“Companies which do not get privacy right are going to face real problems in the years ahead. They should see it as a matter of enlightened self-interest. It’s all about reputation.” Richard Thomas CBE and Keynote at our iappANZ Summit Sydney, 25 November 2013

The new look “Bulletin” is our first attempt at copying Vogue with what is well-known following the movie as the “September Issue”. Whilst we don’t feature fashion, our subject of privacy has in Richard Thomas’s words “almost become sexy”, and we do for the first time have some stunning visuals, and a lot more content than a fashion magazine! Packed with advice, profiles and reflections on many of the different privacy issues we all tackle daily I hope you find this month a good read. You may have noticed there is a blank for the name on the cover – we are re-naming the Bulletin and would love your ideas. Please send them to me, and we will draw the winning entry at our Summit. Send your ideas through.

It is less than 2 months until I hope to meet you all at The Westin for our Privacy Summit 2013. Registration is open and the early bird closes soon as our registration price has not increased as we aim to provide you our members with the best value for money from any privacy Conference you will ever attend. This month there is pieces Don’t forget to submit your article to go in the running for the iappANZ inaugural Writing Prize which will be announced at the Summit.

This month we welcome 2 new Gold sponsors to iappANZ. Facebook, which needs no introduction and AvePoint which have provided a piece inside the covers. iappANZ is delighted to work with two such high profile players in our industry.
As usual we encourage all of our Australian and New Zealand members to submit articles of interest to our Bulletin. This month I am delighted to have both a profile and article of great interest by Tom Bowden, CEO Healthlink. Keep the articles coming New Zealand!

Our Board will change from November 25 at the Annual General Meeting, which will take place immediately following the last session at the Summit and before the Cocktail party. You could be one of the new faces for 2014. It is a lot of fun and I can guarantee you will learn a lot and meet some extraordinary people. Please consider nominating and let me know if you have any queries whatsoever. My details are below.

October brings our next Workshop, all you need to know about Credit reporting and if credit reporting is not your area of interest, tell us what is on our Social Media. Get connected and join us at LinkedIn: http://www.linkedin.com/groups?qid=1128247&trk=anetsrch_name&qoback=.gdr_1281574752237_1

Follow us on Twitter at: https://twitter.com/iappANZ

Finally, if you are not already subscribed to our iappANZ Weekly Dashboard, join up to get a review of Australia and New Zealand’s top privacy news stories, subscribe now at https://www.privacyassociation.org/publications/subscribe/1773

Five Questions for the Commissioner
Guidelines to the Australian Privacy Principles
By Melanie Marks
Treasurer of iappANZ and Privacy Manager
National E-Health Transition Authority (NEHTA)

The Privacy Amendment Act introduces a harmonized set of privacy principles known as the Australian Privacy Principles (APPs) which will regulate the handling of personal information by Australian government agencies and businesses. The APPs will replace the existing Information Privacy Principles (IPPs) that currently apply to government agencies and the National Privacy Principles (NPPs) that currently apply to businesses. The APPs will be in force from 12 March 2014. A number of the APPs are significantly different from the existing principles, including APP 7, on the use and disclosure of personal information for direct marketing, and APP 8, on cross-border disclosure of personal information.

To assist organizations and agencies to understand their obligations and how it intends to administer the changes under the APPs, the Office of the Australian Information Commissioner has recently released a draft set of Guidelines about the APPs. The draft Guidelines covers APPs 1-5 as well as “key concepts” and other general matters. Public consultation on this draft concluded on 20 September 2013. At the time of publication, the release of the draft APP Guidelines covering APPs 6-11 was expected imminently with the remainder to follow in due course. With many of our members currently in the process of reviewing their data handling processes and procedures to ensure compliance come March 2014 (and advising their clients on the same), the iappANZ took the opportunity to speak with Australian Privacy Commissioner Timothy Pilgrim about the Guidelines and what can be expected in the second part of the consultation.

---

1 If you’d like to know more about how data offshoring is addressed under APP8, attend our free seminar “Data Inflight - the ins and outs of offshore outsourcing” on 30 September 2013. See the iappANZ website for more details.
1. Can you give us a sense of the types of issues that stakeholders commonly raised in relation to the consultation on the first part of the draft Guidelines?

We are still in the consultation phase and we are expecting more submissions to come in over the next few days but at this stage we have noted issues being raised about:

- **APP 1** — How agencies and business can develop clear and transparent privacy policies that are tailored to best meet the needs of their clients.
- **APPs generally** — How the APPs will be interpreted in light of rapidly developing technology, for example how the APPs apply to data collected on the internet, the regulation of cloud computing arrangements, the use and disclosure of biometric information or biometric templates.

2. What weight will the Guidelines carry once they are finalised and the APPs have commenced operation?

The APP Guidelines are not binding but are issued under guidance related functions set out in the Privacy Act 1988. The Guidelines outline how the Commissioner will interpret and apply the APPs when exercising powers and functions under the Privacy Act. So, from March 2014, I will certainly have regard to these Guidelines when investigating complaints about possible breaches of privacy, providing advice to agencies and organisations about complying with the APPs, conducting performance assessments about whether personal information held by an APP entity is being maintained and handled in accordance with the APPs and considering whether to accept an enforceable undertaking.

