President’s Letter

New members, sponsors and training sessions have kept iappANZ busy over the last quarter. We are delighted to partner with our Platinum Sponsors McAfee in events such as “Feeling Secure?” This is the first of our free member training sessions which will be held next Wednesday 31st July at OAIC in Sydney (registration details inside). This session will provide a working knowledge of the new APPs as well as specific training on how to practically enhance security in your organisation. The mixture of legal, practical and technical together with a specific address on the issues by our Privacy Commissioner, makes this event invaluable preparation for 12 March 2014. If you have colleagues who have thought about joining iappANZ in the past, now is the perfect time as the non-member registration fee will be deducted from the cost of membership. We will be continuing this special membership discount to promote training and privacy awareness for all of our training sessions up until March 2014.

The recurrent theme in articles this month is the increasing recognition of the value of privacy professionals to business. There is practical advice from one of our New Zealand members (and may I note there are 3 NZ Contributors this month which is a first), and insights into the dangers of treating privacy like a “tick box” compliance exercise. In May we picked up on the theme of data as a
major asset, and this month the importance of security around that asset is a focus both in our articles and in our training session.

As you may be aware, The Privacy Advisor is another great resource available through our sister organisation IAPP in the States, and it has a distribution of over 20,000. We are now going to be offering the articles from our Bulletin for publication in The Advisor, so it’s a wonderful opportunity for you to have your ideas read and spread across the World. Think about contributing for August and send your articles to Kate Johnstone our Editor before 20th of the month. (Dont forget the prize we will be awarding.)

iappANZ will be conducting further industry specific training in Sydney as well as Melbourne and Brisbane, so keep an eye on our website, Bulletins and news flashes for registration details. We are also thrilled to confirm our International Speakers for this year’s iappANZ Privacy Summit at The Westin Hotel in Sydney on November 25th. Richard Thomas CBE former UK ICO will talk about all aspects of data breaches, which is very timely in light of the Privacy Amendment (Privacy Alerts) Bill 2013. Mikko Niva, CPO of Nokia from Finland will discuss the business case for privacy and how Nokia approaches its development with privacy by design. Our third International guest is Danny Weitzner, who has advised the Whitehouse on Privacy and is recipient of the IAPP Privacy Professional of the year Award. A recent presentation by Danny at the IAPP Navigate Conference, can be watched on You Tube at http://www.youtube.com/watch?v=2f5hQ4OSxmg&feature=share&list=PLYVXx3zCnkX5

Those of you who use Twitter and LinkedIn will be interested to know that we have now re-ignited these mediums, and if you want to get involved and start some discussions before we all meet in November, it’s a good way to do it. More details for you to click and get started follow in the Bulletin. This is another way of creating more of a community for and connections with our members.

Finally, we farewell Judith Cantor this month. After 2 years of loyal service to our members, Judith is moving on to concentrate on her Consulting Business. Those of you who have met Judith will know of her warmth and enthusiasm and we all wish her every success in her future endeavours.

Warm Regards
Emma Hossack
President, iappANZ
reforms in March 2014 as well as a new mandatory data breach notification scheme this year or next. During the next 6 months and beyond (taking into account the December/January hiatus!), it is critical that regulators, privacy practitioners, compliance and information experts, industry representatives and privacy advocates share knowledge and insights to raise awareness on implementing new compliance requirements. iappANZ is committed to helping promote and support such connections among members, with regulators and across other professional organisations like the Australian Information Industry Association and the Australian Retail Credit Association, and through our member bulletin.

This month, we are grateful for articles from regular and new contributors! Chong Sao, a consultant with Information Integrity Solutions gives us some interesting stats on the rise of the smartphone and tips on minimising privacy threats. iappANZ Board Director, Peter Leonard provides his usual free flowing content on the challenges of explaining the Australian privacy landscape. Reading the article, I couldn’t help but think of the popular animated children’s flic, ‘Finding Nemo’ - a mix of deep sea diving and amnesia going on!

Moving on to another equally challenging topic is Health IT and privacy. We are pleased to share an article from Tom Bowden, Chief Executive of HealthLink Ltd on the paradigms of health information IT systems and privacy. Finally a few informational updates; one from Board Director, Kate Reynolds on the new risk management guidelines on offshoring applying to government agencies; and second, a breakdown of the security threats/cybercrime attacks on SMBs from McAfee.

Thanks to Matt Poblocki from eBay Australia & New Zealand for volunteering for our member profile this month and don’t forget to check out our international speaker profiles!

I look forward to seeing you at our upcoming events!

Anna Kuperman  
Vice-President, iappANZ

To join the privacy conversation, keep up to date on developments and events and to make connections in your professional community, join us today!

Our LinkedIn group is:  
http://www.linkedin.com/groups?g=1128247&trk=anetsrch_name&goback=.gdr_1281574752237_1

Follow us on Twitter at: https://twitter.com/iappANZ
"Data is the 21st Century’s new raw material. Its value is in holding governments to account; in driving choice and improvements in public services; and in inspiring innovation and enterprise that spurs social and economic growth.”

A recent post by Professor Daniel Solove2 confirms what privacy professionals have long known – a strong grasp of privacy makes for a safer and richer business. The practice of organisations or individuals not sharing data for fear of breaching the privacy legislation is so widespread that there is even an acronym for the frustrating behaviour which manifests in the refusal to divulge information, "BOTP" - Because of the Privacy Act. When information which should be shared legally and usefully is not shared, on account of a misunderstanding of the privacy legislation, the results can be dangerous and expensive. “Organisations that don’t understand what can and cannot be done legally are as likely to disadvantage their clients through excessive caution as they are by carelessness."3 At worst, lives can be lost, but more commonly businesses suffer loss of reputation, client’s trust, and with it, business.

