.health.gov.au
Unfortunately these views remain polarised across the spectrum of stakeholders – often called “the Four Pillars” – namely Consumers, Clinicians and other health care providers, the Medical Software industry and the Government. This lack of cohesion can be expected in any massive IT project affecting personal data, but has not been aided by conflicting reports of apparently privacy positive statements by the then Health Minister on the one hand (above), and then inexplicably complicated architecture for the PCeHR on the other. In actual fact it now appears that a large National Repository is being built by the National Infrastructure Partner, and Clinicians will be actively encouraged – although not paid- to upload patient data onto this system. Protecting the privacy of individual’s personal health data, arguably their most personal information therefore becomes vitally important. Privacy and security are inextricably linked – privacy is the protection of data from computers and other unauthorised use and security is the protection of computers from people- suffice to say in this summary that the statements below are optimistic.10

“It if comprehensive security policies are in place no-one need ever fear that their individual health privacy will be compromised”
Dr Peter Weston, Director of Security &Privacy, European Commission, ICT for Health Unit, HINZ Conference NZ, November 2011

It is encouraging for privacy professionals to note that almost every one of the Submissions to the Senate Inquiry acknowledges the importance of improving the privacy protections in the legislation and operation of the PCeHR. The privacy implications of this legislation have been defended by the Hon Minister Roxon who said following the First reading that:
“Electronic Health Records….can make medical information much more secure and private….This system which we are building will note every time anyone – no matter who they are – has accessed a record”11

However, as anyone involved with electronic communication in the 21st Century is aware, individuals are subject to ‘electronic assault’ 12 and this electronic transmission also results in the possibility of data mining and matching and instantaneous publication of data to millions of people. This can destroy the privacy safeguards that silos inadvertently provide for privacy conscious patients. Put another way, “To err is human, to really stuff something up it takes a computer”.13

1. OPT IN - vs. - OPT Out
I have previously discussed the positives of Australia adopting a privacy by design approach of OPT IN versus OPT OUT14. This has not been universally accepted, and Doctors in particular naturally wish to have all available data to hand to enable them to provide the best care for their patients.

“Critical information needs to be available for treating doctors to make sure they bother becoming engaged. …” Dr Steve Hambleton, President AMA.
Dr. Steve Hambleton

10 The OAIC submission #41 to the Senate Inquiry makes useful comments on this see http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=clac_ctte/pers_cont_elect_health_rec_11/submissions.htm at p.13
13 Anon – Heard at a Conference and very happy to hear if anyone can give me the author reference. For examples of this see New York Times 30 May 2011 Report by Milt Freeman on improper exposure of 7.8 million people which in many cases was as a result of the records being in electronic format , but which in some instances also was the result of human error and misdemeanour. See also the US federal Gove “Wall of Shame” where significant breaches of medical privacy are listed: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html
14 See iappANZ Bulletin September 2011.
This viewpoint clearly has merit, but until the PCeHR is actually fully and finally specified, and well implemented and well understood OPT IN provides greater privacy protection.15

2. It is not prudent to attempt regulation of operation of a yet to be finalised Architecture16
Submissions to the Senate Committee by the Privacy Foundation, the Medical Software Industry of Australia, the Consumer eHealth Alliance, Dr David More and many others17 suggest that “the fog of confusion that constantly swirls around every facet of eHealth”18 may compromise the governance and privacy protection afforded by the legislation. The magnitude of the PCeHR Project was recognised by the Deloitte eHealth Strategy19 which stated that it would be a ten (10) year programme for Australia to implement its National Shared Electronic Health record at a cost of several billions of dollars. This Report was commissioned by and accepted by the Federal Government and endorsed by the National Health and Hospital Reform Commission. Nevertheless, the Government announced in November 2010, that every Australian could access a PCeHR by July 2012 and allocated not billions but $467M for its implementation.
This radically compressed timeframe has meant that the Department of Health and Ageing has been required to add to the number of legislative instruments in addition the Privacy Act 1988 (Cth). A number of concerns would have been addressed had the recommendations in the ALRC’s largest ever report, For Your Information in 2008, been implemented. The 1 July 2012 deadline has also led to a number of practical problems. For example, the week before the Senate Community Affairs Committee sat to hear from invited parties on submissions, 9 of the eHealth 12 waves were “paused”. This was due to the fact that they were working to different specifications from those of the National Infrastructure Partner, making an interoperable system unlikely, and raising the ever present concern that privacy and security could be compromised by errors in the design phase.20

