The concepts of security and privacy in health information systems are distinct but inextricably linked like Siamese twins. The distinction can be expressed as follows: security is the protection of computers from people, and privacy is the protection of people from computers. The maintenance of privacy and security are two of the goals of a health informatics system.1

This month we are delighted to have excellent pieces on the critical need for security where privacy is concerned. The quote above is relevant to all sensitive data, not just health data. The expectation of high levels of security from our financial institutions is now widely recognised as vital for our other data, and to ensure that businesses keep pace with the need to be ever more efficient and productive, the challenges of providing first class security are essential. The McKinsey Quarterly Review touches on this in its current edition, noting that cloud computing and data storage are innovation priorities and the corollary is investment in security to prevent privacy breaches which includes privacy professionals and elevating technology on the Boardroom Agenda.

Lemm Ex, Queensland’s Acting Queensland Privacy Commissioner provides us with a richly footnoted piece on the prospect of cloud services in Government. The statistics he quotes from a recent Ponemon Institute study in Australia highlight the fact that just as most of the privacy breaches in the “terrestrial” World come about through negligence or lack of process, we have the opportunity to put a framework in place to enable us to reap the benefits of cloud computing in the Cyber World. Data flow is the lifeblood of Government (and business) so privacy and security is seen as the way of appropriately enabling its release through cloud computing.

1 Robinson, 1994 in Hovenga E., Kidd M., Cesnick B., (Health Informatics: An Overview. Melbourne Australia, Churchill Livingstone p.77

Melanie Marks, iappANZ Board member looks at the privacy and security issues raised by events surrounding the tragic death of Jill Meagher. The benefits of social media and CCTV to enhance our physical security have a counterpoint – the possible breach of laws necessary for a fair trial and the blurring of the rules regarding personal surveillance cameras. Public education and guidelines are suggested to ensure the benefits of both technologies are harnessed without breaches to law and civil liberty.

On November 14 in Wellington, New Zealand we are pleased to hold iappANZ’s inaugural seminar in New Zealand, at which Mike Flahive, Assistant Commissioner (Investigations), Office of the Privacy Commissioner, New Zealand will present on the major data breach that rocked the Accident Compensation Corporation in New Zealand. Our President, Annelies Moens will be there to launch iappANZ’s inaugural seminar in New Zealand. More information is on our website and the Events section of this Member Bulletin.

This is the last edition of the Members Bulletin before what will be a sparkling Privacy Summit in Sydney 23 November. Take a moment to look at the line up inside the Bulletin, and if you haven’t already registered, there is time. On behalf of the Board, I look forward to warmly welcoming you and your guests to this stimulating event which aims to keep you as a privacy professional up to date and aware of how your colleagues are dealing with the current privacy challenges for business and government.

Warm Regards
Emma Hossack Vice President
Finding the Silver Lining: Moving Government to the Cloud

Introduction

What ever happened to the promise of the paperless office? In 1975, Businessweek confidently predicted that “the use of paper in business for records and correspondence should be declining by 1980 and by 1990, most record-handling will be electronic.”

In this modern age of digital marvels – when even the humblest of smartphones is a research library, a news studio, a business centre and a communications hub – we continue to drown in paper. The consumption of paper has grown 400% in the last 40 years and is expected to rise to 440 million tons by 2015. Despite paper being an environmental vandal, the paperless office - like the personal jetpack and the hoverboard - has yet to eventuate. However the twin impetuses of cloud computing and the rollout of improvements to broadband may bring us closer to that vision.

In an effort to realise greater efficiencies in the public sector, governments are looking at ICT resources, costs, and benefits and asking whether we can afford to sustain traditional models of ICT infrastructure.

The Queensland Government commenced an audit of its ICT systems in May and it has estimated that it would cost $5 billion dollars over the next three to five years to fix the Government’s 50 most vulnerable IT systems. Perhaps predictably, cloud services have been identified as part of the solution to consolidate redundant infrastructure and improve productivity.

The question is not, ‘are governments going to move to the cloud?’ but, ‘when, to what extent, and how will privacy fit within this brave new office?’

It is not the intention of this opinion piece to focus on the privacy risk potential of the cloud—that has been well done on many occasions before. Rather its purpose is to explore the issue of whether the cloud could actually be privacy enhancing for government.