The case of Seung Cho described by Solove, is an instance of what happens when organisations fail to understand when they can and when they can’t share personal information. Seung Cho committed suicide following a number of incidents in an educational institute which were not shared; the information could have averted his death. It was not the lack of laws or policies. People simply didn’t know, or understand what they could legally share. They lacked a privacy officer and training on the implementation of a privacy policy.

These shortcomings are not confined to educational facilities. Findings in the UK that citizens and health providers lacked confidence in the governance around health information led to a recently released report, Information to Share or Not to Share.4 Paradoxically, the fact that clinicians had become so concerned about the legality or otherwise of sharing that they deliberately erred on the side of non-disclosure which resulted in poor health outcomes. The balance between protection of patient information and the use and sharing of that information for improved health outcomes is complex. It is also essential. The duty to share information can be as important as the duty to protect patient’s confidentiality.

The Caldicott Report noted several examples of where failure to share had heartbreaking consequences. In one, a 72 year old totally blind man who was caring for his wife who suffered dementia and Parkinson’s, requested the hospital to email reports to him. This enabled his screen reader to convert the reports to speech. The hospital refused on the basis that email was insecure, so to preserve confidentiality, the hospital sent hard copies in the mail. The man was advised to find someone to read the reports to him.
The underlying reasons given in the Report for this type of behaviour were lack of privacy understanding, training and marginalisation of information governance professionals. Where there was privacy training, one nurse described it as equivalent to an annual “sheep dip” which staff could go through without thinking. These are common themes which play out in many high profile breaches where organisations fail to have privacy experts in the “C Suite”.

Data is the mine of the future, according to Rio Tinto CEO Sam Walsh. Companies which fail to invest in the best privacy and security to protect that data are unlikely to participate in the riches. Emma Hossack is President of iappANZ and CEO Extensia

With thanks to Peter Leonard, an iappANZ Board Director and Partner at Gilbert+Tobin who keeps the iappANZ Board on its toes sharing many fascinating articles and posts like Solove’s LinkedIn post, 9 July 2013. Clearly Peter does not suffer from the ‘knowledge is power’ syndrome which afflicts many of us lawyers.


2 Daniel Solove is the John Marshall Harlan Research Professor of Law at George Washington University law School.


4 https://caldicott2.dh.gov.uk/ March 2013

5 ACC breach and independent report discussed at the IAPPANZ Summit 2012 is a text book example of the cultural deficiencies which resulted in a massive overhaul of the NZ ACC.

6 AFR Boss Magazine 2013
In the face of Board questioning and media scrutiny, there is a sense of urgency in implementing appropriate controls within the organisation to avoid being the highlight of tomorrow’s newspaper headlines.

Organisations are struggling to ensure that they implement appropriate controls to protect information in a practical and sustainable manner. In consulting with clients and through Risk and Audit Committee requests, there is an increased awareness in respect of the potential risk to the business and a requirement to obtain a level of comfort around data protection processes. Reviews within the Internal Audit plan or via management requests are now common place through Privacy Impact Assessments (PIAs) or Privacy Audits.

From an operational perspective, it is also reassuring to see that project managers want to ensure that new systems and processes are cognisant of privacy protection requirements and are calling on privacy professionals to be involved from the earliest stages of design. While this is commendable, ‘Privacy in Projects’ should be assessed from two perspectives:

- Ensuring that the design of the new process and/ or system has appropriate controls to protect sensitive information; and
- Ensuring that the project personnel understand their responsibility to protect sensitive information while in project mode.

Management and project teams often recognise the potential risk from the design of the new process and/ or systems however do not think of the responsibility for protecting sensitive information during the project.

Some key questions for your project team:

- Does the project team understand where the data is stored, the value of the data and the sensitivity of this information?
- Will the data be used for a different purpose from when originally collected?
- If the objective of the project is the formation of a data warehouse – how will the concept of “big data” affect individuals’ privacy? Has the project team thought about resulting privacy risks from the aggregation of data?
- Does the project team understand its responsibility for protecting information? Do project staff know what is actually required?
- Do we understand how affected business data flows, throughout the lifecycle of the data, both now and in the to-be state?
- If we are using third party contractors as an implementation partner how will we ensure that they will protect our information?
• Is the implementation partner on site or accessing our systems remotely? If so, from which country – do they understand our privacy obligations?

• If we are hosting data from other countries then have we understood foreign privacy obligations which may be even more stringent than New Zealand’s

• Do we still have a requirement to retain information from legacy systems – if not, does the organisation have appropriate destruction or archiving processes?

• Do we need ‘live’ data for testing purposes?

• How do we ensure that project team members do not take information off site – whether through printing hard copies or downloading to electronic formats?

• Typically individuals have wide user access while in project mode to design, test and build – how do we ensure that these individuals only have access to the information pertinent for their project role – is this even practical? Do we need to anonymise our data?

• How will the future systems protect sensitive information?

• What is the process to be followed if we have a breach? What is our communication strategy?

• When the project is complete, how do we ensure safeguarding of project documentation – specifically as it relates to private information? How does this transition to business-as-usual (BAU)?

When dealing with particularly sensitive information, I would recommend that you include a privacy or information security expert as a project team member to provide practical solutions to manage the aforementioned project risks.