3. System Operator
Pursuant to the Draft Bill, the System Operator is also the Secretary of Health and whilst the Bill provides for further regulations to be made, the conflict of interest in handling sensitive health information is obvious.21Whilst the Secretary would no doubt operate impeccably, the public perception could view the System Operator being in a conflicted position. The PCeHR should provide for the System Operator be subject to the Privacy Act.

4. Compulsory Breach Notification
Originally the Bill provided for discretionary breach notification, but now it is compulsory for the System Operator, portal operators and repository operators. This needs extension however to all entities which may access consumer’s health information.22

5. Governance of the PCeHR – The Rules
The Rules of operation have not yet been established, and are intended to be put in place in the future, likely to be after the “Go Live” date. This is not a privacy positive approach to ensuring minimum standards or rules for users of system.

6. Consequences of Privacy Breaches

15 Note contrary views: Consumer Health Forum of Australia submission #7 and AMA submission #43, link above fn.8. It is however pleasing to note that the revised Bill includes the role of educating the public as about the PCeHR as one of the System Operators roles.
16 https://vendors.nehta.gov.au/public/index.cfm?returnTo=%%2Findex.cfm, registration is required for this site by DoHA and NeHTA but it is open to the public to register.
17 See particularly Dr Ian Colclough #39 and others link above fn.8.
18 Ibid at p.2.
19 Ibid, fn1.
20 NeHTA presses pause on e-health records, Computerworld 24 January 2012
21 See for example Dr David More submission #21, MSIA #46, CeHA #37 and OAIC #41 link above fn.9
22 OAIC #41 at p. 2
The current Bill absolves Government from liability for adverse errors or privacy breaches. It has been suggested that Government and its agencies ought not to be exempt from liability when the System Operator will have such an extensive role in the operation of the system.

7. **Interplay between the Privacy Act and the PCeHR Bill**
   Clarity in respect of both pieces of legislation is required so that:
   - the Information Commissioner’s powers of investigation for breaches of the PCeHR are confirmed under the Privacy Act
   - it is clear when a breach under the PCeHR is to be treated as an interference with privacy under s.13 or s.13A
   - there is consistency of wording relating to interference of an individual’s privacy in both s.13 & s.13A of the Act and s. 73(a) of the PCeHR Bill.
   - The PceHR Bill allows investigative powers including own motion investigations
   - The PCeHR specifies the Privacy Act mechanisms appropriate for a breach of PCEHR.

8. **Data Security provisions**
   Data security provisions need to be listed for the System Operator, portal operator and repository operator in the PCeHR Bill.

9. **Civil Penalties need to be extended**
   Part 4 of the Bill provides for penalties where the information is extracted from the PCeHR but does not cover information which was originally extracted from the system, e.g. copied. Paper copies are uncontrolled.

10. **Appropriate Remedies**
    There needs to be consideration of appropriate remedies for breach of PCEHR rules and the proposed review under s.108 should include a review of the adequacy of the privacy protections under the legislation.23

It is clear that Australians are becoming increasingly aware of their privacy rights following a number of high profile breaches both here and overseas, and it is hoped that Australia establishes itself as a country which seeks to “preserve autonomy and dignity from the perceived threats of unconstrained market process.” 24 It is disappointing that the timetable surrounding the implementation of this eHealth Reform may result in shortcomings both from a functional and operational level and quite possibly in respect of the rigorous degree of privacy protection individuals rightly demand for their health information.

Emma Hossack  
iappANZ Vice President  
*Emma is also CEO of Extensia, a company linking healthcare providers, consumers and their communities to enable them to achieve more efficient and better health care. Extensia was established through the Commonwealth Research Centre Scheme to develop a Patient Centric Shared Electronic Health Record system and has continued its development meeting the specific requirements of clinicians and patients.*

---

23 OAIC #41, ibid at p.2
Online privacy is a topical news item at the moment. In reviewing the Australian Privacy Act the Australian Law Reform Commission noted that “Developments in technology have always influenced discussions about privacy and the formation of information privacy laws”.