*I came to bury paper, not to praise it.*

There are scatterings of information across the Queensland Government—on over 200,000 work computer hard drives; in in-trays and on desks; in drawers and cabinets; inadvertently left on photocopiers and facsimile machines; saved to a myriad of portable storage devices; and stored on innumerable stand-alone databases.

We’ve all seen the figures – 90% of the world’s data was created in the last two years and every day 18.6 billion GB of data is added to the world’s store. Governments are significant creators, users, and repositories of data and the creaking and cracking of paper libraries and innumerable duplicated digital data stores begs the inevitable question: where on earth are we going to put all this information?

The cloud presents as a one-stop storage solution. But modern governments are not monolithic. They are more akin to the building of the Tower of Babel; a conglomeration of stand-alone information silos where the common language which enables the business of government is ‘documents’. The flow of information between the administrative organs is the lifeblood of government. And whenever there is mobility of personal information there is corresponding privacy vulnerability.

We have met the [privacy] enemy and they are us!

The need for ‘hard copy’ document flow within government is compounded by its polyglot nature and privacy risk is almost an inevitability of the dissonance of a government’s disparate information and ICT systems. A report by...
While these provisions may initially appear daunting, a closer examination of the convenient pair of sections 33(d)(i) and (iv) shows that the cloud service vendor is simply required to treat the customer's personal information in a manner consistent with the privacy principles.

However, despite there being eleven Information Privacy Principles (IPPs)23 in Queensland, there are only two principles of significant concern: data security (IPP 4/NPP 4) and disclosure to third parties (IPP11/NPP 2). Cloud services vendors should have little to no involvement in the other areas of operation of privacy law, i.e. collection, access, amendment and secondary use.

‘Data security’ and ‘data sovereignty’ are the two single biggest points of contention in discussions about the cloud.24 Obtaining robust data security and thereby ensuring compliance with the spirit of IPP4/NPP 4 is a no-brainer. Personal information is a subset of the information a government would store in the cloud. While of course governments are responsible custodians of their citizens’ personal information datasets, they are also concerned about other highly valuable and sensitive information – Cabinet documents, security and intelligence data, financial information, commercial information and intellectual property. Safeguarding of personal information will automatically fall out of the safeguarding of ‘non-personal’ government information.

Ensuring data sovereignty - that is, protecting against the bogey of foreign governments accessing Australian data stored in the cloud by through such legislation as the United States’ Patriot Act 2001, Britain’s Intelligence Services Act 1994, or even New Zealand’s Security Intelligence Act 1969 - is a frequently cited deterrent to cloud uptake.25 However, the ‘principles for the fair handling of personal information’ provide little protection for data sovereignty. The IP Act provides generous flexibility for ‘law enforcement activities’ the definition of which is broadly defined and which apply on a national level to any agency or part of an agency, criminal or civil, conducting the activities26. Put simply, when it comes down to a government’s intelligence services accessing personal information, privacy doffs its cap and respectfully shuffles out of the way.

4. Ibid, at page 27.
8. (ii) the transfer is necessary for the performance of the agency’s functions in relation to the individual;
9. (iii) the transfer is for the benefit of the individual but it is not practicable to seek the agreement of the individual, and if it were practicable to seek the agreement of the individual, the individual would be likely to give the agreement;
10. (iv) the agency has taken reasonable steps to ensure that the personal information it transfers will not be held, used or disclosed by the recipient of the information in a way that is inconsistent with the IPPs or, if the agency is a health agency, the NPPs;
11. And an equivalent nine National Privacy Principles (NPP)
Twin elephants in the room

Privacy can contribute to the conversation in two related areas: data breach notification and privacy complaints. Data breach notification is not generally mandated for in Australian privacy law (yet) but this does not detract from its undeniable benefits. While the Commonwealth Privacy Commissioner’s investigation into the unauthorised access of the personal information of approximately 77 million Sony Playstation customers found no breaches of the Commonwealth’s privacy principles, the Commissioner was nonetheless critical of its delay in notifying affected individuals.28 Playstation allowed seven days to elapse after discovering the breach before publicising it. The Commissioner noted that the ‘delay may have increased the risk of a misuse of the individuals’ personal information’29.

While data is wholly within the control of government – both in terms of location of the data and staff dealings – privacy breach notification can be instigated through other governance mechanisms. Those mechanisms would not be available in the case of a non-government agency. Governments would be prudent to include clear and firm protocols surrounding data breach notification in any service agreement with a cloud vendor.