Dependent on the risk to the organisation and the impact of the project on the community, it may also be prudent to alert the Office of the Privacy Commissioner to the objective of the project at the initiation phase. The Office of the Privacy Commissioner has assisted some organisations by providing guidance on how to actively manage their project risks pertaining to data privacy.

Privacy is not a compliance ‘tick-box’ exercise but a business imperative. If information is a new class of asset – we should be implementing appropriate controls to protect this asset as we would others within our business. It is however important to keep privacy practical to ensure sustainability. A few simple control elements can assist to align to the 12 Privacy Principles and reduce the risk to the organisation.
Businesses can no longer plead ignorance – the risk to their reputation and bottom line is now too great.

Kerry Bakkerus is Senior Manager, Enterprise Risk Services at Deloitte in Auckland kebakkerus@deloitte.co.nz

The Tortuous Road to Privacy Reform in New Zealand
By: Gehan Gunasekara

The Privacy Act 1993 (the Act) has now been in place for twenty years in New Zealand. It was a technology-neutral and progressive statute when passed, as it applied to both public and private sectors and had few exceptions, such as Australia’s small business and employee record exclusions. It is also underpinned by a relatively low-cost forum for complainants to pursue remedies where the Privacy Commissioner has determined there has been a contravention of privacy (and even to challenge her determinations to the contrary). Unsurprisingly, then, New Zealand had little difficulty in obtaining a formal finding of adequacy, by the European Union last year, in respect of the transfer of personal data from there.

Despite these advantages, the Act is now in need of modernisation due to developments such as web 2.0, Big Data and cloud computing. Following a four-year long review of privacy law in New Zealand the New Zealand Law Commission (NZLC) delivered its final report on the Act two years ago, although the Government has yet to implement any of the recommendations made with one exception. The recommendations made by the NZLC include removing the domestic affairs exclusion for individuals where this constitutes putting material online that reasonable people would find offensive and enabling attention to systemic (rather than complaints-driven) privacy issues through giving new powers to the Privacy Commissioner to serve compliance notices on agencies. The NZLC report also addresses cross-border data flows.

The latter differ from Australia in several aspects. In the first place the NZLC proposes a stand-alone strict liability accountability standard for domestic outsourcing. However, for other data transfers, the model proposed is a hybrid between the accountability model adopted in Australia and the data export prohibition model. In the first place, the NZLC proposes that transferors must take “reasonable” steps to ensure that “acceptable” privacy standards will apply to the information. Further, the recommendations propose giving the Privacy Commissioner power to approve “specified overseas privacy frameworks” as providing acceptable privacy standards as well as guidance to agencies when conducting due diligence on transfer. The result would be a regime for cross-border data flows closer to the European Union’s in some respects, than Australia’s.

The one exception to the lack of action on the part of the Government in response to the recommendations has been in addressing the need for better information sharing in order to improve the provision of public services by government agencies. The result has been the enactment, earlier this year, of a new Part 9A of the Act which for the
most part weakens individual privacy, instead of strengthening it. Part 9A permits the adoption of information sharing agreements between public sector agencies and between public and private sector ones. These may be adopted by orders in council, following consultation but do not need prior clearance by the Privacy Commissioner. It is noteworthy that, despite public comments at the time of enactment the measure was to facilitate better provision of services, it replicates provisions taken from the existing Part 10 of the Act (which relate to information matching or automated processing between government agencies) containing safeguards before “adverse action” is taken against individuals as a consequence of the sharing of information. This hints, perhaps, at a somewhat less benevolent purpose.

The pendulum of information privacy regulation in New Zealand has periodically swung between greater weight being given to the public interest (through more disclosure) and strengthening of individuals’ rights to access to and control of their personal information. This was seen with the appointment of a Privacy Commissioner as long ago as 1976 when the Wanganui Computer Centre was opened and the Privacy Commissioner Act of 1991 which facilitated automated information sharing and information matching between government agencies. This was counter-balanced by the enactment of the Act in 1993 as the Act implemented the OECD model of information privacy principles, conferring rights on individuals covering the entire information life-cycle. Although the Act has proved its worth the pendulum has now swung the other way somewhat and it is to be hoped that the enhanced remedies and powers recommended by the Law Commission will shortly be adopted through a new Privacy Bill as promised last year by the Minister for Justice, the Hon Judith Collins.

Gehan Gunasekara is an associate professor in commercial law at the University of Auckland Business School and advised the New Zealand Law Commission in its review of the Privacy Act 1993.

Privacy and Trust in an increasingly mobile world

By: Chong Shao

It is no exaggeration to say that mobile devices – and in particular, smartphones – have become one of the most important pieces of technology for individuals as well as businesses today. With the confluence of processing power, wireless networking and other design innovations, smartphones have become an all-purpose tool and an indispensable part of our lives. Here are some relevant statistics to consider:

- **76% of Australians owned a smartphone by July 2012**, with 84% projected by mid-2013.

- **Global mobile data traffic grew by 70% in 2012 from the year before**, and is projected to increase 13-fold between 2012 and 2017.
• It is predicted that by 2014, mobile Internet users will outnumber desktop Internet users.

• Worldwide mobile payment transactions will reach a value of $235.4 billion in 2013, up 44% from 2012 and is forecast to grow to $721 billion by 2017.

As we are all aware by now, personal data has become highly valued by companies and governments as a new asset class. The proliferation of mobile devices and apps magnifies the data deluge and the ensuing privacy risks. Smartphones are not only subject to all the same kinds of privacy issues as personal computers; they also exacerbate those issues and create new risks:

• Smartphones are (almost) always with the individual and always on – data (especially the individual’s location) is constantly tracked and recorded.