Whilst we have an admittedly evolving legal definition of “personal information”, it has become obvious that the average person’s understanding of “privacy” is considerably broader than just protecting their ‘personal information’ from misuse. We therefore see a gap developing between the personal information that is afforded legal protection under the Privacy Act and all of the other information that some people think should also be treated as private. Privacy means different things to different people.

This predicament is particularly well observed in the context of online behavioural advertising (or OBA as it is sometimes referred). OBA, or interest based advertising, has attracted media attention in the form of headlines such as “Inside the Cookie Monster – trading your online data for profits” and “Browsers beware as political websites plant spy devices”. OBA works by gathering anonymous information about an Internet user’s web browsing activity in order to allocate interest categories to that anonymous user and serve advertisements to them based upon those interests. For example, imagine I am planning a trip to Bali in the next school holidays. I have been carrying out searches for accommodation, reviewing specific hotels on TripAdvisor® and checking on flights. Now, whenever I go onto my favourite news website I see ads for hotels in Bali instead of an ad for a car. In other words, I have been added to an interest category for people who are interested in travelling to Bali. I should stress that there could be 300 other Internet users who have also been placed into this interest category and my favourite news website cannot identify me as an individual, they just know that I am interested in Bali.

The Privacy Act does not regulate OBA because OBA does not involve the collection or use of personal information. The online advertising industry in Australia (much like in the US and Europe) has developed a self regulatory framework within which signatories agree to abide by certain principles if they are engaged in collecting or using OBA data.

One of these principles is that companies engaged in OBA must notify their users of their OBA practices. This is typically done through a privacy policy and there has been much debate around the effectiveness of these privacy policies. In 2006, the University of California Berkeley carried out a survey which found that only 1.4 per cent of users read these sorts of agreements “often and thoroughly”. Privacy policies tend to err on the side of being rather lengthy and often use legal terminology that can be alienating to the average web user. Given how important the concept of notice is, both within the Privacy Act and within the self regulatory framework for OBA, it is critical that companies find a way of notifying their users of their data collection practices in a manner which is intuitive and accessible. An example of a new form of privacy notice is a hyperlinked icon which is placed either in or around an ad unit which alerts the user that the ad in question has either been targeted to them based on their interests OR is collecting data for the purposes of serving an interest based ad to that user at a later time. The icon, when clicked, opens a box which provides information about the ad (who has served

---

it, who the advertiser is) and offers the user an opportunity to learn more about how OBA works. This form of notice is arguably much more contextual, direct and ‘in your face’ than a standard privacy policy. Time, and web analytics, will tell if engagement with these icons is higher than with a standard privacy policy and lessons will be learned around how best to present this important information to Internet users. In the meantime, we should encourage innovation and experimentation in this area as a means of raising the awareness of Internet users of new forms of data collection and use online.

Samantha York
iappANZ Board Member
Sam is a consumer digital media and technology lawyer and policy advisor with over thirteen years experience working in Europe and Asia Pacific. She advises on issues as diverse as the Internet and emerging technologies, consumer laws and regulations, policy development (privacy, safety, security), regulatory affairs and alternative dispute resolution.

Primary Care Centred Patient Records – A Privacy Focused Approach

The emergent NZ health IT strategy is to avoid centralising of electronic health records and to encourage information exchange. With a 20 year history of clinical data interchange, New Zealand's general practices are among the world's most advanced users of clinical IT. By eschewing large “ambitious” projects, focusing on incremental improvements and creating a learning environment they have, over time, created an environment in which they have unparalleled access to patient information while at the same time ensuring that privacy of patient information remains a paramount consideration.

History

New Zealand enjoys one of the world’s most advanced primary care information technology (IT) infrastructures. Key to achieving progress has been the careful attention paid to ensuring that privacy principles are observed at all times. New Zealand adopted a Health Information Privacy Code (HIPC) in 1993, the same year that electronic clinical communications services were launched.