As in most privacy jurisdictions there is the capacity in Queensland for an individual to lodge a privacy complaint concerning a breach involving their personal information, which can be the subject of a hearing and orders in the Queensland Civil and Administrative Tribunal.

Private sector organisations, domestic or international, are not covered by the IP Act. Although there is the legislative obligation for a contracting government agency to ‘take all reasonable steps’ to bind a contractor to comply with the IP Act, the obligation does not demand that the contractor in fact be bound.

So who do Mr and Mrs Jones from Gympie in Queensland go to when there has been a breach of their privacy in the cloud and, although the agency had ‘taken all reasonable steps’ to bind the contractor, the contractor remained unbound? The Jones do not have a contractual relationship with the cloud vendor and it would be impracticable for them to pursue potential civil remedies under international law. In this case the Jones may, through no action or fault on their part, fall into a legal privacy limbo.

While in the Sony Playstation case there was a financial incentive to ‘do the right thing’ by its customers30 this may not necessarily be the case for ‘customer data’ obtained and used by government agencies. However, it is strongly arguable that there is a fiduciary relationship between a government and its citizens which requires that their interests be protected in any dealings the government may have with a cloud vendor.

Summary

This piece does not advocate that governments should move their data to the cloud. Nor does it suggest that the cloud can provide the magic bullet for a government’s ICT needs.

There are privacy vulnerabilities associated with the cloud, just as there are privacy vulnerabilities with paper, e-mails, USB keys, smartphones and current ICT models. It may be too late to fully fix the privacy vulnerabilities associated with paper and other physically mobile documents. However, a move to the cloud, with well considered security and accountability safeguards, can not only be compatible with privacy law, it may enhance the protections for all government-held information.

It may not be hard to find the silver lining in the cloud. We now just need to work on creating a diamond exterior.

By Lemm Ex
Acting Queensland Privacy Commissioner
Samantha Banfield
Senior Privacy Officer
Office of the Information Commissioner, Queensland

---

27 Mandatory data breach notification has just been introduced for e-health records.
29 Ibid.
30 While Sony itself did not ‘lose’ any of its own information, the incident nonetheless cost Sony an estimated $171 million for such remedial actions as the introduction of an identity theft protection program, the ‘welcome back to Sony packages’, customer support costs, legal costs and reduced profits consequently to the breach.
The alleged rape and murder of Jill Meagher continues to make headlines and attract discussion. The Herald Sun recently reported that the man accused of these crimes was told that he was a suspect in a serious crime just hours before he was arrested and while under surveillance. There is speculation of a leak by someone with access to information sensitive to the investigation. This story is only one of many which points to the complex issues regarding information-sharing brought to light by this violent crime. Indeed, the case raises significant questions about social media and free speech, privacy and surveillance and it is these that I’d like to address in this article.

The fine line between productive and obstructive use of social media

The level of public reaction to Jill Meagher’s disappearance and unfolding events was surprising and some have said unprecedented. Thankfully, the violent circumstances of Jill’s death are not a common occurrence in Australia and this is perhaps one reason for the almost instant public fixation with the case which emerged. Another reason is that the story was fed to the community by the community, using social media to publicly appeal for information and help. At 4:56am on Saturday 23 September (only hours after Jill’s disappearance) John Safran tweeted “MISSING PERSON: Jill Meagher works at ABC Melbourne radio & has gone missing. Photo & info here. Please RT.” A Facebook page was set up almost immediately by her family in the hope someone saw something and could share information. Over the coming days, countless Facebook pages, blogs, tweeters and other social media users turned their focus to the case.

Police and Jill Meagher’s family highlighted the role social media had played in the investigation, with Ms Meagher’s family representative in Ireland thanking the public, and investigators recognising that it “… did play a major role in assisting the investigation...”. They also described the social media campaign to help find her as "unprecedented".

Until the point that the accused was arrested, public engagement in and discourse about Jill’s disappearance via social media was fine; even helpful. Then an arrest was made and overnight, the implications of expressing our views changed. Watching the growing “torrent of legally risky” social media, Australian journalist and academic, Julie Posetti tweeted “Dear tweeters: your anger & anguish @ #JillianMeagher's murder is understandable but commentary about her accused may risk his prosecution".

After the accused appeared in court, many angry people continued to use Twitter to vent their views about his guilt, speculate about his history and motives and link to pictures of him. At this point, more than 30,000 people (the same number who marched in Melbourne in honour for Jill) ‘liked’ a page on Facebook calling for the public hanging of the accused. Another hate page directed at the accused attracted 44,000 ‘likes’. Victoria Police similarly called for restraint, tweeting: “Please remember posting comments which endanger the presumption of innocence can also jeopardise a trial” and requesting Facebook to take down several pages (which, after initial resistance, it did).

