PRIVACY UNBOUND

ISSUE 74
SEPTEMBER / OCTOBER
Privacy Unbound is the journal of the International Association of Privacy Professionals, Australia-New Zealand (iappANZ),

If you have content that you would like to submit for publication, please contact the Editors:

Veronica Scott
veronica.scott@minterellison.com

Carolyn Lidgerwood
carolyn.lidgerwood@riotinto.com

David Templeton
David.Templeton@anz.com

Please note that none of the content published in the Journal should be taken as legal or any other professional advice.

CONTENTS

PRESIDENT’S LETTER

VICE PRESIDENT’S FOREWORD

"OPENING NEW TERRITORIES FOR PRIVACY": 38TH INTERNATIONAL CONFERENCE OF DATA PROTECTION & PRIVACY COMMISSIONERS

NOVEMBER - A BIG MONTH FOR PRIVACY, AND DE-IDENTIFICATION

INDIVIDUATION: RE-THINKING THE SCOPE OF PRIVACY LAWS

THE PURSUIT OF CYBER PRIVACY, A LOST CAUSE?

INSURANCE IMPLICATIONS ASSOCIATED WITH MANDATORY DATA BREACH NOTIFICATION REGIMES

INSURANCE & DATA BREACH LIABILITY COSTS

REVISITING THE INTERPRETATION OF PRIVACY PRINCIPLES AND THE RULES ON COLLECTING PERSONAL INFORMATION FROM SOCIAL MEDIA
Welcome to the last Privacy Unbound before the 2016 ‘Trust in Privacy’ Summit and the iappANZ AGM in Sydney on 14th November. At the AGM we will re-cap the previous year’s activities, talking about the plans for the next and electing the new Board and Executive Committee. It would be great to see as many of you as possible there.

I strongly encourage you to consider putting yourself forward as a candidate for the Board. In my four years as part of the team, I have thoroughly enjoyed working with everyone who has been on the Board and our brilliant member volunteers in the various sub-committees. If you’re thinking about standing but have some questions, please feel free to contact me and I’d be very happy to discuss.

For those of you who still haven’t registered for the Summit, get in quick as places are very limited. This year we have one full day with a fantastic program of local and international speakers followed by a second half day hands-on workshop ‘Designing Privacy Controls into Projects’ run by Anna Johnston the Director of Salinger Privacy.

I look forward to seeing many of you very soon in Sydney.
Our last journal edition before our largest privacy event this year Trust in Privacy includes a rich collection of editorial pieces from our valued contributors.

Founding President and iappANZ Board Director, Malcolm Crompton gives us a detailed snapshot (together with snaps from Marrakesh) from the 38th International Conference of Data Protection and Privacy Commissioners (ICDPPC). The ICDPPC brings together privacy commissioners and data protection authorities from around the world. Data protection challenges arising from rapidly developing robotics, artificial intelligence and encryption technologies was a topic, among many others.

Anna Johnston, Director of Salinger Privacy shares her views on rethinking the scope of privacy laws, particularly the binary legal structure of ‘personal information’ as a construct to protect privacy. Anna will be leading the second half day hands-on workshop ‘Designing Privacy Controls into Projects’ at our 2016 Trust in Privacy Summit.

Guillaume Noe, Cyber Security Advisor analyses the quest for cyber privacy and the safety versus convenience story underlying our infinite appetite for new technology.

Susan Elias, National Manager FINPRO, Cyber at Marsh Pty Ltd shares an informative piece on the cyber insurance implications of the Mandatory Data Breach Notification Bill, including a potential rise in litigation with an increased scrutiny of organisations cyber security practices.
iappANZ is the pre-eminent forum for privacy professionals in Australia and New Zealand. We are affiliated with the International Association of Privacy Professionals (IAPP), the largest and most comprehensive global information privacy community and resource with more than 23,000 members. We work with public and private entities across all industry sectors in Australia and New Zealand as well as the Privacy Commissioners in both countries.

iappANZ offers our members a wealth of opportunities to expand their privacy knowledge, compliance, interests and networks. Our members in Australia and New Zealand represent some of the best minds in the privacy field, from large public companies and the government sector to not for profit, SMEs and individuals.
"OPENING NEW TERRITORIES FOR PRIVACY": 38TH INTERNATIONAL CONFERENCE OF DATA PROTECTION & PRIVACY COMMISSIONERS
MALCOLM CROMPTON

What's it all about?

This year, International Conference of Data Protection and Privacy Commissioners was held in Marrakesh, in Morocco. The location alone says a lot about the continuing spread of data protection law around the world.

I travelled there from Casablanca on the Marrakesh Express (the elderly among us may wish to look up the Crosby, Stills and Nash song on YouTube and reminisce...).

The Privacy Commissioner of New Zealand, John Edwards, who is also Chairman of the Executive Committee of the International Conference of Data Protection and Privacy Commissioners, and Assistant Commissioner Blair Stewart, ably led the ANZ contingent. Others in the contingent included Elizabeth Coombs, the Privacy Commissioner for New South Wales, David Watts, the Commissioner for Privacy and Data Protection in Victoria and Chris Connolly from Galexia.

As has been the case recently, the Commissioners held a closed session for a couple of days prior to convening the open session.

Details of the conference and program are at https://www.privacyconference2016.org. Ever since the Commissioners’ conference in Sydney in 2003, Commissioners have adopted resolutions on issues that they consider require attention and this conference was no exception. These are all now listed on the long-term website for the conferences at https://icdppc.org/document-archive/adopted-resolutions/.