In the early 1990s the New Zealand government launched a major reconfiguration of its public health services. A key focus of the reform was to enable the sector to take advantage of information technology to replace centuries old paper based processes. By implementing a British National Health Service styled ‘patient enrolment model’, linking each citizen to a particular general practitioner or practice, a logical point for aggregating patient data was established.

In order to support large scale information exchange a far-sighted Deputy Director-General of Health set in place a number of key infrastructure initiatives. Over a three year period Dr Judith Johnston successfully implemented the following:

- A National Health Information Privacy Code (HIPC), based upon the New Zealand Privacy Act
- A national healthcare identifier number system, the National Health Index (NHI),
- Adoption of the then little known HL7 standard (it is now one of the world’s most widely adopted standards)
- A process for accrediting IT companies to provide various services to the sector.

These measures ‘kick-started’ the formation of a viable healthcare IT industry and created an enduring partnership between government and private sector. Financial incentives were then given to medical practices to automate their electronic medical records systems and by 1998 (five years later) 100% of general practices had some form of electronic medical record system in place.

The Situation Today

The success of these early initiatives set the scene for a significant level of information exchange between healthcare providers. Exchange began with electronic delivery of laboratory results, then discharge summaries and referrals. All kinds of medical information began to be sent as structured messages between healthcare IT systems. Nearly two decades on, 50 million electronic clinical messages are exchanged annually and an average New Zealand general practice exchanges clinical information electronically with 58 other healthcare organisations in any given month.

New Zealand’s efforts to preserve a high level of trust in the integrity of the system have meant that that an ‘Opt Off’ approach has worked well. Patients are told very clearly that their health information will be utilised in a manner that their GP believes is in their best interests, but they can ask for this not to happen if they wish to; few if any do. All of the systems within the sector are designed to conform to the HIPC and there have been very few, if any, privacy related problems reported to date.

Until recently there has been no effort to encourage establishment of any form of patient record sharing framework across the New Zealand health sector. Instead we have relied upon the exchange of information on an ‘as needed’ basis. Clearly this approach has some limitations. But resisting the urge to share records has preserved patient confidence in the integrity of the system and its privacy, enabling the sector to continue moving steadily along its automation agenda, applying constant incremental improvement rather than trying to commission or build a national record sharing system.

Tentative Steps Towards Sharing of Patient Records

New Zealand has however built upon its information exchange systems and some systems currently being trialled now that do enable emergency departments and after-hours clinics to query general practice and pharmacy records online and in real time. These systems use the NHI to locate general practices and pharmacies where a patient has presented during the past year and with patient consent, a record from each of these systems is displayed on the emergency care clinician’s browser. This interchange takes place over a secure network.

These systems were first introduced in mid 2011 and their growth has been significant. Typical use cases are:

- A hospital accident and emergency department querying all of the medical centres and after-hours clinics in its region to obtain current information about a patient it is treating.
- A general practice querying local pharmacies to ascertain whether a patient has been dispensed the medicines that he or she has been prescribed.
- A local accident and emergency provider checking on GP records to see what medications a patient is using
- A surgeon on a hospital ward looking for more information about a patient’s medical history, immediately prior to an operation
Summary

The New Zealand health system has built a highly functional IT infrastructure via cautious incremental improvement developed over a number of years. From the very beginning, New Zealanders have recognised that maintaining patients’ trust is a very important ingredient in building a high performing health system. A key element of trust is effective management of health information privacy. We must ensure patients continue to trust the health system to keep their information private and simultaneously enable clinicians to use patients’ information to deliver high quality healthcare.

Tom Bowden is CEO of HealthLink Ltd, a Health Information Exchange service providing electronic services to 9,000 Australian and New Zealand healthcare organisations.

Identity and Privacy: A special iappANZ – Internet Identity Workshop, 22 March 2012 Sydney
The iappANZ is pleased to present “Identity Woman”, Kaliya Hamlin, from Canada and the United States to facilitate a dynamic, hands-on discussion of the interplay between privacy and digital identity, and the latest initiatives to improve safety online.