What struck me was that the rules changed immediately after the accused was charged and there appeared to be an expectation that the public would be aware of this. In my view, this was hugely unrealistic and a little unfair. We were asked to participate through online forums in the search for Jill and in doing so, social media users were praised for the unprecedented support that they gave to the family and investigators. Then, the rules appeared to change and the same community was being chastised. But most of us are not well versed in the principles of ‘sub judice contempt’ and how they might apply when we use social media. The problem is that society as a whole is not media literate and more to the point, the notion of media literacy is fraught because it suggests there is a clear and coherent set of norms of which one might be aware. Clear and common-sense guidance is needed to explain how the impact of our published words via social media can interfere with or jeopardise a case as it proceeds through the legal system.

Caught on camera – justifying CCTV

The second issue which has attracted controversy within this context is the case for closed circuit television or CCTV surveillance. On 29 September, Victoria’s Premier Ted Baillieu called for more CCTV cameras to protect the public, a direct response to the death of Jill Meagher. Mr Baillieu pledged up to $3 million for local councils to set up CCTV networks. Melbourne Lord Mayor Robert Doyle said there was no doubt in his mind that CCTV cameras were significant in the investigation and a major contributor to public safety and the burden should not fall on the private sector to install surveillance cameras. Victorian Opposition also supported the initiative.

It cannot be doubted that the CCTV footage captured by the bridal shop in Sydney Road where Jill Meagher was last seen was instrumental in ascertaining what had occurred and
ultimately identifying her attacker. But the question is – is the reaction by Ted Baillieu and other Victorian politicians justified?

In their 2004 analysis of “open-street” surveillance, Wilson and Sutton sought to contest conventional wisdom about reasons for its installation. Discrediting the ‘official’ rationale (that CCTV is a cost effective way to combat public crime and disorder) they argue that key triggers for its widespread adoption are often non-tangible, such as “the tendency for security to be commodified and competition between and within urban venues to attract and retain consumers, fuelling demands for ‘something to be done’”.

Indeed there is no consensus on the effectiveness of public CCTV as a deterrent or an effective mechanism for responding to crime. Some suggest that “Organisations responding to the “need to be doing something” are susceptible to spending money on equipment acquisition and deployment without appropriate investment in ongoing monitoring”.

David Brin suggests that the problem with surveillance of public places is one of equity:

“We’re observed but often aren’t aware of being observed, have no choice in being observed and - more importantly - aren’t in a position to watch the watchers or use our knowledge about their observation.”

Most Australian legislation regarding video surveillance relates to its use in the workplace or its use by government agencies or commercial operators on a covert basis within private spaces, rather than use in public spaces. There seems to be a view that any difficulties arising in relation to video surveillance can be addressed within existing legal frameworks.

Significantly, NSW and Queensland have both introduced guidelines for councils and local governments considering the installation of CCTV. Both guidelines recommend that prior to its approval; research into the viability of CCTV should be conducted, to avoid (amongst other things) “knee jerk installation of CCTV following a sensational incident”.

Here we have had a sensational incident with the difference. The alleged perpetrator was caught with the help of CCTV. What better evidence to support an argument that cameras catch criminals? Says the press: “The tragic death of Jill Meagher has clearly shown the value of security cameras.

The cameras, as has been proved in other investigations, are a successful 21st-century approach to violent crime.”

I am in two minds about this one. Like many others, Jill’s case affected me deeply and for this reason I am thankful for the camera footage which led investigators to the accused. One might say if you’ve got nothing to hide you’ve got nothing to fear. But statistics from Britain, where the average citizen is said to be caught on camera approximately 300 times a day (making Britain the “most watched nation”) dampen my sentiment. The reason is for this is that before we respond to the terrible events concerning Jill Meagher by installing more cameras, we need to understand how that data is being stored, accessed and archived and how might it be used in the future. If I am being recorded up to 300 times a day, I’d appreciate more public dialogue about these critical questions.

Jill Meagher’s death and the events that followed raise questions about the boundaries of effective use of social media and recent support for more CCTV to prevent and detect crime. In my view, the dissemination of social media guidelines to help prevent a mistrial caused by the publication of inappropriate comments about the accused should happen imminently while public regard for the topic is high. By contrast, the roll-out of more CCTV cameras is an initiative that should be carefully considered and only pursued if supported by quantifiable benefits to society; it is not satisfactory to go down this path to be seen to be “doing something.”