• Due to its multiple functionalities, many more types of personal and sensitive information are stored on a smartphone – eg, call logs, geo-location, texts and emails, photos and videos, contacts, financial information, health information, web browsing history, etc.

• A single device collects data for multiple entities, including communications service providers, the phone’s manufacturer, mobile platform and app developers, and government agencies (as was recently highlighted by the revelations of PRISM and other intelligence programs).

• The smartphone’s size and value makes it vulnerable to loss or theft.

• There are practical challenges with conveying relevant and useful notice on small screens.

In today’s digital economy, there is a growing tension between businesses who push the boundaries of innovation and regulators seeking to rein them in. In recent months, the Office of the Australian Information Commissioner, the Federal Trade Commission in the US and California’s Attorney-General have all issued guidelines and recommendations for respecting privacy on mobile devices.

Alongside these developments, it is becoming increasingly important to understand how individuals think and feel in order to deliver innovative products and services that they will embrace rather than shun due to privacy concerns.

Survey on mobile phones and privacy
Last year, a comprehensive study into consumer attitudes on mobile phones and privacy was published by researchers at the Berkeley Centre for Law & Technology, in a survey of 1,200 Americans. The results depicted a population that was very privacy-conscious. By overwhelming majorities, the participants opposed:

• Police officers searching a phone during arrest without a warrant.
• Stores who have been provided with their mobile number calling to tell them about products and services.

• Sharing their contact list information with a social networking app in order to receive friend suggestions.

• Sharing their contact list information with a coupons app so that their contacts can also be offered coupons.

• Their cell phone provider using their phone’s location to tailor ads to them.

In light of these results, the researchers suggested that “Americans are likely to reject a variety of uses of mobile phone data that are attractive to merchants, marketers and law enforcement officials.” They proposed that the value proposition offered to consumers by service providers, and the cost-benefit analysis offered to citizens by government officials, should be especially clear and compelling for desired uses of mobile data. These results are likely to be just as applicable for businesses and governments in Australia and New Zealand.

The importance of trust
Organisations must move beyond a take-it-or-leave-it approach when offering mobile products and services that collect and/or use personal information. While this is often a successful short-term method, it does nothing to reassure the consumer. At best they remain passive and ignorant, at worst they grow angry and resentful. As all businesses know, trust is one of the most precious commodities because – among other things – it makes individuals willing to share their information. However, it is not enough to merely say “trust us, we’ll do the right thing.” Trust must be earned by the demonstration of values and good practices, accumulated over time.

With the quickening pace of start-ups and mobile technology, it is hard to establish the initial rapport (and even harder to recover from a privacy blunder). Here are some things to think about:

• **Legal compliance is a start but it is not enough**
  asking people to read a wall of text and click “I accept” to your terms is not good privacy practice by itself, as most people do not actually read it.

• **Not everybody is like you**
  For example, never assume that everyone will enthusiastically embrace that new product or practice, no matter how much benefit – rationally speaking – they might get out of it.

• **Avoid unexpected surprises**
  Ask yourself: what would the individual think about what I am proposing? Would they be OK with sharing this information with me and my business partners? Is this something I should notify them of or seek permission first? It is important to put yourself in the shoes of the individual.
• **The speed of change is faster than we thought**
  Technology has been advancing so fast that many businesses have not yet grasped the significance of what they can do versus what they should do. The global changing landscape is littered with the wreckage of ambitious initiatives that were not properly thought through.

• **Seek professional privacy advice**
  Don’t be afraid to seek advice when you are unsure of the privacy implications, and don’t avoid privacy professionals because you may not like what they have to say! They can help you build more trusted products and services.

_Chong Shao is a Consultant at Information Integrity Solutions. He can be contacted at cshao@iispartners.com_

---

**Lost in the landscape of privacy**
By: Peter Leonard

Explaining the Australian privacy landscape has become increasingly difficult.

The first challenge is explaining that the Australian Privacy Commissioner in fact sits in the Office of the Australian Information Commissioner (OAIC) and applies laws that the Australian Parliament has misleadingly and deceptively called ‘principles’.

Second is the challenge of describing how to read principles as laws and fit them together with other provisions in the Privacy Act that clearly are laws. And then to try to read them fit for the purpose of dealing with cross-border cloud deployment, geo-tracking of devices, database consolidations and data analytics.

Third is the challenge of explaining how privacy and security by design become law (through principles) from 12 March 2014 and must therefore be built into the architecture of information flows and the engineering of how organisations structure their processes and design their products. The law as a matter of practice requires organisations to devise technical, operational and contractual safeguards to implement privacy and security by design, but industry practice has not yet developed to the stage where we can reliably say what safeguards are appropriate when.

Scepticism often sets in when management are told that this isn’t just a case of bolting on some additional technical security to existing information and work flows. Incomprehension usually arrives when the information engineers and the privacy and compliance professionals gather together and the engineers hear that their best practice security risk management frameworks and methodologies don’t really work for personal and sensitive information and, by the way, all that information about customers that looks innocuous and
'everyone must know' is really personal information about individuals that is regulated.

Next is the challenge of explaining the legal status of guidance from the OAIC, particularly in an environment where the Australian parliament dodges hard issues by placing increasing reliance upon OAIC guidance (without giving this guidance any formal legal status) as to principles (law) to give context and meaning to the law.