3. What is your advice for businesses currently reviewing their practices and procedures to prepare for the upcoming changes?

It is important that businesses start preparing for the changes now. We are now only 6 months away from the implementation of the new laws so time is moving very quickly. In particular, if they haven’t already done so, I would encourage businesses to conduct a detailed review of their current personal information handling practices and policies, to ensure that they are managing personal information in an open and transparent way.

Business should also review the circumstances where personal information can be used for direct marketing, sent overseas, or for credit reporting. For example, in relation to direct marketing, consideration should particularly be given to the availability of ‘opt out’ mechanisms.

Some other key areas to consider are whether the business has a robust internal dispute resolution process and how the business is going to ensure staff awareness of the changes.

The OAIC has published a range of guidance that may assist businesses to prepare for these changes. This includes a Checklist for organisations highlighting changes to privacy principles, issues to consider and suggested actions. We have also published a number of reference tools, fact sheet and training resources.

4. APP 6 introduces a limited number of new exceptions to the general requirement that an organisation only uses or discloses personal information for the purpose for which the information was collected. Can you comment on the new exceptions and why they were introduced?

The new exceptions to APP 6 permit an entity to use and disclose personal information where it is necessary:

- to assist in locating a missing person
- to establish, exercise or defend a legal or equitable claim, or
- for the purposes of a confidential alternative dispute resolution.

There are also a couple of special exceptions for diplomatic/consular functions and some defence activities outside Australia.

The new exceptions authorise but do not require an entity to use or disclose personal information in these circumstances. Each of these exceptions raised complex issues and competing policy considerations. They have been introduced because on balance, the circumstances described in these exceptions were considered to reflect the public interest in allowing agencies and businesses to
perform their legitimate functions and activities. In the Guidelines we have given examples that seek to demonstrate the how the exceptions might apply in practice and which will assist in understanding the limits of the exception.

5. For the first time under Australian law, direct marketing is given its own principle under APP 7. APP 7 provides that organisations may use or disclose personal information for direct marketing purposes where the individual has consented or has a reasonable expectation that their personal information will be used for this purpose, and it provides an adequate opt-out mechanism. How would an organisation demonstrate that an individual has a reasonable expectation that their personal information will be used for the purpose of direct marketing?

An organization will need to assess the reasonable expectations of an individual from the perspective of a reasonable person with no special knowledge of the industry or activity involved. It is the responsibility of the organization to show that a reasonable person would reasonably expect their personal information to be used or disclosed for the purpose of direct marketing.

In the draft APP 7 Guidelines that are available for public consultation, a number of factors are listed that may be important in deciding whether an individual has a reasonable expectation that their personal information will be used or disclosed for the purpose of direct marketing. These include where:

- the individual has consented to the use or disclosure of their personal information for that purpose;
- the organisation’s APP Privacy Policy clearly explains that the organisation collects, holds, uses and/or discloses personal information for the purpose of direct marketing;
- the organisation has notified the individual of the purpose of collection and its usual disclosures (including for direct marketing), in accordance with the notice requirements in APP 5.1; and
- the organisation made the individual aware that they could request not to receive direct marketing communications from the organisation, and they do not make such a request.

Visit the OAIC website for more information about how to make a submission to the consultation on the draft Guidelines. We will bring you more from the Commissioner in next month’s Bulletin.

This seven-meter tall art work, painted in giant white letters on a concrete wall in April 2008, was intended as a criticism of Britain’s Big Brother culture and specifically the prevalence of CCTV cameras.

"One Nation Under CCTV", it screams, from a wall on which a CCTV camera is also mounted.

A child figure perched in a letter appears to be painting the message on the wall, which overlooks a post office yard in Oxford Circus, London.

‘Banksy’ (the creator of the work) started out as a street artist, but his work is now coveted by celebrities and has earned him a lot of money.

Reflections on themes emerging from recent iappANZ Presentations in Melbourne and Brisbane

By Emma Hossack
President
emma.hossack@iappanz.org m:+61411478799

Many discussions have arisen from the iappANZ Privacy Training workshops in Sydney during July and October and Brisbane in September. Melbourne is about to have its turn in October and we are hopeful that the big wrap up in February will include Webinar facilities for our New Zealand members. iappANZ has also presented at the ISACA event held in Melbourne where we spoke with PWC and Norton Rose. The introduction of the new privacy laws, together with the number of published data breaches are breathing new life and interest into the privacy industry. One of our Summit speakers former UK ICO Richard Thomas CBE will be speaking in November about “How data protection became sexy...well almost”- and he has a point. The attendance levels and engagement at our Seminars are proof.

In Brisbane, a panel including Helen Clarke from Corrs, Dr. Richard Kidd (on many AMA, Medicare Local and RACGP Boards) James Kelaher from SmartNet, Dr. Trish Williams from Edith Cowan University and myself discussed the complexities of implementing healthcare and protecting privacy.