By Melanie Marks, Board Director, iappANZ

---

Privacy and the value of sharing – a few thoughts

"I think the Government made Facebook in an attempt to make privacy uncool. Think about that. I think that’s true, ‘cause they don’t have to tap our phones or survey us when we just yield to them everything, just of our own free will. Home address? It’s a little weird, OK. Phone number? Call me. Photos of everyone I know? Here, let me tag those for you."

Peter Holmes, Comedian

The concept of privacy has many definitions, for all of us there are different levels which we like to control. For this reason I think Ruth Gavison’s definition captures the multi-dimensionality of the concept best. Gavison’s description of privacy is dependent on “limited access” and a combination of three separate ingredients, being secrecy, anonymity and solitude. The ability for individuals to release or limit the amount of data is of paramount importance to the idea of individual autonomy. During last year’s Privacy Summit we were fortunate to have Professor Alessandro Acquisti address us on some of his privacy research. He found that provided people were asked for their consent for information, they frequently gave more than was expected or asked – as though the invitation marked a respect for the individual’s rights which was then honoured by a generous response. Obtaining consent and then respecting the value of the data with appropriate security and mitigation of loss in the event of a breach are worthwhile processes for businesses to consider in more depth.

Consent

Mining data and sharing data in health and other environments provides an invaluable resource be it for better care, efficiency or shareholders returns. The richer the data, the more valuable it is. Given the research above and many other sources getting the consent model right seems to be a sometimes overlooked aspect in organisations. In health, despite the frequently raised concerns of ‘big brother’, people are very generous with their most intimate data – as long as it is on their terms, i.e. if they volunteer it or are asked for it in a clear and respectful manner. The website established by a brother of a man who died from Lou Gehrig’s disease in USA to help other sufferers deal with the disease, now has more than 50,000 people uploading personal data for it in a clear and respectful manner. The website was made available. Section 6, Principle 5 of the Privacy Act 1993 NZ provides that the repository of the data must do “everything reasonably within the power of the agency” to prevent unauthorised use of the private information they hold. It would appear that there were some holes in the security here and the journalist provided all data to the Privacy Commissioner, so possibly there was no harm done. Of course things could have gone quite a different way with terrible consequences for the victims of the data breach, but in any event the damage done to the credibility of the Ministry would not be insignificant. The public perception of the disregard for security of their children’s information will no doubt linger and block open sharing and the concomitant benefits discussed above.

Mitigation of damage to the victim of data breach

In Australia, like most countries, the economics of increasing productivity are compelling, and a key to this is facilitating the flow of data to the right people at the right time is. The underlying issue with data in every sphere is ensuring its appropriate collection, security and then mitigation of damage in the event of a breach. As Lawyer Peter Leonard mentioned this week, whilst we do not have compulsory breach data notification as a part of the revised privacy Bill before Parliament at present, he wagers that we will within 12 months. Let’s hope so!

By Emma Hossack Vice President, iappANZ

33 Including resources like Iron Ore as reported by AFRBOSS.COM Oct 2012 p.17 quoting Tinto Iron Ore CEO Sam Walsh
34 For example Zogby Interactive Survey of Adults 08/24/10. http://patientprivacyrights.org/patient-privacy-poll/
35 ZD Net, “NZ child protection details were open to public download” Michael Lee, October 15, 2012.
36 Medical Software Industry Association CEO Summit 23 October, Sydney.
37 The Personally Controlled Electronic Health Record Act 2012 (Cth) provides for compulsory notification of a data breach resulting from the use of the PCeHR system.
ANNUAL PRIVACY SUMMIT
23 NOVEMBER 2012 SYDNEY
The SMC Conference & Function Centre

The fifth iappANZ annual one-day conference will be a super-charged day of practical and insightful educational content designed to inspire and inform delegates.

The program brings together on stage luminaries from government (including privacy regulators), privacy professionals in business and academia, making it the most important conference on the privacy professional’s calendar.

The conference comprises a mix of presentations, discussions and panels creating a dynamic platform for delegates to engage with esteemed thought leaders who will share their ideas and debate topical issues faced by professionals in the data protection, academic, governance, risk and compliance sectors.