Then follows the challenge of explaining that although the Privacy Commissioner has a central guidance and enforcement role, the Commissioner has been allocated very limited staff and other resources, notwithstanding a major expansion in the Commissioner’s responsibilities and the importance of privacy throughout the Australian economy. Given the importance of the Commissioner getting out guidance on key interpretative matters as to the application of the new privacy laws from 12 March 2014, one really can’t expect the Commissioner allocated a meagre resources budget to have much to say about the gazillion privacy policy issues exercising privacy regulators and privacy professionals around the globe. And the Commissioner has to also address major government privacy issues, such as facilitating data sharing between government agencies and cloud computing. And deal with PRISM. And just wait until the industry codes (APP Codes) start arriving on the Commissioner’s desk.

And, of course, privacy pops up in lots of different places in Australia nowadays. As well as the OAIC interpreting and applying the Privacy Act, the Australian Communications and Media Authority (ACMA) has become a very active privacy policy maker. First, by applying its Privacy Guidelines for Broadcasters in investigations about privacy related infractions of broadcasting codes, the ACMA has been the chief developer of the law as to serious invasions of personal privacy as applicable to the electronic media. So although we do not yet have an accepted private right of action for invasion of privacy in Australia, the ACMA has developed and applied rules as to what is a serious invasions of personal privacy. Second, through the ACMA’s application of the Telecommunications Consumer Protections Code C628:2012 (the TCP Code), the ACMA has become a principal regulator of handling and use of telecommunications related personal information. The TCP Code has strong privacy provisions which require telecommunications service providers to, among other things, have robust procedures to keep customers’ personal information secure. These provisions have been applied against providers for failing to adequately secure stored customer information from third party hack-in intrusions.

The ACMA has alas been a vigorous enforcer of spam and do not call legislation, two key planks in regulation of electronic marketing. And the ACMA has been using its research and policy budget to good effect, recently releasing detailed discussion papers on diverse privacy related topics, such as why ‘coherent regulation is best for digital communications policy’, cloud services, near field communications and apps. These papers include proposals for an active role for the ACMA in further development of privacy regulation
of all information passing through telecommunications links or over radiocommunications or derived from communications services. In an interconnected digital and cloud based world, that's most information.

But that's not all.

We have the Australian Competition and Consumer Commission (ACCC) in applying the Australian Consumer Law. In the United States, the Federal Trade Commission has used comparable laws to become a de facto regulator as to the fairness and intelligibility — in the new trendy new term, ‘transparency’ — of privacy statements and consumer contracts. These laws are also powerful tools for the regulator to argue that if a corporation does not comply with its own privacy statement, that corporation is guilty of misleading or deceptive conduct.

We also have the Australian Attorney-General’s Department applying the poorly understood Telecommunications (Interception and Access) Act 1979 and Criminal Code provisions relating to unauthorised access to stored communications — such as email servers — and other unauthorised access to information technology systems. Arguably many cookie deployment today infringe these provisions.

And we also have State and Territory Governments and regulatory authorities applying State and Territory privacy laws relating to personal information derived from State and Territory agencies, use of workplace or video surveillance technologies, use of tracking devices and technologies and access to computer data. There is plenty of overlap of State and Federal law, and plenty of variation in the content of State and Territory laws. Not to mention State and Territory based health privacy laws.

And then, of course, there are industry codes of practice, many of which include provisions dealing with privacy and provide remedies for non-compliance.

So privacy and data protection in Australia has become a confusing landscape, with forests of regulation to get lost in, unexplored corners and many poorly understood rules. At a time when privacy and information security is becoming a major area of concern for governments, businesses and consumers, it is unfortunate that Australia has created such a confusing thicket of regulation and quasi regulation. So the next time that the CIO chairs a security and privacy compliance meeting with the CMO, the HR director, the information security experts and the privacy professionals, and that meeting disappears into a cloud of mutual incomprehension, you’ll understand why.

Peter Leonard is a Board director of iappANZ and a partner at the firm of Gilbert & Tobin
Australian Government information in outsourced or offshore ICT arrangements

What is it?
Earlier this month, the Attorney-General’s Department released its Australian Government Policy and Risk management guidelines for the storage and processing of Australian Government information in outsourced or offshore ICT arrangements. The new guideline is intended to complement existing policy such as the Australian Government Information Management Office’s Australian Government Cloud Computing Policy, the Department of Broadband, Communications and the Digital Economy’s National Cloud Computing Strategy, and the Defence Signals Directorate’s Cloud Computing Security Considerations.

Who does it apply to?
The new policy is part of the Protective Security Policy Framework (PSPF), which currently applies to all Government agencies.

What does it mean for personal information?
If an agency wishes to outsource or offshore its storage or processing of personal information, it will have to conduct a risk assessment in accordance with the guidelines and obtain the appropriate level of approval. The guide gives an overview of the risk assessment process that agencies are required to follow.

If services are provided onshore in a private or community cloud, based on the risk assessment the Agency Head may approve.

However, if services are to be performed onshore in a public cloud or offshore in any manner, following the risk assessment, approval is required by the Agency Head, the relevant portfolio Minister and the Attorney-General.

Where can I get more information?
The full guidelines and other PSPF related resources can be found at www.protectivesecurity.gov.au.

Back to Top

CRN Threat of the Month – Securing the safety of SMBs
By: McAfee

Amongst the numerous challenges that Australian SMBs already face, a recent survey by McAfee has found that almost half (44.5 per cent) have experienced some form of cyber attack in the past 12 months.

These threats come in the form of viruses, worms or Trojans with more than half of those affected admitting their company
infrastructure had been attacked in this way three or more times during this period.

Conducted in April 2013, McAfee’s commissioned State of Cybersecurity in Australia SMBs survey revealed there was also a significant threat from within.