“...the concepts of security and privacy in health information systems are distinct but inextricably linked like Siamese twins.”

We discussed this concept with the expertise of Dr. Williams who is the main author of the RACGP Computer Security Guidelines, and it became clear that while it is possible to have a very secure environment with no privacy, privacy without security is very fragile indeed. Dr Williams discussed the challenges for busy clinicians and environments where yellow stickers were frequently used to enable sharing of passwords and access keys where people simply did not have the time or training to adhere to policies making audit trails largely useless. And for those of you expecting an audit, she noted that hiding these stickers under the keyboard will not work – and a sticky screen is a dead giveaway.

In all seminars, the benefits of sharing data appropriately were discussed and the fact that the benefits were significant gave rise to consensus on the need for the best available security. Reference was made to the complexity of the information ecosystem where information is interconnected and processes which were once relatively straight forward like consent, are now a matter for negotiation. The work of the World Economic Forum form earlier this year informed this discussion, and it became clear that it is not just the new privacy laws and penalties which are driving businesses to pay greater attention to privacy, it is actually customer expectations. Note to businesses which fall beneath the $3million turnover threshold – don’t let your competitors get the edge on you by offering superior privacy to your customers. The release of results from the OAIC launch of Consumer Attitudes to Privacy on 9 October will crystallise the need for all organisations to sit up and take notice.

If “Data is the Mine of the Future”, then as Michelle Dennedy CPO McAfee made clear earlier this year in her Privacy Awareness Week Speech, the data value and data risk must be balanced carefully if we are to get the benefits. Security is key in this equation, particularly in respect of sensitive health information as we have seen with many examples of health data breaches both in Australia and overseas. The importance of encryption was highlighted in our Seminar Data in Flight in respect of Australian Privacy Principle 8.

Getting the confidence of the users in security however, is just one part of this equation. When much of the riches of data come from correlations, consent is no longer possible in the traditional format, so the process becomes more one of negotiation. If you cannot tell someone exactly what or when or how you may use their data, there needs to be something in the deal for the individual. The World Economic Forum endorsed the approach by Doc Searles in The Intention Economy, whereby you allow the customers to take charge. In other words instead of surreptitious monitoring and tracking to enable vendors to make a guess at what the customers may want next, arm the customers with the means to tell vendors what they want, where they want it and how much they are willing to pay.

---

1 Robinson, 1996 in Hovegna, E, Kidd M, Cesnick B “Health Informatics and Overview” Melb. Australia, Churchill Livingstone p.77
2 Sam Walsh, Rio Tinto 2013 AFR, Boss Magazine.
As this diagram exemplifies, the concepts and considerations are far from straightforward, and finding creative solutions to enable a fair exchange is not always simple where big data presents big opportunities for data collectors in health and most other fields.

Omer Tene and Polonetsky talk of this as “sharing the wealth” as a concept to replace minimization of data collection and use and access control. This has been called the “featurisation” of data and an example of this has been the “Green Button and “Blue Button” technology introduced by the Obama administration whereby energy and health authorities enabled the aggregated consumer data to be accesses by the consumer so that they can use it for their own management purposes. With our own eHealth environment now so full of exciting new technologies these privacy concepts and their implementation should start to emerge as critical for businesses and governments alike. iappANZ can't claim to have come up with the answers to all of these questions in its Workshops, but feedback like this shows that people are finding the journey worthwhile.

“Privacy concerns are human factors majority do not understand. It is the fact that you must talk to someone first. This workshop just did that.”

“Privacy is not a clearly defined concept, being subject to a number of culturally-dependent variables. Mixing with people like you will help you to understand it.” Dr Tony Sahama

“An eclectic group of experienced professionals spent the afternoon discussing changes in privacy law for Australia. The human factor within IT processes of healthcare delivery was well developed by the group; a great focus group.” Dr Sue Ellen McKelvie
Barnaby Jack and Hacking Humans
By Kate Reynolds - iappANZ Board Director

A tribute to Barnaby Jack & his contribution to the security sector and to a greater extent potential privacy implications.

Earlier this year I had the pleasure of seeing Barnaby Jack, a security professional give a fascinating presentation; *Implantable Medical Devices: Hacking Humans* at the information security conference, AusCERT. I was so intrigued by his work and the potential privacy implications, that I spoke to him after his presentation about the possibility of him flying back to Australia from his adopted home of San Francisco to take part in the upcoming iappANZ Privacy Summit. Tragically, Barnaby, who was originally from New Zealand, passed away two months later at age thirty five.

Whilst he was considered a bit of a celebrity within security circles for a few years prior to his death, Barnaby may be relatively unknown amongst privacy professionals. He first garnered significant attention from the information security community in 2010 as the result of a presentation he gave at the Black Hat security convention. During this he demonstrated how, by exploiting bugs in ATMs he could not only capture personal information from the cards of people who had used them but also get the machines to spit out (fake) cash. In the interests of responsible disclosure, the ATM manufacturers had been advised of the security issues prior to the demo and Barnaby had delayed his presentation after they requested more time to patch the vulnerabilities.