Kaliya’s visit to Australia is timely, as the Australian Government is renewing its strategic involvement in the identity marketplace by studying the concept of a National Trusted Identity Framework. While industry calls for the Commonwealth’s Document Verification Service (DVS) to be opened up, new Electronic Verification services have emerged to enable purely online bank account origination under recent financial transactions reporting law reforms. Debates rage about anonymity, the roles of new identity providers, social login versus traditional evidence-of-identity, smartcards versus smart phones.

About the event
A half day dynamic discussion of privacy and digital identity
The discussion will be self-organised around a number of topics suggested and distilled by the audience. Identity Woman (who has led hundreds of similar workshops) will facilitate the agenda setting. Bring along your questions, your issues and your fervent wishes for a better privacy and digital identity environment, and be prepared to contribute.

Registrations will be open soon at www.iappanz.org.

Price
iappANZ Members: FREE
Non-members: $150 (inclusive of GST)
Non-member group rates will also be available

About Identity Woman
Kaliya Hamlin, known as Identity Woman, co-founded the world’s leading industry forum focused on user-centric digital identity, the Internet Identity Workshop (IIW). Seeing the emerging possibility of individuals collecting, managing and gaining value from their personal data generated as they interact with all kinds of digital systems, she founded the Personal Data Ecosystem Consortium in 2010 to catalyze industry development and collaboration. She identifies as a nymwarrior because she was personally affected by Google’s insistence she use her “real name” as the headline on her profile. With others she fights for the right to have different, unlinked personae: different identifiers for different contexts online.
Kaliya advises the World Economic Forum's Rethinking Personal Data project. In 2010 she presented at the (US) National Strategy for Trusted Identities in Cyberspace Privacy Workshop. She sits on the OASIS IDTrust member steering committee and is active in the Federated Social Web which recently moved its work to the W3C.

**Preparation**

You are encouraged to submit topic suggestions ahead of the event. Please email Judith Cantor, iappANZ's General Manager on Judith.Cantor@iappanz.org

See also:

- [http://www.identitywoman.net](http://www.identitywoman.net)
- [http://www.internetidentityworkshop.com/about](http://www.internetidentityworkshop.com/about)

### Upcoming Events

- Global Privacy Summit, International Association of Privacy Professionals, Washington DC, 7-9 March 2012
  [www.privacyassociation.org/events_and_programs/global_privacy_summit](http://www.privacyassociation.org/events_and_programs/global_privacy_summit) (Please note iappANZ members can attend at IAPP member rates)
- Data Governance, Health Informatics Society of Australia, Melbourne, 29-30 March 2012
- Identity Conference, Wellington, New Zealand 30 April-1 May 2012
  [www.identityconference.victoria.ac.nz](http://www.identityconference.victoria.ac.nz)
- Privacy Awareness Week, 30 April – 5 May 2012
- Privacy Forum, Wellington, New Zealand, 2 May 2012

### 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 the Hon Michael Kirby.

### The Hon Michael Kirby AC CMG, Former Justice

The Hon Michael Kirby AC CMG was Australia’s longest serving judge when he retired from the High Court of Australia in 2009. He was first appointed in 1975 as a Deputy President of the Australian Conciliation & Arbitration Commission. Soon after, he was seconded as inaugural Chairman of the Australian Law Reform Commission (1975-84). Later, he was appointed a judge of the Federal Court of Australia, then President of the New South Wales Court of Appeal and, concurrently, President of the Court of Appeal of Solomon Islands. In later years, he was Acting Chief Justice of Australia twice. Following his judicial retirement, Michael Kirby was elected President of the Institute of Arbitrators & Mediators Australia from 2009-2010. He is a Board Member of the Australian Centre for International Commercial Arbitration, the Editor-in-Chief of The Laws of Australia, and a member of the Eminent Persons Group investigating the future of the Commonwealth of Nations. He has been appointed to the UNDP Global Commission of HIV and the Law and to the Australian Panel of the

**Topic: 30 Years of Privacy**

We were privileged to hear The Honourable Michael Kirby AC CMG make a compelling case for legislation to protect individuals from egregious interference in private matters by media, and how the concepts of publication and media must extend to search engine results.

---

**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