Some conference highlights

The open sessions of the conference covered a huge range of issues and perspectives. The presentations were extensively captured on video and I hope that they will be posted on the conference website. Without any apology whatsoever, these notes only capture aspects of presentations that I thought were interesting.
Opening Ceremony & Highlights of the Closed Session

The Head of the Moroccan Government and Professor Said Ihrah the Chairman of the Moroccan data protection authority, La Commission Nationale de contrôle de la protection des Données à Caractère Personnel (CNDP) formally opened the conference.

John Edwards then summarised the proceedings of the closed session as set out in the communiqué issued by Commissioners here. The communiqué in particular draws attention to the complexity of responding to demands by law enforcement authorities for ways to access encrypted data and the rapidly emerging challenges of Artificial Intelligence (AI).

John also outlined the resolutions adopted this year by Commissioners which covered:

- Resolution for the Adoption of an International Competency Framework on Privacy
- International Competency Framework for school students on data protection and privacy
- Resolution on Developing New Metrics of Data Protection Regulation
- Resolution on Human Rights Defenders
- Resolution on International Enforcement Cooperation (2016)

Privacy and personal data protection as a driver for sustainable development?

Brad Smith, President and Chief Legal Officer at Microsoft opened this session with a powerful statement of about the Cloud of the future, especially if the world is to attain all the promise of the information explosion and AI. For this to occur, the Cloud must be:

- Trusted
- Responsible
- Global

He noted the impact of the revelations by Edward Snowden and the imperative of rebuilding trust. He considered respect for local law to be an essential ingredient to rebuilding trust. This was one of the reasons that Microsoft has resisted access requests by the US Department of Justice to personal information held by Microsoft in Ireland. On the other hand, collaboration and developing better flow of information globally were essential.

He concluded by stating that "privacy won’t come from building higher walls but instead building stronger bridges”.

Chris Connolly, UNCTAD Consultant and a Director at Galexia drew out some highlights from the 2016 report to UNCTAD for which he had been lead consultant, Data protection regulations and international data flows: Implications for trade and development. The report highlighted the spread of data protection laws but also drew attention to the excessive exemptions that they often included or the silence on how to deal with national security and state sponsored surveillance. The report recommended that any such exemptions be tailored, finite and include rights of redress.

The compliance burden on small business is also becoming a bigger issue, both in the EU with the GDPR and in the APEC economies.

Boris Wojtan, Director of Privacy at the GSM Association gave graphic accounts of the use of mobile phone data to address problems in developing countries, for example it can help track the spread of disease and how a population disperses after a natural disaster.

Giovanni Buttarelli, European Data Protection Supervisor made conciliatory remarks about the need for data protection authorities to recognise the importance of information flows, both within jurisdictions and between them. He lauded the cooperation between the EU Article 29 Working Party and the APEC Data Privacy Subgroup as an example of where officials are seeking to find an appropriate way to facilitate cross border data flows. Further cooperation between jurisdictions required both openness and respect and should not focus on quick fixes.

Elena Donchenko, Deputy Division Head at Roskomnadzor (the Russian DPA) defended data localisation as contributing to data protection, among other things, a view not widely shared by some attending the conference. She considered that Russia’s localisation regulatory regime had settled down over the last year.
Vivienne Artz, Managing Director & Counsel at Citigroup provided an interesting classification of approaches to localisation in different jurisdictions.

Jacob Kohnstamm, Former Chairman at the College Bescherming Persoonsgegevens (the DPA of The Netherlands) summarised the Privacy Bridges program that had been the centre of the 2015 conference of commissioners. He noted that the program had been somewhat overshadowed by the combination of the Schrems decision that invalidated the US-EU Safe Harbor arrangement and the implementation of the GDPR. He was seeking to revive the implementation of the Privacy Bridges process through a side event at the end of the Conference.

How to reconcile security and privacy?

Joseph Cannataci, the UN Special Rapporteur on the right to privacy focused his talk on government surveillance, paying special attention to the UK government surveillance program. He noted that aspects of it had recently been deemed illegal by the UK Investigatory Powers Tribunal. He also condemned the oversight arrangements as insufficient. He would be submitting his annual report to the United Nations the week after the Conference.

In summing up, he strongly advocated the view that data flows without borders, especially in surveillance programs correspondingly “need safeguards without borders and remedies without borders” and to be adequately resourced.

Jim Dempsey, Executive Director at the Berkeley Center for Law & Technology reported on a detailed project being led by the Center on Bulk Collection: Systematic Government Access to Private Sector Data, which will be published by the Oxford University Press in 2017.

Key findings include:

- Increase worldwide in government demands for data held by the private sector
- Existing legal structures provide an inadequate foundation for the conduct of systematic access
- Despite progress in some countries, transparency about systematic surveillance programs is weak
- Data protection laws include exceptions for access for regulatory, law enforcement, and national security purposes
- Relatively little discussion of the complex questions regarding application of human rights to trans-border surveillance or relating to citizens of other countries

The core Human Rights Principles in response to these developments were:

- Legality
- Proportionality
- Accountability

Jane Horvath, Senior Director of Global Privacy at Apple provided a staunch defence of Apple’s move towards end to end encryption wherever possible and its resistance against pleas for weakened encryption. “There is no such thing as a safe back door” because “government demands for back doors puts everyone’s data at risk”. In any event, encryption technologies are available worldwide so the end result would be that only the data of “law abiding citizens would be compromised”.

Technology and Science Trends: what impact on privacy?

Peter Fleischer, Global Privacy Counsel at Google started by pointing out that “Google is an AI first company”. As an example, Google Translate can translate realtime 100 input languages into 100 output languages, which equates to 10,000 simultaneous translations.

In his view, long established data protection principles had stood the test of time. AI however brought sharper focus on the question of “just because we can, should we”.

Mark Rotenberg, President of EPIC (Electronic Privacy Information Center) drew attention to Thomas Edison’s quote that “what we make with our hands, we should control with our heads”.

He then proposed an update to Isaac Asimov’s Rules for Robots:

- A robot may not injure a human
- A robot must obey the orders of a human except (1)
- A robot should protect itself except (1) and (2)
- A robot must always reveal the basis of its decision (“Algorithmic Transparency”) [New]
- A robot must always reveal its actual identity

Digital Education

Isabelle Falque-Pierrotin, Présidente of Commission Nationale d’Informatique et Libertés, France (CNIL) & Conference working group on digital education chair outlined the rationale and details for the International Competency Framework for school students on data protection and privacy that was adopted during the Conference closed session, which can be found here.

Sherry Liang, Assistant Commissioner of Tribunal Services at the Information and Privacy Commission of Ontario, Canada gave an excellent presentation on the education resources the Commission had prepared for Grade 5 (age 10 11), Grade 10 (age 15 16) and Grade 11 12 (age 16 18). They are all available on their website, http://ipc.on.ca. They have worked with education authorities to ensure that these resources integrate with the rest of the education curriculum and while not compulsory, have had wide take up within the Province.
**David Watts**, Commissioner, Office of the Commissioner for Privacy and Data Protection of Victoria gave an excellent presentation on the education and training resources developed for use in that State. They are clearly applicable much more widely and are available free of charge.

The resources include a 40 minute “Online Privacy Training Course”. It has been especially successful in workplaces in regional Victoria. Participants are tested for their understanding as they go. Those who complete the course are awarded a certificate of completion. Participants had given it a 95 percent approval rating.

Resources also included an interactive pdf file on information sharing, including encouraging information sharing in situations of family violence.

Interestingly, they had produced an App available in the Apple Store (but not Android) to help enterprises assess Business Impact Level on privacy and security which had been significantly cheaper to develop than the other offerings.

**Stephen Wong**, Privacy Commissioner for Personal Data in Hong Kong described the major revamp of their website in order to make it more attractive to target population groups, especially the young and the elderly (his family’s response being a major test point). He had also introduced a program of Student Ambassadors for privacy protection in schools. They were also producing videos and other materials and publishing them on social media platforms such as Facebook.

**Elettra Ronchi**, Head of Unit and Senior Policy Analyst, Digital Economy and Policy Division at the OECD reported on the results of the 2015 STI scoreboard. It is available in the OECD PISA 2012 database. This evaluation had been conducted across many jurisdictions. The evaluations had include tests of students’ abilities to judge the trustworthiness of online information sources; comprehension etc using lab simulations. Evaluation had included how children spent their online leisure time.

A major aim of the work was to measure the exposure of children to online risks (ranging from predatory marketing to worse situations). However data on this aspect was still limited.

**Next year: Hong Kong!**

The Privacy Commissioner for Personal Data in Hong Kong will convene the **2017 conference on 25-29 September in Hong Kong**. He has hinted that the conference theme will focus on Artificial Intelligence, one of the hot topics in the Commissioners’ communiqué this year. See you there!
SAVE THE DATE!

iappANZ PRIVACY SUMMIT
TRUST IN PRIVACY

8.30AM - 6.30PM | MONDAY 14 NOVEMBER 2016
DOCKSIDE, DARLING HARBOUR, SYDNEY

The annual iappANZ Privacy Summit is the only event of its kind in ANZ, providing a forum for those working in the privacy arena to connect and enhance their privacy knowledge and consider what the future of privacy will look like. We are delighted to confirm that iappANZ will be hosting its annual Summit in Sydney this year, at Dockside Darling Harbour on November 14th, 2016.

As with previous years, the Summit will showcase best practices, tracks trends and offer guidance on opportunities in the field of privacy as well and thought leadership.

This year’s theme for the Summit is ‘Trust in Privacy’. iappANZ is proud to announce Simon McDougall as its keynote speaker. Simon, based in the UK, is the Managing Director of Promontory’s London office and leads Promontory’s global privacy and data protection practice. A Chartered Accountant, with 16 years of experience in regulatory issues and until 2010, lead Deloitte’s UK Privacy & Data Protection and Payments Regulation teams.

Come and join us, and catch up with fellow privacy professionals for an insightful day full of information and thought provoking discussion on the key issues for privacy in a local, regional and global context, now and into the future.

+ Half-day workshop
Designing Privacy Controls into Projects
Featuring Salinger Privacy’s Anna Johnson
Tuesday, 15 November 2016, 9.00am – 1.00pm
Limited spaces available
The Office of the Australian Information Commissioner is looking forward to two highly significant events this month.

Firstly, on the 14th of November the Australian Privacy Commissioner, Timothy Pilgrim, will open the IAPPANZ Annual Summit, to be held in Sydney. With the past 12 months including some very significant events and issues in Australian privacy, the Commissioner is very much looking forward to discussing some of the key issues of the past year, and the key challenges for the year ahead. It is a year in which we expect a greater focus than ever on privacy in Australian businesses and agencies – with a MDBN scheme now back before the Parliament. The Privacy Commissioner’s update will provide insight into these legislative changes, how they relate to shifting community expectations, and how the principle of transparency can be incorporated into privacy practices to support innovation. The Commissioner will also touch on privacy’s hot-topic of 2016, de-identification, which has gained renewed community and legislative attention recently through the proposed re-identification amendments to the Privacy Act. So it is timely that, just two days after the IAPPANz Summit, the OAIC is hosting a major workshop at the GovInnovate Conference in Canberra. The Commissioner will host a panel with de-identification thought-leaders including Dr Khaled El Emam, Anna Johnson from Salinger Privacy, and Dr Vanessa Teague, who recently made headlines after ‘white hatting’ some potential risks in published Medicare data.