For the first time, the afternoon session will be split into two streams and delegates can choose from an engaging panel on global privacy regulatory changes or a workshop on how to conduct privacy impact assessments. The latter will be run by Malcolm Crompton from Information Integrity Solutions P/L and Anna Johnston from Salinger Privacy. Both of the workshop and panel sessions are also available separately for people who aren’t able to attend the whole conference.

Other conference highlights include, ‘A Day in the Life of a Privacy Professional’ panel where delegates will hear from representatives in the telecommunications, health insurance and banking industries on managing privacy for their companies’ customers.

The conference will also provide delegates with the opportunity to learn about the impact of the new privacy reforms from a regulatory and business perspective, surveillance and privacy as well as many other topical issues.

To maximise on the day’s learnings and continue the conversation, there will be a Cocktail Reception directly after the close of the conference. This is free for delegates.

Confirmed speakers

- Australian Privacy Commissioner, Timothy Pilgrim
- New Zealand Privacy Commissioner, Marie Shroff
- NSW Privacy Commissioner, Dr Elizabeth Coombs
- Dr Juanita Fernando, Academic Convenor, Faculty of Medicine, Nursing and Health Sciences, Monash University
- Dr Emmeline Taylor, Lecturer, School of Sociology, Australian National University
- Malcolm Crompton, Managing Director, Information Integrity Solutions
- Anna Johnson, Director, Salinger Privacy
- John Pane, Regional Lead, Privacy Compliance & Data Protection – Asia Pacific, Johnson & Johnson
- Mei Ramsay, General Counsel, Medibank
- David Batch, Portfolio Manager - Customer Privacy & Awareness, Commonwealth Bank of Australia
- Helen Lewin, Chief Privacy Officer, Telstra
- Dr Paolo Balboni, Founding Partner, ICT Legal Consulting and Scientific Director, European Privacy Association

For more information visit www.iappANZ.org.
Upcoming Privacy Events


iappANZ Privacy Summit, Sydney 23 November 2012 [www.iappanz.org]

Inaugural iappANZ seminar in New Zealand, Wellington, 14 November, 4:30-6pm [www.iappanz.org]

Find out more about iappANZ and how you can benefit from your regional privacy association. Annelies Moens, President of iappANZ, will provide insights on certification, IAPP affiliation, the annual Australia/New Zealand Privacy Summit and more.

Special Invited Guest Speaker: Mike Flahive, Assistant Commissioner (Investigations), Office of the Privacy Commissioner, New Zealand

Mike will present the Office of the Privacy Commissioner’s perspective on what the ACC data breach looked like and discuss what was happening at the ACC and how it unfolded and address what is happening now.

Mike joined the Office in April 2006 and manages the Investigations Team based in Auckland and Wellington. His previous roles were in the NZ Police as an investigator, private legal practice in Hamilton and in-house counsel for a regional council. Mike manages the day to day complaints investigation processes of the Office. He is also in charge of the enquiries answering service, the Office’s education function, and production of case notes.

Venue
KPMG, Level 9, 10 Customhouse Quay, Wellington

Cost
This is a free event. – but registration is required at [www.iappanz.org]

KPMG will be providing drinks and canapés for attendees. Stay to network with your fellow privacy professionals and colleagues.

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 Peter Leonard, partner Gilbert + Tobin Lawyers

Peter presented on the competing visions the Australian Government is considering in reaching a decision on whether Australia needs a statutory cause of action for an invasion of privacy. Peter entertained the audience with anecdotes, whilst providing a deep insight into the various complex matters that must be considered before deciding this question including:

• a summary of the common law cause of action so far developed by the Australian courts,
• the common law cause of action for privacy as it has been established in New Zealand,
• a deep analysis on the cases that have come before the English courts including the development of the somewhat controversial “Gagging” & “Super” injunctions,
• freedom of expression and the media.

Peter than proceeded to dissect and analyse four contending visions that have so far been provided to Australian State and Federal Governments:

• the Australian Law Reform Commission (ALRC), the discussion & recommendations for a statutory tort,
• the New South Wales Law Reform Commission report (NSWLRC) recommending a statutory tort and excluding the common law,
• the Victorian Law Reform Commission Report (VLRC) - Surveillance in Public Places which recommends a statutory tort with the defence of public interest; and
• Peter’s alternate vision for consideration, developed by Peter and his partner Michael Burnett and submitted to the Government’s issues paper and provided to the iappANZ’s Privacy Summit.
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.