President’s Letter

By Anna Kuperman
President
M: 0419 803 263

Dear Members

This will be my last letter as President for 2015. I would like to thank the Board, the Exec team and General Manager, Emma Heath for their significant individual and group contributions and valuable support during 2015.

I am thrilled to be ending my term at the Privacy@Work Summit next week where we have full capacity attendance and an unbelievable line up of international and local privacy gurus taking the stage @ Zinc and guiding us through current and emerging privacy trends, drawing on practical examples and analysing the day-to-day impact of the matters under discussion.

2015 has been a huge year for iappANZ with our PAW road-show featuring the very talented Professor Fred Cate and followed by several training events across Sydney, Auckland, Wellington, Melbourne and Brisbane. Our Privacy Unbound journal has received record contributions from our privacy networks and has been an outstanding resource of knowledge sharing and professional development. Many thanks to our Editors, Veronica Scott and Carolyn Lidgerwood for their outstanding efforts each publication cycle on producing an exceptional journal.

As a volunteer organisation, it is vital to have a group of dedicated professionals that take time out of their busy schedules to provide the strategic insight, leadership and vision to supporting the organisation and maximising the benefits to our members. This year, we have had many volunteers outside of the Board providing significant support to various sub-committees across memberships and partnerships, Privacy@Work Summit, events and training and our NZ network. I want to extend our appreciation to each of our volunteers for their generous commitment and passion for spreading the P word in particular those who have volunteered on our sub-committees (Summit, New Zealand Training & Events, Membership and Sponsorship):

- Emma Pond
- Jacqui Peace
Tobin has been an incredible force of knowledge, expertise and support to our Board. Peter speaks regularly at our events and his team at Gilbert + Tobin lend immense support to our association. Kate Monckton is also retiring this year from the Board and for those of you that have heard Kate speak at our events, will know the energy she brings on each occasion. Behind the scenes, Kate has provided guidance to members on running a privacy program and shared her own trials and successes. We know that Peter and Kate will both remain close to the association and continue to play their part in empowering privacy practice and connecting privacy professionals.

Finally to our loyal members and sponsors without whom our association could not function and engage in the way it has. Thank you for your continued support, participation and generous resources.

Happy reading!

Anna
Vice-President’s Foreword

By Melanie Marks
Vice-President
melanie.marks@cba.com.au

Dear Members

Welcome to the October issue of Privacy Unbound, our last edition for the year. On 18 November the Board and members will gather in Melbourne for the iappANZ Annual General Meeting, following the Summit. On the agenda will be re-election of the Board.

I would like to take this opportunity to thank those who have contributed to the iappANZ over the past year – whether it has been through attendance at our events, written contributions to Privacy Unbound, participating in a Sub-Committee or one of the many other many things that our members do to help and support the iappANZ and the privacy professionals community.

We kick off this month with a case note on the UK decision of James Rhodes v OPO and others, by Martin Soames, Partner at the London firm of Simons Muirhead & Burton. In this decision, the UK’s Supreme Court upheld freedom of expression and clarified the law in relation to the tort of intentionally causing harm, blocking off an unwelcome attempt to extend the law of prior restraint into new territory, for personal information. The case concerned a challenge to publication of Instrumental—a book described as a ‘searing account’ of the life of James Rhodes, a successful classical pianist. Rhodes’ ex-wife objected to publication on the basis that the book would cause distress amounting to harm to their 11-year-old son. Soames’ case note is particularly noteworthy given that he acted for the publisher of Instrumental, Canongate Books.

Next up, Alex Webling Director of Resilience Outcomes outlines the impacts and likely ramifications of the recent decision that the Safe Harbour arrangements between the USA and European Union are invalid as a means for authorising the transfer of personal data from the EU to the USA. To find out why Australia, New Zealand and countries of similar scale should be pushing hard diplomatically for an international ‘Law of Cyberspace’, turn to Alex’s article on page 9.

Next up is our regular column with the Office of the Australian Information Commissioner. This month, Angeline Falk,

Assistant Commissioner, Regulation and Strategy, reflects back on the last year, invites submissions on the OAIC’s Draft guide to developing a data breach response plan (deadline 27 November) and highlights the OAIC’s recent acceptance of an enforceable undertaking from TeleChoice.

Do you think that we privacy professionals can figure out what is unduly privacy invasive by applying a creepiness test? The Theory of Creepy (by Omer Tene and Jules Polonetsky) suggests that creepiness arises when new technology rubs up against social norms. If social norms don’t shift to accommodate the new technology, a consumer backlash occurs. Anna Johnston, Director of Salinger Privacy, shares her views on the Theory as a means of determining likely privacy invasiveness, pointing out that humans are both irrational and inconsistent in their responses, which makes perceptions of creepiness hard to predict. A better approach? Turn to page 13 to find out.

A bevy of esteemed Summit panelists join me in the next article to discuss their views on how to manage aspects of the Ashley Madison fall out. As a precursor to their session at the Summit next week, which will cover what to do when things go wrong, our panelists share their views on what the initial organizational response should be, how to consider notification, public messaging, preventing harm to customers and limiting reputational fall out for entity. New Zealand’s Chief Privacy Officer outlines its role in supporting public sector agencies to respond to breaches and the OAIC gives us some tips and considerations in reporting a data breach in Australia.

Will any of these authors be the winner of this year’s writing prize? It’s possible! Entries for the year have now closed with the winner to be announced at the iappANZ Privacy@Work Summit next week. Good luck to our contributors from 2015.

We hope you enjoy Privacy Unbound this year and as always, invite your feedback to make it even better in 2016.

All the best

Melanie
A message about iappANZ membership:

Membership benefits

iappANZ has grown into the pre-eminent forum for people with an interest in privacy in Australian and New Zealand, offering our members a wealth of opportunities to expand their privacy knowledge, compliance, interests and networks. We continue to work with private entities across all industry sectors as well as regulators in both countries.