More recently, Barnaby had turned his attention to implantable medical devices. Whilst working for security vendor McAfee in 2011, he showed how insulin pumps could be hacked wirelessly and controlled to administer fatal doses without even knowing the device ID number. He took this a step further the next year at the RSA conference he demonstrated how he could hack an insulin pump more than 90 metres away.

During his presentation at AusCERT earlier this year, Barnaby dispelled a Hollywood myth but probably not in the way that you would expect. Remember that scene in the nail-biting episode of the TV show *Homeland* where Congressman Brody hunts around in the Vice President’s office to find the serial number of his pacemaker to provide to the terrorists who subsequently use this to take remote control of the device and kill him? Did that seem totally unrealistic to you? Barnaby agreed. Echoing comments he had previously made that; “TV is so ridiculous! You don’t need a serial number!” he went on to explain just how it could be done. It’s scary but fascinating and if you are interested in the science behind it, you can read his post “Broken Hearts”: How plausible was the Homeland pacemaker hack? on the IOActive (his employer at the time of his death) blog.

The research work Barnaby did on implantable medical devices will undoubtedly continue to be highly regarded and invaluable to the industry in improving the security of such devices and hopefully contribute to making such scenarios in the future implausible. His untimely death created a widespread sense of loss with the security community; not just because of the calibre of his work but also his down to earth, unassuming personality which will be fondly remembered by many.

---

2. https://www.computerworld.com/s/article/9179844/Barnaby_Jack_hits_ATM_jackpot_at_Black_Hat?taxonomyId=12&pageNumber=1
4. http://blog.ioactive.com/2013/02/broken-hearts-how-plausible-was.html

---
Your Primer for Addressing Updates to the Privacy Act

By Karen Cheung - Marketing Manager with AvePoint

Unless you have spent the last six months stranded on a deserted island, it is highly probable that you have read that many countries around the world are working to define ways to best manage “Private Information” in the digital age. In Australia, the Privacy Amendment (Enhancing Privacy Protection) Act 2012 will come into effect in March 2014. The new act will, as this author has recently read in the ether, “put some teeth in the toothless tiger”. In other words, it will give Timothy Pilgrim, the Australian Privacy Commissioner, more powers to enforce the 13 Privacy Principles that he and his team will be mandating. Along with the changes, his powers will also be augmented in the areas of: Investigations, Determinations, Enforceable undertakings as well as Civil Penalties. These changes will better protect Australians, as well as foreigners whose data is stored in Australia, from inappropriate disclosure.

These changes, in combination with the general public attitude, has resulted in both public and private organizations addressing the new Privacy Act with vigor and enthusiasm.

So begins the challenge of not just addressing the topics in the Privacy Act, but improving how your organization will manage the risks associated with the collection, use and retention of Private Information. While every organization has its own unique needs and challenges, there are several steps that Privacy Professionals can take to start implementing a framework to addressing the new Privacy Act initiatives.

Understand the business risks

- Despite this new interest in Privacy, it in and of itself is unlikely to drive the business. In an effort to increase your visibility, Privacy Professionals need to be actively involved with their company’s operation lifecycles and integrate good privacy strategies.
- One of the highest risk areas relating to the operation of secure, compliant privacy environments is how to manage Private Information effectively. Most organisations, despite having great business processes, have trouble knowing where Private Information is stored and whether it is appropriately classified let alone who has access to it.

Understand your “information” risks

- One of the biggest challenges most organisations face is understanding where its data resides and who has access to it. More often than not, there is a disconnect between “the business” and “IT” as they both speak very different languages. Privacy Professionals, as well as other management functions, should have a clear understanding of where existing information is located as well as where future data is expected to reside.
- To better understand these risks, organisations should evaluate their current environment by scanning existing data to determine where sensitive data and better gauge just how much risk to which they are exposed.
- These risks should be well documented, and Privacy Professionals should be proactive in keeping the Board of Directors informed of these risks.

Establish governance

- Once you have an understanding of the risks surrounding Private (or other sensitive) data, Privacy Professionals should work with all key organisational stakeholders to review policies and procedures. These policies and procedures should be designed to help ensure that data is always in the right place, appropriately classified and that only authorized people have access to it. These processes should be automated where possible to lower complexity and increase efficiency. To ensure ongoing conformance, these processes should be augmented with associated roles, responsibilities and expected reporting requirements.
- By establishing a clear governance strategy, Privacy Professionals will be able to outline the expectations in which to benchmark compliance. This will enable the organisation to state what they are going to do and, through the automated process, be able to prove it.
Convert risk into funded initiatives

- Once the aforementioned steps have been implemented, Privacy Professionals will be in an optimal position to leverage the governance model and transform their initiatives into funded efforts. It is critical to keep senior management informed of the risks to which they are exposed. This process should be very positive dialog. When collaborating with senior management, Privacy Professionals will be providing them with critical insight that will put them in a better position to understand the value that the Privacy Professional brings and just how important it is to support the initiatives that must be addressed.