One in four SMBs said they don’t have adequate protection from electronic threats and under half (46 per cent) indicated they had experienced security breach or data loss by deliberate sabotage from current or ex-employees in the last year.

So what is an SMB to do?

1. **Make your employees aware of the importance of security.**
   The strength of your company’s security is only as strong as its weakest link. It’s critical that employees are trained on strong password use and avoid dangerous links and suspect email attachments. Weak passwords were the gateway for 76 per cent of network intrusions.

2. **Know the data you’re trying so hard to protect**
   Before you set up protection you first have to know what you’re protecting and where you’re protecting it. Knowing where your confidential information is stored will make it easier for the company to limit access.

3. **Identify and secure the devices your employees use on your network.**
   BYOD is a growing trend in the corporate world by employees, but it could prove to be the weakest point if steps aren’t taken to secure these devices especially if they contain company data. 56 per cent of Australian SMBs admitted to having no protection on their employee’s smart devices.

4. **Protect your networks from all entry points**
   Thanks to our 24/7 connectivity work is a thing you do rather than a place you go so users can link to a company network anywhere and anytime. Protect access to your company network with VPNs (virtual private networks) and firewalls.

5. **Keep your physical devices under lock and key**
   Servers form the backbone of a company’s security system and therefore should be secured behind locked doors along with unused devices that would be used on your network.

6. **Keep your facilities safe and secure**
   Control who can enter your offices and limit access to secure areas granted to authorised employees using a managed entry system.

7. **Use diligence to avoid human error**
   Human error is a key contributor to data loss, with 61.5 per cent of Australian SMBs indicating that this had occurred in
the last year. Make sure your employees understand the risks involved and carry out tasks with care.

8. **Create clear company cyber security policies**
   Make it clear to your employees that there are rules when it comes to usage of your network and sharing information. Employees’ use of social media and email can account for an increase of malware attacks.

9. **Properly dispose of sensitive material.**
   From the low-tech solution of document shredding to the more advanced data shredding, it’s important to responsibly dispose of files and end-of-life devices.

10. **Screen your employees before you hire them**
    Reliable and trustworthy employees are just as important for the security of a company as the strongest firewall. Conduct background and reference checks before hiring new staff members.

So if you’re thinking cyber criminals only target big companies, you’d better think again. More than 75 per cent of data breaches targeted small and medium businesses so it pays to step ahead of the hackers and ward off a potentially crippling cyber attack.

For more information on how to protect your customer visit [www.mcafee.com/smallbusiness](http://www.mcafee.com/smallbusiness)

---

**iappANZ Profile - Matt Poblocki, Director of Legal Affairs, eBay and PayPal, Australia & New Zealand**

What privacy challenges are you dealing with in your current role as Legal Director for eBay and PayPal?
Privacy is an important consideration of everything we do at eBay and PayPal – if you think about it, with PayPal it’s the cornerstone of our product – ie how do you transact online safely, without sharing sensitive details or giving away information that could be used against you for fraudulent purposes (eg credit card details or bank account details). We’re not dealing with any challenges as such but two main issues are:

1. as a global company ensuring we maintain harmonisation of our privacy policies to the extent we can; and

2. being aware of the Australian federal privacy regime reforms.

One issue to call out is the different approaches that different generations have to privacy in an online world and reconciling them. With such vast and diverse user bases across eBay and PayPal globally we have to always consider the customers’ expectations for privacy too - and these expectations are evolving. So in addition to the legislated privacy obligations in the different jurisdictions it’s important to stay across these customer expectations. A global company should also factor in the highest privacy standards from a
jurisdictional perspective when determining where to set its privacy benchmark and policies.

Australian national privacy reforms – have we got it right?
I think Australia is heading in the right direction but we’re certainly not at the stage where say the European Union is. The internet has thrown a lot of challenges at privacy and other areas of law. We have to see privacy in a global context now and not just limited to Australia. The proposed legislation starts to address that new paradigm with reforms like ensuring accountability for entities which partake in cross-border data flows and enhanced enforcement powers as a deterrent. These reforms are a good thing for consumers and a step in the right direction. In that context whether we’ve ‘got it right’ or not needs to be judged against the fine balance between enabling domestic and global commerce on the one hand and protecting the rights of our citizens on the other. That can be a tough balancing act. At the end of the day better and clearer customer privacy disclosures and consents can be the right way to start addressing some of these challenges.

What are you reading at the moment?
Carl Sagan’s final work - Billions and Billions, Thoughts on Life and Death at the Brink of the Millennium. Sagan was a true visionary, awesome scientist and communicator with a poetic way for describing the cosmos. He’s a real inspiration.

Ideal Asia Pacific city and why?
That’s a tough one as APAC has so much to offer and is so varied. Technically it’s in APAC and I’d genuinely have to say Sydney, as it is such a great place to live. There are so many unique cities in APAC offering differing experiences but as I’m forced to pick one I’ll pick Hanoi – the richness of food is a big draw card for me and I’m slightly addicted to pho.

Tell us about a good conference you have attended or spoken at recently.
I have to say the most recent conference, our PayPal Leaders’ Day, in the US was inspiring. It focussed on PayPal going into the future and culminated in a ‘fireside chat’ discussion between our president, David Marcus, and second man on the moon Buzz Aldrin. It was also announced at SETI the next day that PayPal would be pushing for space with PayPal Galactic (check out the blog) but it’s all about forging a new economy in space and exploring space regulation.