Titled ‘Data sharing and interoperability’, the workshop will provide an in-depth exploration of the legal, privacy and technical dimensions of de-identification. Attendees will gain knowledge from individuals on the front line of de-identification technology and governance. We are delighted to offer IAPPANZ members are 20% off the workshop registration. Simply use the code OAIC16 when you register.
INDIVIDUATION: RE-THINKING THE SCOPE OF PRIVACY LAWS
ANNA JOHNSTON

In Australia, as in many other parts of the world, our information privacy rights turn on the definition of ‘personal information’. If data meets the definition of ‘personal information’, there will be privacy obligations attached to it; otherwise, all bets are off. But is this approach to protect privacy serving us well?

Although certainly a less nebulous term than ‘privacy’, relying on the phrase ‘personal information’ has its own drawbacks, because challenges can be made to its breadth. The components of the definition which are argued about include that the information must be ‘about an individual’, and that the individual must be ‘identified ... or ... reasonably identifiable’.

The full bench of the Federal Court has just heard submissions in the Privacy Commissioner’s appeal against the AAT decision in Grubb v Telstra. In December last year, the AAT ruled that mobile network data is not ‘personal information’ subject to the Privacy Act, because it is ‘about’ connections between mobile devices, rather than ‘about an individual’, notwithstanding that a known individual triggered the call or data session which caused the connection.

You might think this distinction is – as Minister McCormack said about privacy concerns and the Census – ‘much ado about nothing’. (Boom tish!) But as I have noted before, taking such a narrow view of the word ‘about’ is a slippery slope, that could undermine our privacy laws. If banks start arguing that their records are only ‘about’ transactions, not the people sending or receiving money as part of those transactions – or if hospitals claim that medical records are ‘about’ clinical procedures, not their patients – we may as well all pack up and go home. Let’s hope the Federal Court sees sense on this question.

The even more contentious part of the definition of ‘personal information’ is the notion of identifiability: is an individual reasonable identifiable from the information at issue? The flip side of identifiability is the challenge of de-identification.

These debates are an attempt to create clarity from ambiguity: Is it personal information or not? And thus: is it in or out of the scope of the privacy principles? Is it worth protecting?

But increasingly, I am of the view that trying to force the world into this type of ‘personal information or not’ binary legal structure is not helpful. Perhaps, if our objective is to protect people’s privacy, our laws need to grapple with a broader view of the types of practices which can harm privacy – regardless of whether ‘personal information’ is at stake.

The UN’s Special Rapporteur on Privacy, Joe Cannataci, has written about privacy as enabling the free, unhindered development of personality. You could think of privacy as related to the right to self-determination, or as an element of autonomy.

And if you think of the purpose of privacy laws as protecting individual autonomy, we should be ensuring that our laws regulate all types of activities which can impact on autonomy. Because it is individuation, rather than identification, which can trigger privacy harms.

In other words, you can hurt someone without ever knowing who they are.

Individuation means you can disambiguate the person in the crowd. This is the technique used in online behavioural advertising: advertisers don’t know who you are, but they know that the user of this device has a certain collection of attributes, and they...
Gilbert + Tobin - 2016 Australian Law Firm of the year – is currently looking to recruit experienced lawyers to join our commercial technology practice, based in Sydney. We seek to innovate in how commercial lawyers work with our clients and to deliver significant value in maximising opportunities of innovation and digital transformation.

A successful candidate will enjoy negotiating commercial agreements and focussing on data driven businesses. Responsibilities will includes advising on privacy, information governance and risk management and as to data rights. Applicants should possess superior analytical and drafting skills with strong business awareness.

We are seeking lawyers with strong commercial contracting experience (3+ years PQE) with a passion for privacy, data and technology and willingness to embrace continuing change. If you are looking to fast track your career with industry leading technology lawyers we would welcome the opportunity to speak with you.

Should you require any further information please call Melissa Gavagna (02) 9263 4149 or send your CV and academic transcript to mgavagna@gtlaw.com.au.
Individuation can lead to price discrimination, like surge pricing on Uber based on knowing how much phone battery life you have left. Or market discrimination, like Woolies only offering car insurance to customers it has decided are low risk. Or in the world of Big Data, social or government interventions can be triggered by an algorithm assessing your collection of attributes, without necessarily knowing who you are.

Geolocation data likewise offers high rates of individuation, even without identification. I have written before about how privacy harms could arise from using geolocation data to figure out the likely home address of people who have visited a strip club or an abortion clinic. Individuals could be targeted for harm, without the perpetrator ever knowing who they are.

The Facebook / Cornell University ‘research’ project on emotional contagion offers another fine example of causing privacy harm, without ‘personal information’ being involved. Although the researchers argued that no personal information was at stake (and, thus in theory there were no privacy impacts) because they did not know who their research subjects were, they deliberately manipulated the news feeds of almost 700,000 Facebook users, in order to trigger emotional outcomes for people who had no idea they were even part of a ‘research’ project.

Other examples are on a smaller scale, but no less disturbing. Taking photos of the genitals of a sedated patient – even if those photos do not lead to identification of the patient, and even if the photos are never shared – is a gross violation of a person’s dignity and autonomy.

All these activities hold the potential to impact on individuals’ autonomy, by narrowing or altering their market or life choices.

Philosophy professor Michael Lynch has said that “taking you out of the decision-making equation” matters because “autonomy enables us to shape our own decisions and make ones that are in line with our deepest preferences and convictions. Autonomy lies at the heart of our humanity”.

Yet for now, our legal protections for privacy only kick in when there is an ‘identifiability’ dimension to an activity.

Perhaps it is time to re-think the scope of our privacy laws, to encompass individuation and autonomy as well as identification.
“Your entire life is online. And it might be used against you. Be vigilant.” (Febelfin)

Three years following the explosive mass cyber surveillance revelations from Edward Snowden and the global privacy debate that they ignited, the release of the Snowden movie gives us an opportunity to reflect on the current state of our cyber privacy:

- How much do we care about our cyber privacy?
- What are we doing about it?
- How achievable is it to attain enough cyber privacy?

The importance of Cyber Privacy

Cyber privacy is our right to understand and control what happens with our personal information online. It relies on our appreciation of what personal data of ours is stored, processed, transited and accessed in the cyber space and whether it is managed accordingly to applicable privacy regulations, such as the Australian Privacy Act, the privacy policies of the online service providers we choose to entrust our personal information to (e.g. online banking, Facebook, Skype), and our own confidentiality expectations of the online services we use, such as for example sharing a family picture with a select group of people only, or texting or making a private VoIP call or video with somebody.

Cyber privacy is simply privacy and it should essentially be as important to us as we value privacy in the physical world, such as when we send a private paper letter by good old fashioned mail. However, privacy risks are significantly amplified online because of the scale of access points to digital information, the speed of access to that information, the scale of vulnerabilities and threats the cyber world is increasingly subject to and I think a general lack of information security and privacy awareness education amongst many cyber users. As such, the likelihood and impact of privacy breaches is significantly increased online, and even more so as we further extend the realm of the cyber world to many connected devices in our lives (the Internet of Things) that also collect, process and may put at risk private information.

Cyber Privacy risks are inherent to the following key trends:

1. Over-publishing personal information online, or publishing information without enough control

Personal information published online, such as personal details, photos, locations and activity updates can be used maliciously and expose people to key risks including identity theft and cyber-preying for example. The further data we publish, especially with not enough control, the greater is the privacy risk.

General cyber privacy risks can be simply presented through the amazing performance of Dave, an alleged Belgian “psychic” revealing intimate details about random volunteers in search of clairvoyance enlightening. The video can be found on YouTube, for example here: https://youtu.be/F7pYHN9iC9I. Dave was actually sourcing intelligence from his subjects during his consultations through a team of “hackers” mining the internet and feeding him with the personal information they uncovered. The video was part of a campaign from the Febelfin, a Belgian federation organisation for the financial sector, to demonstrate how easy it is to access someone’s personal information online, and raise awareness on the subject. It concluded with “Your entire life is online. And it might be used against you. Be vigilant.” – very true!
We trade-off privacy for more personalised online services. Telstra’s research on Milenials, Mobilies and Money reports that young adults or “Milenials” (18 to 34 years old in 2014/2015) “demand speed, convenience, exiblity and customisation” for banking online services and mobile apps, where “the optimum trade-off between privacy and personalisation is changing daily”.

We trade-off privacy for convenience, such as for the privilege of using personal mobile devices to access corporate data. Such a privilege is increasingly subject to the deployment and operation of enterprise security agents on personal devices. For instance, I recently had 2 enterprise mobile security agents deployed on my personal mobile phone as an enforced security requirement to my enjoyment of work email and calendar access from my device. My knowledge of what those agents were doing on my device, what personal data they might be capturing and what they were doing with it was rather limited.

We can also appreciate a level of trade-off for state and citizens’ security purposes.

However, the extent to which we can and do really appreciate the privacy risks we are trading-off with is really questionable.

What do we do about our Cyber Privacy?

Options?

There are options to improve the security of personal data and communications.

For a start, personal data management practices can be improved through education and the application of further caution online about privacy. For example, in Australia, we can highlight the program ThinkUKnow, which is oriented toward children cyber safety, as one of the great initiatives sponsored by the Government and industry partners. Such programs are growing and I hope will change behaviours over time.

Technology is also available to reduce some privacy risks, such as for example (non-comprehensive list):

- VPNs for private web-browsing (a myriad of service providers, but which to trust?),
- Anonymous web surfing browser such as the TOR browser,
- Encryption toolkits such as PGP to protect communications such as emails,
- Applications to secure mobile communications (messages and calls), such as Wickr and WhatsApp (both of which have been reported to be used by leading Australian political figures), Signal, and ChatSecure just to name a few. The Electronic Frontier Foundation (EFF) provides a very good reference and security scoreboard on Secure Messaging Applications,
- Applications positioning a more identity centric view of privacy, such as SudoApp (virtual identity management), etc.

While some of those options appear to be growing in popularity, perhaps amongst the most security and tech-savvy community, they are not of widespread use – too many options? Perceived as too technical to use? They are also the subject of a relative privacy protection due to technology vulnerabilities and also the increasing pressure from some law and intelligence agencies to tap into those technologies, sometimes through backdoors that would also present a risk of exploitation by malicious parties.

For more information on options and better communication privacy practices I would recommend the following 2 sites: EFF and The Guardian Project.

Are we doing much with the options we have?

According to the 2015 Pew’ survey, few individuals would appear to do anything tangible to protect their Cyber Privacy. For instance, very few individuals would have adopted effective privacy protection measures such as encryption of their communications, hereby accepting – if not ignoring – the risk of compromise of their private communications and data.

How achievable is it to attain enough Cyber Privacy? (Conclusion)

The Pew’ survey offers an element of answer as to why we may not do much about better managing our privacy risks. The report refers to the following quote from some information scholars, which may well summarise the high “cost” of attaining privacy: “privacy is not something one can simply ‘have,’ but rather is something people seek to ‘achieve’ through an ongoing process of negotiation of all the ways that information flows across different contexts in daily life”. The referred ongoing process of negotiation may imply a high effort of discipline to achieve better privacy and it may simply be too hard to do to achieve great cyber privacy.

We are clearly concerned about our online privacy, but we don’t do much about it. We trade-off privacy for the sake of convenience, opportunity and security without measuring the implications of it. Technology options exist to better manage some privacy risks, but we also don’t use them much (too hard) and they are themselves the subject of risks.

The focus and the development of cyber safety education programs may however provide the best opportunity for improvement longer term, especially as they start with young children. Such programs may provide the key to achieving over time enough Cyber Privacy.

What do you think about it?

Guillaume Noe
Cyber Security Advisor. Business & Technology
What certifications are available? Are they relevant to my work here?

Currently, the iapp offers six specialised credentials, two of which are particularly relevant to iappANZ members, namely the Certified Information Privacy Professional/ Information Technology (CIPP/IT) and the Certified Information Privacy Manager (CIPM).

To achieve either of these credentials, 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 the distinct iapp privacy certifications.

What about testing?

Certification testing is available to iappANZ members locally (at iapp-approved computer-based testing centres). The iapp manages certification registrations and materials, and you can set an appointment to sit your exam online at a testing centre in Australia or New Zealand.
INSURANCE IMPLICATIONS ASSOCIATED WITH MANDATORY DATA BREACH NOTIFICATION REGIMES

SUSAN ELLIS

With the recent announcement that the Notifiable Data Breaches Bill 2016 was introduced to the House of Representatives by the Federal Attorney – General on 19 October 2016 it is timely to consider potential insurance implications.

Borrowing a quote from the sage of Omaha, Warren Buffett, “You never know who is swimming naked until the tide goes out.”

Applying this sentiment to the topic of Mandatory Data Breach Notification Regimes;

Currently in Australia, the Tide is IN (without a Mandatory Data Breach Notification regime, other than the My Health Record Scheme).

1. There is no public scrutiny of an organisation’s cyber security adequacy or inadequacy following a cyber incident, as there is no legislative imperative to notify the event. The cyber security procedures and protocols remain “clothed”

For countries with a Mandatory Data Breach Notification regime, the Tide is OUT

1. A cyber incident must be notified to affected individuals and parties, along with relevant regulators, in accordance with the Mandatory Data Breach Notification Regime obligations.
2. Typically it would be expected that the incident would also be well publicised, creating an opportunity for scrutiny of the organisation’s “unclad” cybersecurity’s procedures and protocols by the general public.

“Unclad” cyber security procedures and protocols may reveal a disconnect between the actual level of cyber security procedures and protocols and the professed level of cyber security procedures and protocols.

Potential Insurance Implications

Based on experience in Mandatory Data Breach Notification Regime jurisdictions, it is reasonable to anticipate the following Insurance implications.

1) The disclosure of a disconnect could result in increased litigation:

- claims being made against the board of directors for misleading or deceptive conduct, which could be contemplated under a Directors & Officers’ Liability Insurance policy or a Management Liability Insurance Policy.

2) Unrelated to the disclosure of a disconnect, A Cyber Insurance Policy would be recommended as a mitigant to defray costs the Organisation would incur in relation to a Mandatory Notification Regime, such as:

- Legal costs to determine who needs to be notified
- Costs to create the database of parties to be notified
- Costs to create the notification (typically involving Public Relations consultants)
- Costs to establish a call centre to respond to questions from individuals whose information has been compromised
- Costs of providing credit monitoring to affected individuals

3) With the general public being made aware of a cyber incident, and possibly the incident remaining in the media for a prolonged period of time, the likelihood of third party claims or litigation is heightened. Cyber Insurance would respond to third party claims alleging security breaches or privacy breaches that have impacted on the third party. Cyber Insurance would provide legal defence costs to these allegations, and damages in the event that the allegations against the Organisation prevailed.

4) Cyber Insurance also extends to legal costs in relation to an investigation by the Regulator overseeing Privacy breaches, and subsequent fines & penalties imposed by the Regulator, where insurable under law.
PHOTOS FROM THE AISA 2016 CONFERENCE

MC Tracy Spicer welcoming delegates to AISA 2016

Winners from the AISA 2016 Awards Night

iappANZ Exhibition Booth

Telecom Panel - Day 2
This article discusses the rising liability costs of data privacy breaches; specifically the ‘first party’ expenses incurred by a business on regulatory response, penalties & legal fees. The article also looks at how available insurance policies address such expenses.

A data privacy breach by a business covered under the Privacy Act triggers liability which carries associated costs. Such costs include staff time of the relevant business in preparing regulatory response. If the Australian Privacy Commissioner does impose a fine – it may be as high as $1.7 million and if legal action follows (e.g. brought by individuals or third parties affected by the breach) - it can require the business to incur a range of legal costs, including legal defence and settlement costs.

Data breaches are costly. The recent Ponemon Data Breach Cost study cites cost of a data breach (including non-liability costs) in Australia as USD134/-per record. Plus, businesses prone to data breaches can have repeated incidents A business faced with recurring incidents may struggle to plan for unexpected expenses related to data breach liabilities or to even classify such costs appropriately. A common view is that businesses view related liability costs as ‘nuisance costs’ as the incidents are caused by malicious intent or unintentional mistakes of third parties and ‘no fault’ of the business itself. However, the author suggests that businesses will come to accept data breach liability expenses as are just a part of the cost of doing business in the information age.

Businesses do have the option to now seek insurance for data privacy liability expenses resulting from a data breach. Policies are available that provide extensive coverage and offer limits as high as $50 million.

Current insurance policy wordings

The author has evaluated some of the insurance policies available on the market to present a brief summary of findings:

Coverage: Many policies cover reasonable costs in settling a third party claim (brought against the insured) for an alleged data breach and the following legal and regulatory liability expenses:

- Advisors/Legal Counsel fees
- Investigation expenses for assessment of a claim
- Claim Defence & Appeal- Legal Expenses
- Regulatory Defence and Penalties payout
- Settlement expenses
- Punitive and exemplary damages insurable per the law applicable to the claim

Not included:

- Overtime, wages, salary of Insured’s personnel including Directors
- Preparing regulatory response is a time consuming activity. Current policies do not provide coverage for use of extra staff for the purpose – but owing to dedicated resource requirements, this aspect of policy coverage may be included in the future as policies evolve

Scope

Scope of policies may vary depending territorial scope. Some polices specify coverage for the breach of any privacy legislation worldwide by the Insured

Limit

Total aggregate limit of the insurance policy applies to the claim payout unless a sub limit is imposed to a specific clause in the policy. Assessing your liability costs:

Assessing your liability costs

Assess your potential liability costs and the maximum coverage required before seeking an insurance quote. For instance healthcare businesses, irrespective of size are covered by the Privacy Act. If your businesses is a health practice, you may at risk of a higher liability cost compared to a small application development business who may suffer from loss of revenue as a result of data theft.

Meena Wahi

Cyber, Data, IP Insurance Specialist
Privacy risks to both individuals and organisations generally start with collection of personal information.

The nature of social media as a means of social communication and how it is structured, has created a rich source of publicly available personal information on social media accounts which organisations may wish to access, collect and use for various reasons. These include, during the recruitment process, as part of workplace investigations, for marketing purposes, to profile consumers and to support identity verification of customers. The social media accounts may be operated by individuals who identify themselves or who may be anonymous or pseudonymous and may be subject to different privacy settings and availability. The posts, chats and comments that are accessible may concern one or more individuals who may be identifiable and which are uploaded by them in various capacities.

In a recent decision in Jurecak v Director, Transport Safety Victoria [2016] VSC 285, the Victorian Supreme Court had the opportunity to consider the interpretation and application of the rules and standards in the principles that apply to the collection of personal information from such social media accounts and notification of the collection.

Key points

While the decision relates to the application of the Victorian Information Privacy Principles (IPPs) on collection, it has broad application beyond Victoria and public sector employers as it helps to remind and inform organisations on the appropriate approach to the responsible collection and handling of personal information sourced from social media. Some key points to take away:

• The nature of the personal information that is being collected and the different ways it is collected will influence how the collection obligations will apply to an organisation and how it must discharge those obligations.

• It can be reasonably necessary and will not be unreasonably intrusive for an employer to collect their employees’ social media comments made on their personal accounts outside of work for the purposes of conducting a workplace investigation and the employer does not need to notify the employee at the time of collection, if this could compromise the effectiveness and integrity of the investigation.

• Whether personal information in a social media account such as a Facebook page generally available to the public will depend on all the facts and circumstances, rather than whether the posts may simply be accessible on the Internet.

• Before collection, organisations should consider what information they propose to collect, the purpose of collection, whether it needs the information or has sufficient information from other sources, when and what steps will the organisation need to take to inform the individual about the collection of their information, what collection notices does the organisation make available.

• If an organisation is engaging a third party to collect the information on its behalf, such as an investigator, aggregator or other service provider, it should consider what instructions or other arrangements are in place to ensure the third party’s acts and practices in collecting the information from social media comply with the applicable collection obligations.

• Finally, organisations should review what their privacy policy says about the sources from which they collect personal information, including social media, and for what purposes, as well as other policies they have in place, to help inform individuals about when and what they can expect the organisation to use their social media posts or other communications for? For employers, this will include proper notice of their IT Use, Bullying and/or Social Media policies.
**Context of decision on appeal**

In the Victorian Civil and Administrative Appeal Tribunal (VCAT), a Victorian public sector employee had challenged the collection of her personal information by her employer in the context of a workplace investigation into her conduct on her Facebook account which she operated under a pseudonym. She claimed the practices had breached IPP1 in the (then current) Victorian Information Privacy Act 2000 (IPA).

After her complaints to the Victorian Privacy Commissioner, as he then was, were not upheld, the Commissioner referred the complaints at her request to VCAT in accordance with the IPA. VCAT generally found that her employer had not breached the IPPs in the IPA when, as part of its disciplinary investigation, it accessed, collected and used her posts and chats with another employee on her Facebook account, without her knowledge and without first attempting to obtain the information directly from her.

The court gave the employee leave to appeal from VCAT's decision, on the basis that it raised ‘important, novel and reasonably arguable’ questions of law about the application of the IPA to personal information on Facebook. The court generally upheld VCAT's findings that the employer has substantially complied with its IPP obligations.

**Collection obligations considered**

The IPPs have been retained without amendment in the Privacy and Data Protection Act 2014 (Vic) (PDPA), which repealed and replaced the IPA. The relevant rules on collection and notification of collection which the court considered are set out in IPP1. Victorian public sector employers must comply with the IPPs, including IPP1, when collecting and handling their employees’ personal information, and this is the factual context in which VCAT and the court considered the application of IPP1.

However, there is an exemption from complying with the IPPs in relation to personal information in a generally available publication. (Section 11(a)(a) of the IPA, now found in section 12(1)(a) of the PDPA. The information collected was found not to be from a generally available publication and so the exemption did not apply.)

In addition, the IPPs were required to be interpreted as human rights legislation and subject to the Charter of Human Rights and Responsibilities Act 2006 (Vic) (the Charter). However no notices were served under the Charter and therefore the court did not consider the interaction of the IPPs and the Charter.

**Why is the decision relevant?**

The relevant rules on collection in IPP1 are similar to the collection and notice obligations in the Australian Privacy Principles (APPs) 3 and 5 in the Privacy Act 1988 (Cth)1988 (Privacy Act) and also in other State and Territory based privacy and health records legislation.

Therefore, the court’s findings provide useful guidance not only to Victorian public sector employers, but also to any organisation that may collect personal information from social media posts for various purposes or form other third party sources rather than direct form the individual, including APP entities to which the employee records exemption in the Privacy Act applies.

The reasons for this are because:

- an APP entity may not be collecting information for employment related purposes;
- not all information collected for employment related purposes will be subject to the ‘employee records’ exemption in the Privacy Act, for example, the employee records exemption does not apply to job applicants;
- much of the social media activity that is targeted is conducted by individuals in their private capacity and may combine information about other individuals who are not employees; and
- the ways individuals use social media and how information they post can be accessed and collected, the organisation may not necessarily know prior to collection, the precise nature of all the information they have collected – whether it is only information about the particular individual, whether it is de-identified or anonymous or pseudonymous, whether it includes information about others or whether it is all information that relates to the purpose for which they are collecting the information.

**Information collected from Facebook**

The information collected by the employer as part of its disciplinary investigation into the employee were posts and chats it had accessed on a Facebook account that the employee had used under a pseudonym. These posts included some inappropriate and abusive comments about the employee’s work colleagues, as well as comments and opinions about non-work related matters. According to the employee’s evidence in VCAT, she had not been made aware of the collection until she realised the information had been collected based on notification by the employer of the outcomes of its investigation and proposed disciplinary action (some 3 months after the collection).

**Alleged breaches of collection obligations**

The employee claimed the employer had breached the requirements in IPPs 1.1, 1.2 and 1.4 that organisations only collect personal information:

1. that is necessary for one or more of its functions and activities (IPP 1.1); and
2. by lawful and fair means and not in an unreasonably intrusive way (IPP 1.2); and
directly from the individual if that is reasonable and practicable (IPP 1.4); and

The employee also claimed that the employer failed to notify her of the collection of her personal information at the time it was collected, in breach of IPP 1.3.

Understanding and interpreting the collection principle - what is reasonably proportionate

The court considered the proper interpretation and application of IPP 1, noting that privacy principles are a particular kind of statutory provision which, while subject to the usual rules of statutory interpretation, are intended to operate in a practical and sensible way so as to afford privacy protection to personal information held by the Victorian governmental organisations. It stated that the privacy principles should be interpreted consistently with Australia’s International obligations, including article 17(1) of the ICCPR, which protects privacy as a human right and provides that 'no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence...' (a right which is also reflected in the Charter).

Drawing on these human rights principles and jurisprudence, the court stated that privacy protections were not absolute and the standards in the principles (such as what was 'necessary', or 'lawful and fair', or 'reasonable') are evaluative in nature. Therefore they were to be evaluated on the basis of balancing, in a reasonable and proportionate way, the interests of the individual being interfered with against the nature and importance of the legitimate purpose and the extent of the interference.

Findings

In addition to the key points noted at the start of this article, other key findings the court made in the circumstances of the case applying the approach set out above to the interpretation of the principles were:

- the test of when collection is 'necessary' for the functions and activities of an organisation should not be narrow - the obligation to only collect personal information from the employee's Facebook account that was 'necessary' for the employer to conduct the misconduct investigation would be met if collection was 'reasonably necessary'. The collection does not need to be 'essential' or 'indispensable' to be permissible. (In any event APP3.1 and 3.2 states that the collection by APP entities must be reasonably necessary, but for Commonwealth agencies it can also be directly related to one of their functions or activities);

- it is mandatory to collect personal information about an individual directly from them if it is reasonable and practicable to do so and this is an objective test;

- while the employer's officers had not turned their minds to its collection notification obligations, the

employer had taken reasonable steps to notify the employee of the collection of information and of the specified matters, by notifying her as soon as it was practicable in a way that did not jeopardise the integrity of the investigation;

- there is no requirement as to how notice of collection should be given, and, depending on the circumstances, the individual (in this case she was an employee of the organisation), may already be aware expressly or impliedly of some of the matters listed in IPP 1.3 or they may not apply;

- a post on social media that that does not explicitly identify the author (in this case as the Facebook account was operated under a pseudonym) may still be personal information if the content of the post, combined with other information available to the organisation, may be used to identify them; and

- the obligation in relation to notification that personal information has been collected applies to the personal information recorded in a document which is held by the organisation rather than notification of the document itself.

Veronica Scott is Special Counsel at Minter Ellison and a Director of iappANZ