Navigating through the implementation of sound processes that meet any Privacy Act requirement can be a tricky, long and colorful journey. AvePoint Compliance Solutions can help Privacy Professionals gain insight into the information stored in multiple repositories, such as file shares, enterprise social feeds, SharePoint, and websites.

By understanding how and where data is stored and accessed thin the above (and other) platforms, organizations place themselves in a strong position to meet the challenges that "new world digital regulations", as well as public expectations, are placing on them.

For more information on how AvePoint can help arm you with the tools necessary to help address the Privacy Act, please visit our website.

Privacy Protection in Europe
By Mikko Niva
Director - Privacy Legal, Intellectual Property & Government Relations with

Dealing with a simple problem is easy. You know what the problem is and you apply applicable best practice to it. Dealing with a complex problem requires a different approach. A prescriptive approach does not work, as there typically are no best practices that directly apply. Instead, organizations need to have in place systematic and flexible measures to identify the issues and to plan appropriate mitigations thereof.

Over time, through experimentation and sometimes competition, these mitigations become emerging practices, then mature into best common practices and standards, while new solutions are being identified to new issues at the same time.

Managing privacy has rapidly become a very complex problem. More and more products are processing personal data. User data has become a valuable business asset. New technologies are bringing about completely new types of privacy threats and problems and often there may not be any best practices to apply.

The risks of not doing it right have raised dramatically. Collection and use of personal data is today regulated globally. Failures to comply with these regulations are typically heavily sanctioned with obvious economic effects. Consumers, employees, business partners, regulators and other stakeholders expect organizations to manage privacy appropriately.

Nokia manages this complexity and drives towards Privacy by Design through a comprehensive, industry best practice privacy program that is based on the so called Accountability –model. We will explore our approach on e.g. the executive oversight, training and awareness building measures, policy and requirements management, privacy engineering and assurance methodology that we use to identify and mitigate privacy threats in often very agile software development environment, staffing and delegation and other such measures that we have deemed necessary to manage privacy in a growingly complex global business and technology environment.
The Profile of Privacy – Higher, but is it Sexy?

By Richard Thomas

Richard Thomas CBE was the UK Information Commissioner between 2002 and 2009. He is currently an Adviser to the Centre for Information Policy Leadership, the think-tank associated with the Hunton & Williams law firm.

When I started as the UK’s Information Commissioner at the ICO in 2002, data protection had a low and negative profile – in the political and legal worlds, in the media and with the public. It was seen as nerdy or irrelevant, with strange language, vague requirements and toothless laws. It almost had a theological feel, with a handful of regulators and cognoscenti talking to each other as the High Priests. Who could ever imagine that “data subjects” meant men, women and children? No wonder that few companies or public bodies were taking it seriously. Worse still, it was great way to duck out of responsibility – “We can’t help you sort out your mother’s bank account because of data protection”. Even worse – until he had to back down - when a Chief Constable blamed data protection for his force’s failure to link previous complaints against the main suspect in the notorious Soham child murders.

If I am frank, I mainly wanted to be Information Commissioner to oversee the introduction the new Freedom of Information law. This duly generated half a million requests in the first four years, transformed the fabric of public life and led to publication of the formal Advice to Tony Blair about the legality of the Iraq invasion and to the MPs’ expenses scandal.

But I quickly worked out that privacy and data protection were destined to have just as much impact as FoI – and for private firms as much as government. Technology and globalisation were about to transform people’s lives – and spread their electronic footprints all over the place. There were real worries about the ways some organisations – whole sectors in some cases - were handling personal information. Scandals were waiting to happen. There was an acute lack of genuinely helpful guidance. My experience as a consumer regulator (in charge of consumer affairs at the Office of Fair Trading, the UK’s ACCC) told me that privacy had to become reputational matter, so that companies in competitive market places really worried about what their customers thought. Likewise employers needed to understand the importance of respecting the privacy of their staff.

What a change over the last decade! Google and Facebook have made something of an appearance. Big Data is everywhere and getting bigger. Privacy issues are now rarely off the front pages, whether it is hacking by tabloid journalists, interception of communications by US spy agencies, or the spread of CCTV cameras - and of course the media just love data breach stories. ICO surveys show the growth of public concern. Numerous parliamentary inquiries and debates have resulted in stronger laws. The issues are now high on corporate and governmental agendas. As the success of IAPP shows, the privacy profession has mushroomed.

At the IAPP-NZ summit in November, I’ll be talking more about the transformation of privacy and the ICO’s part in raising its profile. There are plenty of war stories which raised the temperature – battles over ID cards, warnings about “Sleep-walking into a Surveillance Society”, denouncing the government for losing 25 million child benefit records, exposing the illegal trade in personal information and closing down the construction industry’s blacklist.

I’ll also be discussing what the higher profile means for Commissioners and other regulators – the benefits (and the perils) of media campaigns, being “Selective to be Effective”, how to use carrots and sticks simultaneously, the value of “Naming and Shaming”. Above all, how to get companies to understand why getting privacy right is a matter of enlightened self-interest.

The profile of privacy has come a long way, and will continue to climb. It’s almost become sexy - and the risks are getting greater all the time. We ain’t seen nothing yet.
Making Adherence to Privacy Principles a Source of Competitive Advantage

By Tom Bowden

Tom is the Chief Executive of HealthLink Ltd, one of the world’s largest health information exchanges. He has been involved in a series of international health system comparisons and performed consulting assignments for government healthcare agencies in Australia, Canada and Denmark as well as presenting papers on eHealth strategy at The Commonwealth Fund’s International Symposium on ‘Developing High Performance Health Systems’ in Washington DC.

I have been developing health information exchange systems used by the New Zealand and Australian health sectors for just over twenty years. From the outset, I was acutely aware of the profound importance of maintaining high levels of patient privacy, but it is only recently that I have understood the extent to which incorporating good privacy design principles in any new e-Health system greatly improves its uptake and long-run performance. Because of the ‘obvious benefits’ of greater use of information technology within the health system, everyone is cheering for new Health IT systems to work, provided that they maintain patients’ privacy and deliver some real value. Unfortunately you don’t need to look too far afield to see worthy and well-funded HIT projects that have either failed to get out of the starting gates or are stuck in first gear because patients and clinicians are unconvinced about their ability to manage patients’ information and maintain its privacy to an adequate standard.

We all agree on one thing; Health IT is Important

Clearly every health system is capable of benefitting from better information management. In most countries increased use of information technology is seen as one of the most promising means of increasing health system efficiency. In 2005 the US RAND Corporation recommended rapid adoption of Health Information technology (IT) in order to save the US a likely $81 billion annually and improve the quality of care. The RAND Report gave a great deal of impetus to many governments’ plans to invest in healthcare IT. 

http://www.rand.org/news/press/2005/09/14.html Unfortunately merely investing in something does not guarantee success and not all of the countries that have expended considerable sums on health IT initiatives have achieved worthwhile results. Some countries have done well, some have failed and in other countries, such as Australia, the jury is still out. One of the major factors that determines a health IT investment’s success or failure is the level of trust the system engenders. A key reason behind the failure of the United Kingdom’s National Programme for Health IT was the widespread perception that patients’ health information would be eventually be compromised.

Strategic Options for Record Sharing

So what does a patient record system that is designed to protect patient privacy look like? In my experience, there are two broad strategic options. The first, a system with terrific security, where information is inaccessible except to those who are authorised to get it, the second, a system in which the only access patient information, from its source (point of origin) is on an ‘as needed’ basis. These are two quite different paradigms and it is fair to say, that there is as yet no agreement as to which of them is best and under which circumstances either or both of them can be made to work.

The majority of shared electronic records systems focus upon aggregating data either in a central database or in multiple feeder repositories and then securing it to the maximum extent possible. My own preference however is for systems in which information is requested from the source, only when needed. In some instances it makes sense to aggregate data, for example when a patient is enrolled in a chronic care management programme. However, for utilizing previously generated, general patient records, I believe it makes most sense to leave the original records under the stewardship of the clinicians that create them and ensure that they can be accessed quickly and reliably when needed. In particular I am advocating that primary care clinicians’ electronic records systems become the primary source of most patient information; especially information generated in the community (as opposed to hospitals).

Is Privacy Still Important in the Internet Age?

Until quite recently many of our challenges have been in developing technology capable of meeting our information management needs. However, technological advances have moved ahead rapidly. We have as much technology as we could wish for. We have 3G and 4G, ultra fast broadband, limitless cheap data storage capacity, i-phones, i-pads, RFID, the list goes on and on.
However one thing that has not changed is the vital importance of managing patient privacy very carefully and sensitively. Earlier in 2013, some colleagues and I surveyed New Zealand’s 1150 general practices. We established that the overwhelming majority of practices view privacy as being important now as it ever was. However, many of the people that are making our IT decisions are telling us that privacy no longer matters. For example; “Consumer privacy issues are a red herring. You have zero privacy anyway. Get over it.” - Scott McNealy - chief executive officer of Sun Microsystems in 2002. And “The Age of Privacy is Over” – Facebook founder Mark Zuckerberg in 2010. We are also told quite often that attitudes toward privacy are changing, that there is a “generational shift” and that one day information privacy won’t matter to anyone. However, I don’t believe that and nor it seems do most general practices.

The of Health Information Privacy – A Battle of Warring Paradigms

Looking at the state of play with respect to health information privacy, I am coming to a view that we are engaged in an important philosophical battle, between technologists who are focused on creating faster, more efficient, cost-effective and easy ways to do things and sociologists, who are eager to use technology to improve delivery of healthcare but not at the cost of basic human rights; especially privacy. I believe that the battle for dominance between technologists and sociologists has only just begun, but it is as important a battle as any ever fought. Until protection of privacy is recognized as a fundamental precondition to patient information sharing, we will be unable to make progress at the rate we need to. It is a battle we have to win.

There is no doubt in my mind that one day, one of the key differentiators used for evaluating health records systems, will be the degree to which competing systems can be shown to be competently managing patients’ privacy.

AvePoint

Introduction

We are pleased to welcome AvePoint to iappANZ as a new Gold Sponsor. AvePoint helps more than 10,000 organisations to enable enterprise collaboration with confidence, while meeting needs of privacy, security and accessibility. AvePoint is a corporate member of the International Association of Privacy Professionals. The company’s compliance and risk management practitioners participate in International Standards bodies, including the W3C and United Nations Internet Governance Forum in addition to providing privacy guidance and expertise to a wide range of domestic and international government agencies and corporate organisations.

AvePoint joins us at such a crucial time for privacy professionals. With the Privacy Amendment (Enhancing Privacy protection) t
Personal computing has grown in leaps and bounds over the last decade. It has actually accelerated after the “dot com” boom of the early 2000’s. With the availability of enterprise grade compute resources now accessible for consumption through mobile and hand held devices for personal use has ushered an era where the volume of private information and data stored online has increased exponentially.

For enterprises the increased usage of cloud computing services where customer data is increasingly stored external to the organizations physical and logical boundaries creates a complex web of responsibilities and accountabilities.

We now live in a connected world and the age of “Big Data”, where online and electronic transactions are the order of the day and all transactions are stored by organizations with whom we interact. The stored is used by organizations to analyze behaviors and patterns that help them improve their understanding of customer behaviors, which in turn assists in the provision of improved services.

The phrase "scientia potentia est" (or "scientia est potentia" or also "scientia potestas est") is a Latin aphorism often claimed to mean "knowledge is power". "Big Data" provides ingredients to harvest knowledge and like a bank vault databases that store personal information, multiple facets of personal information are targets for criminals who harvest personal data to then undertake criminal activities using false identities generated from compromised data sources.

Both government and private sector entities have recently suffered data breaches, 2013 EverNote and Yahoo, 2012 Apple, 2011 LinkedIn, Sony, 2010 St George Bank the list goes on. The scale and impact of these data breaches from the number of data records compromised has been significant.

Without mandatory data breach notification legislation can organizations be trusted to do the “right thing”? This still remains to be seen. Obviously once a breach is identified and reported in the media there are existing privacy laws that provide legal protections but where an organization chooses to not report the breach a gap exists.

There is still some distance that is required to be covered to implement the “Australian Privacy Breach Notification” however once its there, appropriate guidelines will be required to be developed in support of the legislation, which in broad terms will provide guidance on how the legislation will be interpreted.

A companion guide of prescriptive controls across people, process and technology domains will be required to be developed that provides clarity to organizations on what constitutes privacy data in its various permutations and combinations.

Readily available standards that provide that level of prescriptive controls guidance are Payment Card Industry Data Security Standard (PCI DSS) and the Australian Government Protective Security Policy Framework (PSPF) supported by The Australian Government Information Security Manual (ISM). Whilst the "Australian Privacy Breach Notification" once approved will enhance the security posture of PII and citizen data held within organizations, in the absence of workable guidance on how it should be implemented there will be a gap in application and the potential safeguards this legislation is looking to provide will be reduced.
Privacy Practitioner Profile
TOM BOWDEN
Co-Founder of HealthLink - New Zealand
By Veronica Scott, Special Counsel - Minter Ellison Lawyers

Tom Bowden co-founded HealthLink in 1994 and has led the organisation since that time. Tom has direct responsibility for leadership, strategy development, marketing and public relations with the aim of lifting government and funder awareness of the value that Health System Integrators create in making health systems more efficient (as in New Zealand and Denmark). Tom gained an MBA from Auckland University in 1993 and is currently studying part time for his PHD. HealthLink is a health-system integrator. Their key purpose is to enable medical practices to communicate electronically with the rest of the health system. By exchanging clinical information healthcare providers become more efficient and they are able to improve the quality of care they can provide their patients.

Here we ask him a few questions around HealthLink, Privacy and about himself.

1. Can you tell our members about the work that HealthLink is doing?
   HealthLink is a Health-system Integrator that connects 10,000 medical organisations in three countries (Australia, New Zealand and Canada). Each year approximately 60 million pieces of clinical information travel across its networks.

2. How near are we to a nationally integrated electronic health system?
   Until we come to understand that the most valuable use of IT in healthcare is in linking systems locally, we will continue wasting money trying to build systems that are not needed nor wanted. In my view we are a considerable distance from building a truly useful health IT infrastructure, though New Zealand is certainly well ahead of Australia in that respect.

3. What are your favourite app(s) and why?
   I don’t really have a favourite app. I make very limited use of smart-phone apps and I won’t let my children put anything on my phone as they consistently snarl it up, making it unusable. For me, my phone is first and foremost a business tool. My children have taken my iPad and I haven’t seen it for months. I am not an IT geek.

4. New Zealand has been noted as an overseas jurisdiction with high standards of privacy protection. What aspects of the privacy regime do you see as being crucial to that?
   New Zealand’s privacy rules are similar to those prevailing in other countries; the same concepts of appropriate use, consent, disclosure have been key to progress. What is different in New Zealand is that we have developed advanced health information systems that are used very extensively. The average NZ general practice exchanges information with 65 other organisations each month, whereas the average Canadian general practice with four and the average Australian practice with eight. Understanding privacy at all levels across the health system has enabled that.