What advice do you have for your fellow privacy professionals?
I think a challenge for privacy professionals sometimes is getting the message out there to their internal clients and stakeholders first, ie driving business awareness. Everyone has their own view on privacy matters and how far obligations should and do extend – it’s important to tap into that so you can advocate the need for privacy and have the business keep it front of mind in what they do. Make it relatable, make it relevant and engage the business so they automatically think privacy first in what they do.
What do you see as the emerging issues for privacy online?
I've touched on some of these themes, at a high level at least, in my earlier answers. It will be interesting to see how or if there are any changes or developments in respect of “express consent”. With the rapid developments in computer technology, and the fast way people communicate with each other, I think notions such as what constitutes adequate “consent” and notice are still to be refined and again they’ll evolve as technology usage evolves – and they don’t often evolve in harmony. Customers don’t necessarily want to read a 5 page document on privacy, just to buy a $10 iPod cover for example. A lot of online commerce exposes the tension between what customers want (ease of use) and what legal requirements there are to protect them in their need to transact simply and quickly. I think we’ll also see cloud storage providers present more challenges, ie offshore data and enforcing Australian rights where there may not be an Australian nexus. Geotracking and ‘big data’ initiatives will continue to generate questions of how far organisations can go in leveraging customer data and sharing that with third parties or how broad the purpose of sharing can really be. We’ve seen all that play out in the recent past with social networking and search engine platforms.

Favourite app and why?
Star Walk! Try it – it’s amazing. I think I’m seeing a space theme emerge here…

Ideal job?
At the risk of sounding cheesy I’d say I have it – it’s challenging, dynamic and enriching to be dealing with legal and regulatory challenges in the fast moving worlds of ecommerce/commerce and payments/financial services. Other than that I’d say Richard Branson has a great ‘job’ but it’s not really job – more a lifestyle.

Matt has been in the world of online law and regulation for over 8 years and is responsible for legal affairs across the eBay Inc group of companies in Australia and New Zealand, including Gumtree and ebay Commerce Network. He is the Legal Director for PayPal Australia and Director of Legal Affairs for eBay Australia & New Zealand.
Richard Thomas CBE LLD
Richard was the UK Information Commissioner from 2002 to 2009. He held independent status with a range of responsibilities under the Freedom of Information Act 2000, the Data Protection Act 1998 and related laws. The functions of the Information Commissioner’s Office (ICO) include promoting good practice, ruling on complaints and taking enforcement action.

He is currently part-time global strategy adviser at the Centre for Policy Leadership (CIPL), the data privacy and information think-tank associated with the Hunton & Williams law firm. His has previously worked as Director of Public Policy at Clifford Chance; Director of Consumer Affairs at the Office of Fair Trading, Head of Public Affairs and Legal Officer at the National Consumer Council and a solicitor with the Citizens Advice Bureau Service and Freshfields. Since September 2009, he has also been the part-time Chairman of the Administrative Justice and Tribunals Council (AJTC) which independently oversees the arrangements for resolving disputes between government and individuals.

In 2008 he was awarded “Privacy Leader of the Year” by IAPP and was voted 3rd in Silicon.com’s global “IT Agenda Setters” poll. In July 2009, he was included in the “Law 100” - the London Times list of the 100 most influential British lawyers. In June 2009, Richard was awarded the honour of Commander of the British Empire (CBE) for public service.

Extract:
Nightmare in Downing Street: The day when the British government lost 25 million child benefit records on two discs was a turning point for data protection and for my term as Information Commissioner. For longer than anyone could have imagined, this and other data breaches which came to light at the same time, dominated the headlines and the political agenda. It led to much stronger enforcement powers and sanctions and changed the attitudes of both data users and consumers. Things got better for a while, but sadly things have continued to go wrong in too many quarters.

What’s been happening with data breaches in the UK and elsewhere? Who might be next? What are the real risks? What should data users be doing? What can laws achieve? What cannot be done by laws alone?

Danny Weitzner
Danny is a Director of MIT Decentralized Information Group and Principal Research Scientist at MIT Computer Science and Artificial Intelligence Laboratory, Cambridge, MA in the US. He is IAPP Privacy Professional of the Year winner for 2013 and was the United States Deputy Chief Technology Officer for Internet Policy at The White House between 2008 and 2012 having worked as a member of the Obama-Biden Presidential Transition Team during the election in 2008/early 2009, leading efforts on the Consumer Privacy Bill of Rights and the OECD Internet Policymaking Principles agreement now endorsed by 24 nations. He has been invited to give testimony before the United States House of Representatives, Committee on Energy and Commerce, Subcommittee on Commerce, Trade and Consumer Protection on the Do Not Track Privacy Legislation and the Senate Judiciary Committee, Subcommittee on Human Rights and the Law on Human Rights Challenges Facing the Technology Industry.

His cv is extremely impressive and we could not do it justice here. Come and see and hear him for yourself at our Privacy Summit to learn about the need to
redouble our efforts to find greater interoperability among different privacy regimes across the world.

Mikko Niva
Mikko is Director of Privacy at Nokia Corporation. He is responsible for the operational management of Nokia’s privacy compliance program as well as Nokia’s group-wide privacy policies and requirements for consumer and employee privacy practices. Mikko oversees and supports various consumer and employee privacy-related activities, from strategic advice to product creation to privacy impact assessments. He regularly participates in various privacy-related regulatory working groups and comments on legislative proposals. He is a member of the IAPP European Advisory Board. Mikko is a lawyer by training.

Extract: “In today’s connected world, data and trusted user relationships have become key assets. Successful management of privacy and security are crucial enablers for organizations to optimize their data processing practices while ensuring continuous trust of their users.”