As an iappANZ member you are entitled to receive a range of great member benefits as outlined at: www.iappanz.org.

Through our affiliation with the global body, the International Association of Privacy Professionals (iapp), you are also entitled to additional member benefits, including the knowledge and resources located within the members’ only area of the iapp website at: www.privacyassociation.org.

You can access benefits available to you through your iapp account. Simply login to your MyIAPP account using your email address as the username. If you do not yet have a password or have forgotten yours just click on the “Reset your password” link and instructions on how to create a new password will be sent to you. If you don’t want us to confirm your membership details to iapp in accordance with iappANZ’s privacy policy, please let me know by emailing me at emma.heath@iappanz.org.

I hope that access to these additional privacy resources will be of benefit to your work as a privacy professional.

Emma Heath, iappANZ General Manager

Visit our website, 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, connect with us today!

Our website is www.iappANZ.org.au. You can log in to our member area from our website homepage with your email and password to access past bulletins. You can also get a new password or be reminded of your username if you have forgotten it. Just click on the links on the log in box. If you still need help email us at admin@iappanz.org.

Our LinkedIn group is:
http://www.linkedin.com/groups?gid=1128247&trk=anetsrch_name&goback=qdr_1281574752237_1

Follow us on Twitter at: https://twitter.com/iappANZ
AISA National Conference Summit ticket winner

iappANZ is delighted to announce the winner of our business card draw at the AISA national conference that took place in Melbourne in October.

Nang Tip, an IT Security Consultant, Technical Services with the Australian Bureau of Statistics is our Summit ticket winner.

Congratulations Nang and look forward to seeing you there!
An undead privacy law: *James Rhodes v OPO and others*

by Martin Soames

**Introduction**

The tort of intentionally causing harm was established in 1897 in *Wilkinson v Downton*, an action arising out of a misconceived personal hoax targeted at the claimant by the defendant. The essential elements of the tort are: i) unjustified conduct towards the claimant, ii) with the intent of causing physical harm or severe mental or emotional distress, iii) followed by harm as a consequence.

It is unlikely that the original Victorian judge ever imagined his decision would be used more than a hundred years later to try and block publication of a truthful autobiography. The Supreme Court in the United Kingdom (UKSC)\(^2\) has upheld freedom of expression and clarified the law in this unusual area. In doing so it has blocked off an unwelcome attempt to extend the law of prior restraint into new territory, for personal information.

**Facts**

James Rhodes is a successful classical pianist. His book, *Instrumental*, published by Canongate Books Ltd, is described in the UKSC's judgment as giving a 'searing account' of his life as well as the physical harm and psychological effects he suffered as a result of years of rape as a young child by a teacher. Interwoven with these 'dark descriptions of emotional hell, self-hatred and rage', he describes his relationship with music.

Rhodes' ex-wife objected that the book would cause distress amounting to harm to their 11-year-old son. A pre-publication injunction was sought on behalf of the child, identified as OPO, supported by his litigation friend. The book contained minimal personal information about the child and his mother, neither of whom was identified.

The claim had three heads:

1. Negligence: the father owed a duty of care to his son;
2. Privacy: publication would infringe the right to respect for private and family life; and
3. Wilkinson v Downton: publication of the father’s book amounted to intentionally causing harm to the child.

The injunction was dismissed on all counts in the High Court in July 2014, but in a wild card decision in August, the Court of Appeal allowed it on the basis of Wilkinson v Downton. The UKSC gave leave for an expedited appeal in January 2015 and handed down its decision on 20 May 2015.

**The Decision**

The UKSC unanimously reversed the Court of Appeal’s decision. It reviewed the historical context of the tort and its development across jurisdictions, including the United States, New Zealand, Australia and Canada, and defined the narrow limits of it as wilful infringement of the right to personal safety.

The judgment of Lady Hale and Lord Toulson (with which Lords Clarke and Wilson agreed) considered the constituent elements of the tort with reference to the facts in this case. In relation to conduct, it held that the Court of Appeal had wrongly assessed the justification for publishing the book to the child rather than to the general public; properly it was not conduct directed towards the child. Their findings in this regards are worth repeating:

> "The conduct element requires words or conduct directed towards the claimant for which there is no justification or reasonable excuse ... We are concerned in this case with the curtailment of freedom of speech, which gives rise to its own particular..."
considerations. In the present case the Court of Appeal treated the publication of the book as conduct directed towards the claimant and considered that the question of justification had therefore to be judged vis-à-vis him. In this respect we consider that they erred.

The book is for a wide audience and the question of justification has to be considered accordingly, not in relation to the claimant in isolation ...

When those factors are taken into account, as they must be, the only proper conclusion is that there is every justification for the publication. A person who has suffered in the way that the appellant has suffered, and has struggled to cope with the consequences of his suffering in the way that he has struggled, has the right to tell the world about it.’ (paras 74 – 76)

Further, the UKSC emphasised the cardinal importance of truth in this field:

‘Freedom to report the truth is a basic right to which the law gives a very high level of protection ... It is difficult to envisage any circumstances in which speech which is not deceptive, threatening or possibly abusive, could give rise to liability in tort for wilful infringement of another’s right to personal safety. The right to report the truth is justification in itself.’ (para 77)

The UKSC considered intention, finding that recklessness was not enough to found liability. There was no evidence in the case that Rhodes intended to cause psychiatric harm or severe mental or emotional distress to his son. Intention was a matter of fact, and it could not be imputed as a matter of law:

‘Impugnation of an intention by operation of a rule of law is a vestige of a previous age and has no proper role in the modern law of tort. It is unsound in principle. It was abolished in the criminal law nearly 50 years ago and its continued survival in the tort of wilful infringement of the right to personal safety is unjustifiable.’ (para 81)

Lord Neuberger, in his separate judgment, clarified the public interest requirement:

‘While I agree that many people would regard the book as being in some respects in the public interest, it is not necessary to decide this appeal on that ground. Unless it is necessary to do so, I am unenthusiastic about deciding whether a book, or any other work, should be published by reference to a judge’s assessment of the importance of the publication to the public or even to the writer. In the present case, I do not consider that it would make any difference if the experiences which the defendant describes could be shown to have been invented, or if the book had been written as a novel by someone who had not been sexually abused.’ (96)

The UKSC was critical of the Court of Appeal’s attempt to take ‘editorial control’ over the manner in which Rhodes told his story:

‘The Court of Appeal recognised that the appellant had a right to tell his story, but they held for the purposes of an interlocutory injunction that it was arguably unjustifiable for him to do so in graphic language. The injunction permits publication of the book only in a bowdlerised version. This presents problems both as a matter of principle and in the form of the injunction ... A right to convey information to the public carries with it a right to choose the language in which it is expressed in order to convey the information most effectively.’ (para 78)

The Court should not interfere in how the story is told. As Lord Neuberger states:

‘It is true that the book contained material which some people might find offensive, in terms of what was described and how it was expressed, but “free speech includes not only the inoffensive but the irritating, the contentious, the eccentric, the heretical, the unwelcome and the provocative provided it does not tend to provoke violence” – see Redmond-Bate v. DPP (1999) 7 BHRC 375, para 20, per Sedley J. As he memorably added, “[f]reedom only to speak inoffensively is not worth having.’ (para 96)

The UKSC added that the lower Court’s restriction on the publication of ‘graphic’ information was legally defective because it lacked the clarity and certainty which an injunction properly requires. Any injunction must be framed in terms sufficiently specific to leave no uncertainty about what the affected person is or is not allowed to do’ (para 79).

Although the UKSC carried out a balancing exercise between the rights of the parties in this case in accordance with the requirements of the European Convention on Human Rights, its conclusions were reached without reference to those principles. Lord Neuberger
stated that ‘it would be arrogant to assume that there may be no assistance to be gained from the Strasbourg jurisprudence’ (para 120), but added that the relevant authorities did not take matters much further. He added that the case had been decided with reference to English law rather than that of the US, where the claimant lived, but that it was possible the relevant American law was the same.

Conclusion

The tort in Wilkinson v Downton will only apply to conduct or words directed by a defendant towards a claimant for which there is no justification or reasonable excuse, where the defendant has the actual intention of causing the claimant at least severe mental or emotional distress, and that conduct causes the claimant physical harm or a recognised psychiatric illness.

It follows that the tort will very rarely extend either to publication to the world at large or to true speech. The UKSC decision has upheld freedom of expression not only in allowing the dissemination of true facts but also in protecting the chosen form of words. The judgment has effectively restored editorial control to author and publisher.

The other notable event in 1897 was the publication of Bram Stoker’s ‘Dracula’. We can celebrate that the UKSC has not only put an archaic tort back in its box, but also put a stake through an attempt to extend the law of privacy by stealth.

Martin Soames is a Partner at the London firm of Simons Muirhead & Burton and acted for Canongate Books, publisher of ‘Instrumental’.
Australia, New Zealand, Safe-Harbour and the Internet*

by Alex Webling

Early in October, the European Court of Justice declared the Safe Harbour arrangements between the USA and European Union invalid as a means for authorising the transfer of personal data from the EU to the USA. The decision will have interesting implications for Australia, New Zealand and other small advanced economies that increasingly rely on services for GDP.

Safe Harbour, was supposed to give protection to personal data collected by multinational companies on EU citizens when it was transferred to the USA, and from there to other locations. This allowed Facebook and 4000 other companies to store EU citizens’ data in the USA or wherever it was most efficient, but required them to treat the data to the EU’s standards, rather than the more relaxed USA standards.

It began as a university assignment on Facebook’s privacy policy for an Austrian postgraduate student. Max Schrems’ case against the Internet giant has ended up in a decision which threw out the ‘safe-harbour’ arrangements for around 4000 companies from the USA that were handling European citizens’ personal data.

The Safe-Harbour arrangements had been in place since 2000, but have been increasingly brought into question following the revelations by Edward Snowden regarding mass surveillance. For Facebook, it means that their European privacy practices will be investigated by the Irish data protection commissioner in some detail.

In the USA, the decision has been greeted by some as an attack on Silicon Valley’s libertarian ethos. But it is more than this. The judgement is a further indication of the deep unhappiness in Europe with perceptions of the USA’s cavalier approach to non-US citizen’s data when undertaking mass surveillance.

USA agencies are restricted from undertaking mass surveillance of USA citizens, but non-citizens do not have the same rights. Whilst Angela Merkel might be able to brush off the NSA’s activities, the USA’s binary approach to citizen rights continues to make many USA non-citizens bristle. It reminds of the Pax Romana of the Roman Empire 2000 years ago where the cruelty of torture that could be inflicted under law was determined by citizenship as much as crime. It is true that the USA is not alone in this conceptual approach. However, because USA owned information systems are still at the heart of the Internet, in practice non-USA citizens are the ones most affected.

In the end, the collapse of safe-harbour will not ‘destroy the cloud proposition’ in Europe or elsewhere. However, it will require some reorganisation, particularly for organisations without subsidiaries in EU member states. In this, it will hurt second and third tier players more than Facebook, Amazon and Google.

Moreover, the decision will not seriously curb mass surveillance. The dirty little (not so) secret is that all countries spy on their citizens and others for mostly good reasons, including the Europeans. It’s just that the US is better at it than most others and both Australia and New Zealand gain greatly from the intelligence sharing alliance.

For Australian organisations, not only those who hold EU citizens’ data, this decision should cause them pause for thought. Organisations that do not take privacy seriously, or only respect the privacy of a subset of their stakeholders, need to rethink their approach, if only in terms of the reputational damage of a breach in markets like the EU.

Smaller countries like Australia and New Zealand should be concerned despite their tight intelligence relationship with the US and UK. The Internet has never been one network for all, it is a motley collection of many nets with varying governance across varying geographic boundaries. The main effect of the decision is to further balkanise the Internet in a similar way to content geo-blocking and country firewalls. The EU has recently released a near final version of the Data Protection Regulation which will establish greater harmony in privacy protection across the EU and the EU and USA have been negotiating on the successor to the safe-harbour

* An earlier version of this piece appeared in the www.resilienceoutcomes.com blog.

arrangements since 2013. However, both these moves are likely to create further restrictions on services trade for non-EU organisations, particularly those that are too small to create a physical presence in EU member states like most Australian and NZ entities.

Australia and New Zealand need to be able to trade on an even playing field in services. And that means having an Internet that is common to us and our competitors, in terms of technology and policy at all levels including privacy. We need common laws governing cyberspace as much as we need trade barriers on physical goods like rice to be reduced.

This is the time that Australia, New Zealand and similar countries should be pushing hard diplomatically for an international ‘Law of Cyberspace’ which achieves the equivalent that the conventions on the Law of the Sea achieved for maritime commerce. This could be a good outcome for individual privacy and for Internet commerce.

It took several hundred years for the Law of the Sea to come to pass and it’s still being updated – let’s hope that the law of cyberspace takes much, much less time.

Alex Webling BSc, BA (Hons), Gdid Comms, GdidEd, ZOP, is a Director of Resilience Outcomes a registered security professional in the area of enterprise security management and has 20 years experience as a senior executive for the Australian Federal Government including in cyber-security, critical infrastructure protection, identity security and resilience. is also the 2014 winner of the iappANZ writing prize o tell Alex what you think, please email him on alex@resilienceoutcomes.com. He would love to hear from you.

Further reading:
- CIGI-Ipsos Global Survey on Internet Security and Trust | Centre for International Governance Innovation
The year in review and other updates
Office of the Australian Information Commissioner

By Angelene Falk

With the tabling of the OAIC’s 2014–15 Annual Report, we have an opportunity to reflect on what we’ve achieved in the last year, and to look to the future.

Over the past year the OAIC has worked collaboratively with business, Australian Government agencies and consumer groups to embed the most significant reforms to the Privacy Act 1988 (Privacy Act) since its enactment. We produced a comprehensive range of privacy resources to assist both businesses and individuals to understand their rights and obligations under the amended Privacy Act including the OAIC’s Privacy Management Framework, launched during Privacy Awareness Week in May 2015.

Our Annual Report also highlighted a number of trends, including a continued interest in, and awareness of, privacy rights, with 16,166 privacy enquiries and 2841 privacy complaints received. The OAIC also received 110 voluntary data breach notifications — a 64% increase from the previous year.

And our strategic privacy assessment program ensured we engaged with privacy risks facing over 100 regulated entities, noting good privacy practice and working with government and agencies on areas for improvement.

Looking ahead at some of our proactive privacy work, the OAIC will be conducting further privacy assessments, developing and refining our guidance to assist the regulated community and individuals, and also engaging with government and industry on the mandatory telecommunications data retention scheme that commenced on 13 October 2015.

At the iappANZ Summit in November, the Acting Australian Information Commissioner, Timothy Pilgrim, and I will be speaking about a range of topics covering the broad thinking behind international regulatory cooperation and cross border data protection; through to the specifics of what informs the regulatory response to a data breach.

Data breach response plan consultation

We have also developed a draft Guide to developing a data breach response plan to complement our established publication, Data breach notification — A guide to handling personal information security breaches. The consultation on the draft Guide to developing a data breach response plan opened on 28 October, with the closing date for comments Friday 27 November.

The draft guide is aimed at helping agencies and organisations that handle personal information to develop a data breach response plan.

A data breach response plan is a framework which sets out the roles and responsibilities for managing an appropriate response to a data breach. This includes:

- the actions to be taken if a breach is suspected, discovered or reported by a staff member, including when it is to be escalated to the response team
- the members of the data breach response team
- the actions the response team is expected to take.

The guide emphasises that an entity’s actions immediately following the discovery of a breach are often crucial to the success of a response and that quick responses can substantially decrease the impact on the affected individuals.
TeleChoice enforceable undertaking

On the 22nd of October, the Acting Information Commissioner accepted an enforceable undertaking from TeleChoice, following an incident in which the personal information of former TeleChoice customers was found in a shipping container located on publically accessible land. The information included the records of individuals who were TeleChoice customers prior to 31 March 2013.

As part of the enforceable undertaking, Telechoice will take specific steps to improve its information security and destruction practices to mitigate the risk of a similar incident occurring in the future. TeleChoice also agreed to reimburse the cost of a 12 month credit monitoring service for affected individuals who are concerned about the possibility of credit fraud.

This is the second enforceable undertaking to be made this year, following an agreement for an enforceable undertaking between the OAIC and Optus in March 2015.

OAIC website upgrade

In late October we launched a website upgrade, with a range of new usability and accessibility features. The upgraded site includes a more user-friendly menu system and new search and filter functions as well as a range of updates to publications and guidance. This includes new FAQs on Social media, ICT & identity security (for individuals), ID scanning (for business), and credit reporting (for business).

The changes to the site also include a range of accessibility improvements, providing an improved user-experience for anyone who uses accessibility software.

44th Asia Pacific Privacy Authorities Forum

I will be attending the 44th Asia Pacific Privacy Authorities (APPA) Forum, which will be held in Macao in December. Some of the topics that will be explored at this meeting include global privacy developments, personal data and telemarketing fraud, big data and privacy trust marks and certifications. APPA is the principal forum for privacy authorities in the Asia Pacific region to enhance cooperative privacy regulation and is an important opportunity to debate emerging privacy issues across jurisdictions.

Angelene Falk is the Assistant Commissioner, Regulation and Strategy, Office of the Australian Information Commissioner.
Creepiness is in the eye of the beholder*

by Anna Johnston

As a privacy adviser, I am often called upon to determine whether or how a particular initiative can comply with privacy law. But often a more compelling and relevant question is: will this project fly, or will it crash and burn?

The answer to both questions is often “it depends”. The principles set down in privacy laws in Australia and around the world are examples of what’s known as fuzzy law, meaning they offer plenty of blank space around phrases like “reasonable expectations” and “take reasonable steps”, that the privacy adviser has to fill in. And then even if you do comply with the law, a backlash from your customers or the wider public can bring your project undone faster than you can say “Australia Card”.

So how are we supposed to figure out in advance what will be considered unduly privacy invasive, and what won’t?

A couple of my favourite privacy academics, Omer Tene and Jules Polonetsky, have proposed a “Theory of Creepy” to help us figure it out.¹ They suggest that creepiness arises when new technology rubs up against social norms. Sometimes social norms shift to accommodate the new technology – but sometimes they don’t, and a consumer backlash ensues.

Using their categorisation method, we can see examples of the kinds of activities that might be seen as cool – or creepy – depending on the context:

- Ambient social apps: These take publicly available location data about people and present it to other users, which might end up being regarded as ‘cool’ – such as Foursquare - or ‘creepy’: Girls Around Me showed the social media profiles of women physically near the user at any given time; and the Obama app used in the 2012 US election campaign plotted voters’ names, age, gender and political leanings on maps of residential areas.²
- Social listening: This involves monitoring customers via social media, and anticipating their needs or responding to their concerns. This kind of intensive surveillance of and approaches to individual customers can be regarded as brilliant best-practice marketing (KLM’s Surprise initiative), or a disastrous cross-over into stalking behaviour (British Airways’ Know Me initiative).³
- Data-driven direct marketing: Using a customer’s history of past purchases to offer suggestions as to what they might like to purchase now, which can be seen as expected business practice (Amazon’s book recommendations), or as so surprising that it becomes the case study in what not to do (Target’s marketing to a teenager it figured out was pregnant before her father did).⁴
- New products: The failure of Google Glass wearers to anticipate and adhere to social norms led to the creation of a new epithet – Glassholes – and sent the product back to the drawing board.

*The blog from on which this article is based can be found at www.salingergovernment.com.au
Their conclusion is that any new project requires a social or ethical value judgment to be made – and that this judgment should not be left to the engineers, marketers or lawyers. As Tene & Polonetsky say: "Companies will not avoid privacy backlash simply by following the law. Privacy law is merely a means to an end. Social values are far more nuanced and fickle".

In my view, that fickleness is the core of the problem. Humans are not rational or consistent in their responses. Why was British Airways’ social listening deemed creepy, but KLM’s deemed cool? Both involved unexpected online identification and analysis of customers waiting for flights, and then real-world interactions with those customers. Why do we accept CCTV manned by unseen agents, but not a guy with a camcorder? I don’t have the answer.

So, how can we avoid creepiness, if we can’t predict where a new initiative will fall on the cool-to-creepy continuum?

Unlike Tene & Polonetsky, I still find privacy law to be our best starting point. Yes it is fuzzy law; yes it has some ridiculous loopholes. But at their core, privacy principles represent both common sense and good manners: Only collect what you need. Ask the subject for the information directly. Tell them what you’re going to do with it. Don’t go using data in new and surprising ways that the subject wouldn’t expect. Don’t expose the data unnecessarily. Etcetera.

There are pragmatic ways to develop customer trust and protect privacy but maintain your business objectives, and in many ways, the privacy principles themselves point the way.

The value of proposing a ‘creepiness’ test as part of project management is that it might be a useful way to start a conversation with your marketing department, your engineers or even your CEO, if talking about the law tends to send them to sleep. Of course anticipating and reflecting community expectations is also critical to fleshing out your analysis of potential privacy pitfalls. But ultimately, our principles-based privacy law is the best place to start.

Other than on Halloween, ‘tis better to be cool than creepy.

Anna Johnston is Director of Salinger Privacy.

Salinger Privacy provides specialist privacy consulting and training services, and publishes eBooks on privacy law, including an annotated guide to the NSW privacy laws. You can find her and read Salinger’s blog at www.salingerprivacy.com.au

---


Life is short. Have an affair

by Melanie Marks

In August 2015, hackers made public the private information of millions of users of Ashley Madison, a dating website which promotes itself as the go-to website for infidelity. Its motto: "Life is short. Have an affair."

Now take yourself to that fateful day in July 2015 and imagine yourself as one of the key advisors to the company. Maybe you're the CEO, the CISO or the CPO. Maybe you're Head of Legal or Media and Communications. You're notified by the hackers of the stolen data and threatened with public release of the data. What do you do?

As a prelude to their much anticipated panel session at the upcoming iappANZ Summit, the following Privacy super stars have come together to share their views and insights on the Ashley Madison breach.

Featured panelists

Jennifer Mulveny
Director, Cloud Policy and Government Relations, ANZ
Intel Corporation

Nicole McKechnie
Director of External Communications, Telstra

Anne Marie Allgrove
Partner, Baker & McKenzie

Russell Burnard
Government Chief Privacy Officer
The Department of Internal Affairs Te Tari Taiwhenua

But first – the Ashley Madison facts (according to Wikipedia¹)

On July 15, 2015 the Ashley Madison website was hacked by a group known as “The Impact Team”. Claiming that security had always been weak, the hackers claimed to have stolen personal information about the site’s user base, and threatened to release names, home addresses, search histories and credit card numbers if the site was not immediately shut down. The demand was said to be driven by the site’s policy of not deleting users' personal information following their invoiced requests.

The first release, validated by experts, occurred on August 18. Another release was made on August 20, but a 13 GB file — which allegedly contained the emails of Avid Life Media CEO Noel Biderman — was corrupted. This was corrected on August 21, when the Impact Team dumped Biderman’s emails in a separate 19 GB file.

Some users reported receiving extortion emails requesting 1.05 in bitcoins (exactly C$300) to prevent the information from being shared with the user’s significant other. Clinical psychologists argued that dealing with an affair in a particularly public way increases the hurt for spouses and children. On August 24, the Toronto Police Department spoke of “two unconfirmed reports of suicides” associated with the leak of customer profiles along with extortion attempts, offering a $500,000 reward for information leading to the arrest of the hackers. At least one suicide previously linked to Ashley Madison has since been reported as being due to “stress entirely related to issues at work that had no connection to the data leak”.

For a full recap see The Ashley Madison hack...in 2 minutes

¹ https://en.wikipedia.org/wiki/Ashley_Madison#Data_breach
What does the Panel say?

Anne Marie Allgrove – What are the first steps that Ashley Madison should take in relation to the suspected breach? How should Ashley Madison go about the question of notification of customers and privacy regulators in Australia?

The first thing anyone who is subject to an incident should do is to assess the nature of the incident as soon as possible and what data, data subjects (type, location and number) have been affected, and the likelihood and seriousness of the risk of harm to the data subjects.

In this case it was clearly a hacking but it could be a lost device or insider theft or other event. It is important then to determine who is aware of the incident internally and externally and set up a response team with representatives from various functions in the organisation to be able to address the issues that will arise and to ensure adequate resources are available to address the dimensions of the crisis. Importantly, the internal PR function or an external function should be engaged to help manage the messaging and the communications. Further, the board and senior management should be informed.

The company needs to quickly take steps to protect the security of the system while avoiding destruction of critical electronic evidence, including activating any right to have the database taken offline until it is secure, and to ensure access is given to the site to be able to assess what has occurred. Hopefully the company’s contracts enable such steps to be taken.

The company should then look to engage a reputable forensics firm to assist with reviewing and assessing what occurred and collecting and preserving critical evidence. Consideration needs to be given to the best way to engage any relevant forensics firm to protect privilege as much as possible. Often in common law countries that will mean using external counsel to engage the forensics experts.

Consideration needs to be given to the company’s data breach reporting obligations. In some jurisdictions the obligations arise as soon as the company becomes aware of the breach. It is important to assess what those obligations are and develop a notification plan taking into account the obligations globally. This might involve notifying regulators in jurisdictions where notification is not required if notifications are made elsewhere.”

Nicole McKechnie – What are the top three messages that organisations should include in a media release, in the early stages of identifying and understanding a privacy breach? What is your advice as more information comes to light?

In the early stages of understanding the nature of a privacy breach, any media release should:

1. Acknowledge the issue, make it clear you are aware and take responsibility
2. State that further investigations are underway so the impact on customers can be fully understood and assessed
3. Commit to keeping customers and key stakeholders informed of developments as more information comes to hand. Make sure a timeframe is given for the next update.

Jennifer Mulveny – Once the full scope of a breach is understood, what can organisations do to prevent harm to customers and limit brand and reputational damage themselves?

Latest reports are that Ashley Madison is still growing, which is remarkable. Step number one would be to retain a top-notch PR firm to help control the damage, and of course determine to what extent the company publicly takes direct responsibility for any weaknesses discovered in how the immensely personal data of the AM customers was protected. This is a challenging one because the very nature of Ashley Madison’s business is to collect very sensitive personal data, so a responsible policy to “collect as little data as possible” sort of flies in the face of the business model in this instance. Nonetheless, it’s not a bad time to review the privacy policy, and announce that it’s being reviewed, along with a comprehensive overhaul of the security apparatus for storing this sensitive data. The company should be working 24/7 to get ahead of potential future incidents using a mix of PR and technological enhancements. Making technological changes internally to the encryption of the data in a way that can be communicated to existing customers would be one way to prevent future harm.
Russell Burnard – What role does the Government Chief Privacy Officer have in supporting public sector agencies to respond to breaches, especially of sensitive personal information? What has the GCPO learned in its first year of operation?

The GCPO has responsibility for privacy leadership across government, including standard setting and the development of guidance, building capability within agencies in privacy management, and undertaking system-wide engagement with the Privacy Commissioners and other stakeholders. We have an active engagement programme and provide support and advice to agencies when requested. Final accountability for privacy management within agencies remains vested in their chief executives.

The GCPO role was established in June 2014 as part of the Government’s response to several high profile privacy breaches. It followed on from an earlier decision by Government to establish the role of Government Chief Information Officer to provide functional leadership across ICT in the public sector. The initial mandate was for 43 core departments and crown entities and that was expanded on 1 July 2015 to include 20 District Health Boards (DHBs). There is information on the Review of Publicly Accessible Systems and the follow-up reports on progress available here: [http://www.ssc.govt.nz/GCIO-publicsystemsreview](http://www.ssc.govt.nz/GCIO-publicsystemsreview)

Last year, we issued Core Expectations for good practice and a Privacy Maturity Assessment Framework (PMAF) to guide agencies in assessing their own capability in relationship to the inherent risk of the information assets they have stewardship over. In March 2016, we expect agencies to report formally to us on their privacy capability and plans for future development using a tool based on the PMAF maturity scale.

Privacy management maturity was sub-optimal and remains ‘patchy’. We have pockets of very good practice but often at significant cost. Agencies have made admirable progress in the last two years, as shown in their responses to the reporting done on the progress since the GCIO Review referred to above. Most agencies have responded favourably to the PMAF and found it useful in discussions with their senior management teams about what capability they have and what they probably should have. Many agencies have created new positions for and appointed new privacy officers.

We are seeing agencies with more sophisticated understanding bringing a collaborative or cross-functional approach to privacy management bringing together privacy, information management, security, and risk management functions.

Join us at the iappANZ Summit in November to hear from these panelists and others on the topic of:
Managing Privacy – A Stakeholder Perspective

The stories of technological advancements that are revolutionising everyday interactions and transactions are an undeniable reality today, in both the private and public space. Privacy rhetoric around the globe suggests that accountability for privacy needs to be a joint effort among governments, regulators, organisations and individuals themselves. In this world of dynamic change, the issues are evolving at a rapid pace, stakeholders are sophisticated and challenges exist across borders. But what is the true effect on organisational privacy governance or data breach management in every day practice? What does it really mean to affected stakeholders (individuals, regulators, organisations) and how can each party remain accountable in a world where yesterday’s thinking will not solve tomorrow’s problem.

Stakeholders from regulator offices in Australia and New Zealand, an expert legal advisor, a specialist privacy barrister, a media specialist and a privacy officer across ANZ all powerfully combine to share their unique practical insights on managing privacy, including data breach crisis management. The panel will provide insights into establishing privacy programmes that minimise risk but recognise that things can go horribly wrong. What are the practical strategies for an organisation with good privacy risk management to handle a privacy disaster and move through a crisis without unravelling major stakeholder relationships? How do you engage internal and external stakeholders with different points of view on desired outcomes both before, during and after a crisis?

Turn over for the OAIC’s tips and tricks on reporting a data breach....
Tips and considerations in reporting a data breach

Generally, in circumstances where a data breach may result in a real risk of serious harm to the individuals involved, the Office of the Australian Information Commissioner (OAIC) strongly recommends organisations promptly notify affected individuals, and the OAIC, of the breach.

When the OAIC receives and responds to a voluntary notification we provide general guidance to assist the organisation in responding to the breach. The OAIC also gathers information to allow the Commissioner to be satisfied that the organisation is handling the breach appropriately. If an incident points to a breach of the Privacy Act, the Commissioner will consider if further regulatory action is appropriate, such as commencing a Commissioner initiated investigation. However, the Commissioner would consider the fact that an organisation has promptly and voluntarily notified the OAIC, has taken appropriate steps to respond to the breach, and has cooperated with the OAIC in remediying any breach, when deciding whether to take regulatory action.

When notifying the OAIC, organisations should do so in writing via enquiries@oaic.gov.au. Notifications should generally include information such as a description of the incident, the type of personal information involved, their response, what assistance has been offered to affected individuals, the name and contact details of the appropriate person, and whether the breach has been notified to other external contacts.

The OAIC’s Data breach notification guide, particularly the Data breach response process flow chart will help organisations to respond appropriately. Information about the manner in which OAIC will use its regulatory powers is contained in the Regulatory Action Policy. The Guide to Privacy Regulatory Action contains more detailed information about the OAIC’s use of particular regulatory powers.

Melanie Marks is Executive Manager - Digital Trust and Privacy at Commonwealth Bank and the Vice President of iappANZ
iappANZ’s writing prize 2015: entries are now closed

Entries are now closed for this year’s writing prize. The winner will be announced at our Privacy Summit on 18 November 2015 in Melbourne and their name and details will be published on our website. Thank you and good luck to all those who have contributed eligible articles in 2015. Please keep them coming in 2016. The quality is outstanding.
Employment opportunities for privacy professionals

News about employment opportunities is provided as a service to iappANZ members. If you would like a notice about employment opportunities at your organisation published in Privacy Unbound, please contact our editors (see details on last page).

Calling Privacy Professionals
Join a company dedicated to your career development.

'Yes'. A small word that speaks volumes about our attitude as a company. Our vision is to provide outstanding customer experience as we strive to become Australia's most loved and recommended service brand. We're excited about creating a culture that encourages people to achieve their best.

At Optus our vision is to lead Australia in outstanding customer experience and we believe our people are at the heart of this. We are passionate about creating a climate that encourages our people to achieve their best - personally and professionally.

We are currently looking for multiple Privacy professionals both senior and junior. The team is responsible for developing and leading the vision for the Optus's Privacy Program - designing and building, implementing and operating the program.

To be successful you will have the following experience:

- Previous administration experience in a large corporate privacy environment
- Experience and intimate knowledge of Australian privacy laws and regulations
- Knowledge of best practice frameworks, technologies, emerging trends to data privacy
- Previous experience with privacy and information security programs, including requirements definition, incident response plans, monitoring, reporting, and training and awareness programs.

If you feel like this could be the role for you, you should apply below by emailing nathan.nankivell@optus.com.au or alternatively please contact Nathan on +61 2 8082 6785.

Heads Up!!
Due to the fast paced nature of the Optus business, our vacancy close dates may be subject to change. Don't dilly dally and make sure you apply as soon as possible. We will assess applications as they are received.
One last thing, Optus operates a direct sourcing model so no agency introductions, sorry folks.
Technology Consulting - Cyber Security Consultant - Penetration Tester, PwC

Close Date 11/30/2015

Locations: based in Brisbane, Canberra, Melbourne and Sydney

Job Description:

Technology Consulting - Cyber Security Consultant - Penetration Tester

- Full time OR Part-time
- Permanent role
- Melbourne/ Sydney/ Brisbane/ Canberra positions available

PwC Australia helps organisations and individuals create the value they're looking for. With over 6,000 staff nationally we are a member firm of the PwC network globally and one of Australia's leading professional services firms. We assist a range of clients including Australian businesses, not-for-profit organisations and governments to assess their performance and improve the way they work. Underpinning our success is our firm vision "To realise and discover the potential of..." which is achieved through our values of Performance Matters, Have a Go, Be Open and Authentic, Hunger for Growth, Embracing Differences and Care.

Join PwC's Cyber Security team as a Penetration Tester and provide clients with an end-to-end solution to building cyber resilience.

About the role:

You will provide hands on expertise around assessments of the information and operational technology environment of our clients, and formulate recommendations to better manage their business risks.

- Proficient in penetration testing and vulnerability assessments of applications, systems and networks
- Review and recommend business process improvements and technical improvements to systems, applications and network security controls
- Incident response services
- Report and present to technical and business stakeholders

About you:

- Between 2 to 5 years of experience working within IT security
- Have completed or working towards relevant professional qualifications (OSCP/ CREST/ GPEN/ GCIH)
- Familiar with mobile device programming/ security
- Knowledge of cyber security principles and practices
- Possess advanced analytical and problem solving skills
- Have working knowledge of the following:
  - Network security
  - Security architecture
  - One or more scripting programming languages
  - One or more web development programming languages
- Microsoft Windows and Active Directory security
- Linux security
- Database security
- Wireless security
- Security testing methodologies
- Security source code assessment methodologies
- Eligibility to obtain and maintain an Australian Government security clearance

The offer at PwC:

PwC is one of Australia’s leading professional services firms, bringing the power of our global network of firms in 157 countries to help Australian businesses, not-for-profit organisations and governments assess their performance and improve the way they work.

The PwC Australia experience will offer you the opportunity to work with the best people and technology, flexible working arrangements, activity based working, a diverse work place, up to 18 weeks paid parental leave and embedded cultural values in everything we do. We offer reward and recognition for your efforts so you can realise your potential through coaching and career development.

How to apply details:

Ready for the opportunity of a lifetime? Apply online now.

PRIVACY@WORK Summit

Connect and enhance your privacy knowledge

Hear from three international privacy thought leaders Bojana Bellamy (UK) – President, Centre for Information Policy Leadership, Hunton & Williams LLP, Marie Shroff (NZ) – former New Zealand Privacy Commissioner and iappANZ Privacy Hall of Fame inductee, Hilary Wandall (USA) – Assoc. Vice President, Compliance + Chief Privacy Officer, Merck.

Webcam, by kind permission of artist, Sherry Karver, Rebecca Hossack Gallery

Three keynotes, five panel discussions, 24 panelists exploring themes: Managing Privacy – a stakeholder perspective, Metadata Conversation, New Technologies and Privacy Impacts, Privacy in Sport and The Politics of Privacy.

When:    Wednesday 18 November, 9.00am to 6.30pm, incl. AGM & networking time

Where:   ZINC, Federation Square, Melbourne

Earlybird:    Now closed

Details:  www.iappanz.org/events

Join us for a full day of insightful information and discussion regarding best practices, new trends and guidance on opportunities in the field of privacy.
## Privacy Events

<table>
<thead>
<tr>
<th>Time, Date &amp; Location</th>
<th>Information</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tuesday 17 November</strong>&lt;br&gt;4.00pm – 7.00pm&lt;br&gt;Baker &amp; McKenzie&lt;br&gt;Level 19, 181 William Street&lt;br&gt;MELBOURNE</td>
<td>Privacy in Pharma seminar and Q&amp;A&lt;br&gt;Are you across the new transparency requirements introduced by the updated Medicines Australia Code of Conduct? Would you like to gain an overview of the changes and how these may impact your pharmacy company or you as a healthcare professional? Would you like to understand better the requirements when collecting clinical trial participant data and best practices for consent statements and managing data transfers overseas to parent companies?&lt;br&gt;We are offering our Privacy in Pharma Seminar and Q&amp;A again in Melbourne offering insights and best practice guidance when dealing with personal information of participants and healthcare professionals, the new transparency requirements, as well as privacy guidelines for clinical trials from four industry experts.</td>
<td>Free for iappANZ members&lt;br&gt;$99 incl GST for non-members&lt;br&gt;<a href="#">Register here</a></td>
</tr>
<tr>
<td><strong>Wednesday 18 November</strong>&lt;br&gt;9.00am – 6.30pm&lt;br&gt;ZINC, Federation Square,&lt;br&gt;MELBOURNE</td>
<td><strong>iappANZ Privacy@Work Summit</strong>&lt;br&gt;The only event of its kind in the region, the Privacy@Work Summit will provide a forum for people in the privacy arena to connect and enhance their privacy knowledge. The Summit showcases best practices, illuminates new trends and offers guidance on opportunities in the field of privacy.&lt;br&gt;<strong>Keynote speakers:</strong>&lt;br&gt;<strong>Bojana Bellamy (UK)</strong> – President, Centre for Information Policy Leadership, Hunton &amp; Williams LLP. Bojana has over 20 years data protection and privacy executive experience. The Centre is a global information policy think tank and leader in global information policy, privacy and cyber security.&lt;br&gt;<strong>Marie Shroff (NZ)</strong> – A pre-eminent privacy thought leader, former New Zealand Privacy Commissioner and iappANZ Privacy Hall of Fame inductee, Marie will provide independent comment on significant policy issues.&lt;br&gt;<strong>Hilary Wandall (USA)</strong> – Assoc. Vice President, Compliance + Chief Privacy Officer, Merck - a global healthcare company operating in 140 countries. Hilary</td>
<td><a href="#">REGISTER HERE</a>&lt;br&gt;After 7 October 2015:&lt;br&gt;iappANZ Member: $687.50 incl. GST&lt;br&gt;Non-member: $907.50 incl. GST</td>
</tr>
<tr>
<td>Time, Date &amp; Location</td>
<td>Information</td>
<td>Price</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------</td>
<td>-------</td>
</tr>
<tr>
<td></td>
<td>has broad multi-disciplinary experience in HIV research, genetic and cellular toxicology, internet marketing, corporate law, ethics, compliance, privacy and data protection.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Key themes to be explored this year include:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Metadata conversation</strong> – perspectives in protecting sources, confidentiality and whistle blowers</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Internet of everything</strong> – is privacy a disruption to new technologies?</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Politics of privacy</strong> – regulator challenges across jurisdictions - making entities accountable for personal data and the influence global legislation</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Managing privacy</strong> – exploring the internal and external elements at play in a data security breach or privacy management challenge</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Privacy in sport</strong> – advantages, challenges and your rights</td>
<td></td>
</tr>
</tbody>
</table>
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.

Our global body, 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 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.

Our contact details

*Privacy Unbound* is the journal of the International Association of Privacy Professionals, Australia-New Zealand (iappANZ), PO Box 193, Surrey Hills, Victoria 3127, Australia (*http://www.iappanz.org/*)

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)

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