5. How do you see New Zealand organisations dealing with the privacy challenges of using cloud services?
   I think that as long as privacy principles are consistently employed and appropriate levels of encryption and security are used, it doesn’t matter whether data is stored under your desk or in a server centre in Outer Mongolia. Privacy is critically important wherever patient data is stored.

6. What books are you reading at the moment?

   ‘Wired to Care’ by Dev Patniak
   -how companies prosper when they create widespread empathy – Quite a worthwhile take on business philosophy, it’s all about alignment of ethics and attitudes.
And

‘No Mercy’ by Eleanor Learmonth and Jenny Tabakoff
True stories of disaster, survival and brutality It is about understanding why behave well even under significant pressure.
I can only read novels when I am on holiday.

7. Can you share with us some of the achievements that have been experienced by some of HealthLink's clients through integration?
We have been working very hard on developing online referral systems in which hospitals and other secondary-care providers publish referral templates that can be automatically populated by general practices’ EMR (electronic medical records) systems. These systems are really taking off and are enjoying widespread use, they revolutionise the ‘transfer of care’ between one provider organisation and another.

We are also pretty keen on CareInsight, a system we have jointly developed with DrInfo, another New Zealand company. CareInsight enables after-hours physicians to query general practice and pharmacy systems and upload current details of patients’ condition, prescriptions, allergies. It is an extremely useful system to have late at night with a sick patient in front of you. Knowing a patient’s precise medical history, current medications and similar key data makes an excellent starting point to an emergency consultation. It is helping a huge number of patients on a daily basis.

8. Working as a privacy professional- what tips do you have?
Be very clear about the key issues; purpose for collection, consent, legitimacy of re-use and communicate in those terms. Don’t over-complicate it. After all, good privacy is just applied common sense.
Be clear about why we are doing it; an individual’s privacy is important to them, we cannot progress use of information technology unless we can engender confidence that privacy will be protected, society won’t let us and for good reasons.

9. Big data is seen as the next frontier in Analytics. What are your views and how can we balance the privacy priorities with the benefits.
I think that it will be very important that we can properly annonymise any aggregated patient data and that isn’t as simple as it sounds. Also I’d urge ‘making haste slowly’ i.e. not merging large databases from multiple sources in the first instance but focusing on data analysis within organisations (which is in my view, where most patient data should be retained).

10. Building the business case for privacy by design is the message getting across?
I hope so! Certainly, in New Zealand we are making good progress in developing systems that improve patient care. By and large, the successful systems follow the key privacy by design principles.

"The guy with the weird skin disease forgot to sign the privacy forms."
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.

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.

Watch this space for new positions with the OAIC

The OAIC brings together in one agency the functions of information policy advice and independent oversight of privacy protection and freedom of information. Its vision is a community in which government information is managed as a national resource and personal information is respected and protected. If you would like to work with the OAIC or to find out what positions are currently available, how to apply for jobs, and conditions of employment at the OAIC keep an eye on our recruitment section here. The OAIC welcomes applications from the diverse Australian community including Aboriginal and Torres Strait Islander people and people with disability, people of all ages and those from culturally and linguistically diverse backgrounds.

For more information go to the OAIC website.
# Up coming Privacy Events

<table>
<thead>
<tr>
<th>Date &amp; Details</th>
<th>Information</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wednesday 9 October 2013</td>
<td>Launch of the 2013 Community Attitudes to Privacy survey results</td>
<td>Free for iappANZ members</td>
</tr>
<tr>
<td></td>
<td>For more information follow the link</td>
<td></td>
</tr>
<tr>
<td>10.30am–12:00pm.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Please join us for morning tea from 10am</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Commonwealth Bank</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Colonial Theatre, Level 20, 201 Sussex St, Sydney</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Launch of the 2013 Community Attitudes to Privacy survey results</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>For more information follow the link</td>
<td></td>
</tr>
</tbody>
</table>

**Monday 21 October 2013**  
**“Earn Your Credits – Understanding the prohibitions, obligations and rights of the new Credit Reporting System”**

Minter Ellison Lawyers  
L23, 525 Collins Street  
Melbourne, VIC 3000

**Monday 25 November 2013**  
iappANZ Privacy Summit  
For more information on our World Class Speakers and networking event, and to catch the Early Bird prices, follow the link  
More on how to register coming soon. Please contact our GM Emma Heath at [emma.heath@iappanz.org](mailto:emma.heath@iappanz.org) for more information or to register early.

**Wednesday 12 February 2014**  
The Big Wrap up on the Privacy Act  
TBA

OAIC  
Room1 Level 3  
175 Pitt Street (nr crnr King St)  
Sydney
IAPP Certification

Privacy is a growing concern across organizations 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 recognized 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.


Join us on LinkedIn or follow us on Twitter

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?qid=1128247&trk=anetsrch_name&qback=qdr_1281574752237_1

Follow us on Twitter at: https://twitter.com/iappANZ