We look forward to hearing Mikko explain the rigorous steps Nokia has taken to improve the maturity of its privacy program and to implementing an accountability based privacy program on global scale to ensure privacy by design. This includes developing a pretty interesting group wide training and awareness approach and reaching out to international standardization bodies such as ISO and W3C with a proposed approach to incorporate privacy considerations into technology standardization.

Win a cash prize: iappANZ’s writing prize 2013

iappANZ is very excited to announce the launch of a new [$250 cash] writing prize for an article that is published in our monthly Bulletin between February and October 2013. Anyone can enter (you don’t have to be an iappANZ member), simply by writing and submitting an article between 500-1500 words that tells us something interesting, new and relevant about privacy. Opinions are most welcome but nothing too extreme.

All articles must be submitted by email, preferably in Word, to [kate.johnstone@suncorp.com.au or an iappANZ email] by 20 October 2013. We will need the author’s email address and contact number. You can submit as many articles as you like. Click here for more details.

The winner will be announced at our Privacy Summit on 25 November 2013 and their name and details will be published on our website. [We also hope to publish profile of the winner in our Bulletin].

So alert your network and get writing!
More details about the writing prize if you are interested:

- Our Editorial team, Kate Johnstone, Veronica Scott plus President Emma Hossack and Past President Malcolm Crompton, will decide on the winner whose article they judge to be the most interesting, original and relevant to our members.

- Articles submitted and published in the February, March and April Bulletins will also be eligible for the prize – we don't want anyone who has already made a valuable contribution to miss out.

- Some people won't be eligible for the prize (sorry!). They are: iappANZ board members, contractors and employees and their family members.

- After the winner is announced we will notify them and arrange for the prize to be delivered to them if they are unlucky not to be at our Summit.

- There will (sadly) be one prize only. Its value is AUS$250, so that's pretty good really.

- We may need to verify the winner's identity so we don't give the prize to the wrong person.

- If the prize is not claimed for any reason (and we hope this won't happen) the author of the runner-up article as judged by the Editorial team will receive the prize.

To make sure things go smoothly and fairly (and we are sure they will) we just have to say that our decision in relation to any aspect of the award of the prize, including the content and publication of submitted articles, is final and binding and not up for discussion.

**Upcoming Privacy Events**

<table>
<thead>
<tr>
<th>Date &amp; Details</th>
<th>Information</th>
<th>Price</th>
</tr>
</thead>
</table>
| **Wednesday 31 July** | Join us for a practical iappANZ workshop about embedding privacy and information security in your organisation on 31 July in Sydney.  
Office of the Australian Information Commissioner (OAIC)  
Room 1, Level 3  
175 Pitt Street  
iappANZ presenters include industry leaders and privacy professionals Joel Camissar, Peter Leonard, Kate Reynolds and Samantha Yorke, introduced by Timothy Pilgrim, Australian Privacy Commissioner. | Registration is FREE for iappANZ members and $99+GST for non-iappANZ members. It is essential to reserve your seat however. Please fill in your details below. If you are a member, your registration information will be |
The Australian Cyber Security Forum is the only dedicated independent cyber security conference in Melbourne, targeting senior IT and security managers with the latest tools, strategies and best practices needed to stay ahead of the rising cyber threat landscape. As a member of iappANZ you will receive 10% discount on verification of your membership. For more details see: [http://www.aventedge.com/event-details/?eid=164](http://www.aventedge.com/event-details/?eid=164)

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Location</th>
<th>Event Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monday 26 August from 9am to 5pm on Tuesday 27 August 2013</td>
<td>Melbourne</td>
<td>The Australian Cyber Security Forum is the only dedicated independent cyber security conference in Melbourne, targeting senior IT and security managers with the latest tools, strategies and best practices needed to stay ahead of the rising cyber threat landscape. As a member of iappANZ you will receive 10% discount on verification of your membership. For more details see: <a href="http://www.aventedge.com/event-details/?eid=164">http://www.aventedge.com/event-details/?eid=164</a></td>
</tr>
<tr>
<td>Thursday 29 August 2013 2.30pm</td>
<td>Queensland Health, 147-163 Charlotte St, Brisbane</td>
<td>HEALTH and Privacy training</td>
</tr>
<tr>
<td>Monday 30 September 2013</td>
<td>Sydney</td>
<td>Overseas Transactions and the APPS A free member training session to be held at the OAIC Sydney Free</td>
</tr>
<tr>
<td>Wednesday 18 September 2013</td>
<td>Melbourne</td>
<td>ISACA Security and Privacy Conference Melbourne. To be held at PWC. More details later this month Free for iappANZ members</td>
</tr>
<tr>
<td>Late October 2013</td>
<td>Melbourne</td>
<td>The new credit reporting provisions TBA</td>
</tr>
<tr>
<td>Wednesday 12 February 2014</td>
<td>OAIC Sydney</td>
<td>The Big Wrap up on the new Act all at OAIC Sydney TBA</td>
</tr>
</tbody>
</table>
Recruitment

Standard Chartered Bank is hiring 2 Global Privacy Analysts in Singapore

Working in the Bank’s Data, Technology & Operations Group L&C (DTO L&C) team based in Singapore and London, the role holder will, as a member of a bigger team of lawyers and privacy professionals of varying seniority, be responsible for corporate oversight of privacy policies, practices and procedures across global operations.

This role will be a key resource in the Global Privacy Programme and serve as a data privacy consultant to in-country and global business lines, and support functions (e.g., information technology and human resources) by providing expert advice and guidance across the Bank on all strategic privacy projects and on BAU projects and requirements.

Please click here for a detailed description.

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

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

FIND OUT MORE at: