President’s Letter

By Kate Monckton
President
M: 61 409 613 029

Dear Members

I am so excited, honoured and humbled to be writing this as the recently appointed President of the iappANZ after three very enjoyable years as a Board Director. I’m very much looking forward to learning from you all about how iappANZ can help you in your organisations and agencies over the coming year – and have some fun whilst we do it!

The iappANZ Board is made up of an awesome team of volunteers from Australia and New Zealand who are supported by an equally awesome part time GM and team of members who sit on various sub-committees as well as our committed our sponsors, to help us to deliver information and events that we hope you all find valuable and helpful. I’d like to take this opportunity to thank everyone who has been involved over the last year for all their efforts. Without your time, energy and commitment we wouldn’t be the organisation we are today. THANK YOU!

We’re always on the look-out for anyone who would like to get involved in any of the activities we are running (or have ideas for new ones). That could be writing an article for the Bulletin, speaking at an event, being on a sub-committee or anything else you think of. If you’d like to be involved in iappANZ activities, please contact our General Manager, Emma Heath (emma.heath@iappanz.org). On that note, if you have any feedback, suggestions or comments at all, I’d love to hear them.

This year’s summit in Melbourne was on another level. We were packed out to capacity in a fantastic venue in Melbourne with amazing, engaging speakers and I think I heard the most laughs I have ever experienced at a privacy event! I was personally ecstatic to see how many members from New Zealand had made the trip over, we really are an ANZ organisation. Thank you to everyone who helped make it such a success.

I can’t wait to see what 2016 has in store for us and our profession. I hope you all enjoy a well-deserved summer break - I’ll be back home in England - no doubt whingeing about the cold and absence of seafood at Christmas dinner, but enjoying the company of friends and family and my very new baby niece.

I’m really looking forward to another great year with you all – roll on 2016!

Kate
Dear Members

The last edition of Privacy Unbound for the year promises a great beach read.

December has produced a few important legal and regulatory developments, summed up by Board Director and Rio Tinto Global Privacy Counsel, Carolyn Lidgerwood. Firstly, text for the new European Union Data Protection Regulation was agreed in Brussels this month. It is anticipated to be formally adopted in 2016 with a transition period of 2 years. See page 12 for a hot off the press summary provided by one of our keynote speakers at the recent iappANZ Privacy@Work Summit, Bojana Bellamy from Hunton & Williams. Of no lesser significance – and indeed long awaited news in Australia – consultation has now opened on the exposure draft of the Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 (the Bill). Following consultation, the Bill is proposed to be introduced into Parliament in 2016. And finally, iappANZ congratulates Philip Green on his appointment as the new Privacy Commissioner for Queensland. All the links you need to read up on these developments are in Carolyn’s summary on page 4.

If you missed the iappANZ Privacy@Work Summit, turn to page 5 for a view from the floor by Lucy Scott, a Sydney based privacy consultant and lawyer. Lucy reflects on the “frank confessions” of colleagues, the reflections of regulators, and the insights of entrepreneurs who shared their views and insights at the Summit.

More about the Summit on page 11 and 12 with Board Director and Secretary of iappANZ, David Templeton who recaps the panel discussion on new technologies and future privacy featuring Ben Carr (Chief Privacy Officer, Telstra), Ron Bartsch (Managing Director AvLaw, Chairman AvLaw International), Ros Harvey (Founder and Managing Director, The Yield) and Stephen Wilson (Analyst and Adviser, Digital Identity and Privacy, Lockstep). Aforementioned multi-tasker Carolyn Lidgerwood also recaps on a panel – this time “The Politics of Privacy”, the closing panel featuring the Summit’s three accomplished keynote speakers – Marie Schroff, Hilary Wandall and Bojana Bellamy.

The iappANZ’s Annual General Meeting followed the Summit on 18 November and iappANZ Secretary David Templeton presents its notable outcomes. In this context, the Board would like to welcome new Director Alex Webling. A Director of Resilience Outcomes, a consultancy specialising in identity, biometrics and information security, Alex will be known to readers of Privacy Unbound as a former winner of the writing prize. We welcome his contribution in 2016. More about Alex on page 9. We’d also like to acknowledge Peter Leonard’s decision to retire from the board. Peter served as director since November 2012 and brought a tremendous depth of knowledge and a wonderful sense of humour. We want Peter to know that now that we know all of his vital personal information, retirement from the board may be a slippery notion.

In the excitement over the proposed mandatory data breach legislation, a little known bill known as the “Gladiator Bill” has been introduced by Bob Katter MP. Known in full as the Privacy Amendment (Protecting Children from Paparazzi) Bill 2015, the Bill would insert a new criminal offence provision into the Privacy Act for anyone who, without consent, harasses children of celebrities or of any other person due to that person’s vocation or occupation, who are aged under 16. iappANZ Board Director and Special Counsel at Minter Ellison Veronica Scott together with Perry Singleton, a vacation clerk with Minter Ellison share their views on the problems with the Bill and the implications of the proposed reforms.

And finally, for those who missed out on finding out whether Bradley Cooper is a bad tipper, Anna Johnston, Director, Salinger Privacy knows the answer and as the winner of the iappANZ’s 2015 Writing Prize has written about it really well. Originally appearing in the September-October edition of Privacy Unbound, we are happy to republish her winning article “Bradley Cooper’s taxi ride: a lesson in privacy risk”.

For those who don’t usually make it to the end of Privacy Unbound, that is where the job ads are. And as Christmas passes and you write your new year’s resolutions, perhaps IIS or Air New Zealand are calling.

Finally a big shout out and thank you to all members, sponsors and friends for your contributions in 2015. I wish you and your families a happy and healthy festive season and all the best into the new year.

Melanie

By Melanie Marks
Vice-President
melanie.marks@cba.com.au
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=.gdr_1281574752237_1

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

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!
Stop the press … current developments in privacy

by Carolyn Lidgerwood

As we go to print with the final issue of Privacy Unbound for 2015, we’ve received some Christmas presents for privacy professionals – in the form of some important legal developments. Here are some things to add to your reading pile over the festive season …

1. New European Union Data Protection Regulation

On 15 December 2015, agreement was reached in Brussels on the final text of the new General Data Protection Regulation (GDPR). It is anticipated that the text will be formally adopted in 2016 and that there will be a transitional period of 2 years.

In this edition of Privacy Unbound we have included a ‘hot off the press’ summary provided by one of our keynote speakers at our Privacy@Work Summit, Bojana Bellamy from Hunton & Williams.


2. Mandatory reporting of serious data breaches in Australia

On 3 December 2015, consultation opened on the exposure draft of the Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 (the Bill). Following consultation, the Bill is proposed to be introduced into the Parliament in 2016.

The Bill would require Government agencies and businesses subject to the Privacy Act 1988 to notify the OAIC and affected individuals following a ‘serious data breach’.


3. New Privacy Commissioner for Queensland

On 11 December 2015, it was announced that Philip Green has been appointed as the new Privacy Commissioner for Queensland. The media release from the Queensland Information Commissioner Rachael Rangihaeata noted as follows:

Throughout his career, Mr Green has worked in many different Queensland Government roles and in private practice. Most recently, Mr Green was Executive Director, Small Business – Department of Tourism, Major Events, Small Business and the Commonwealth Games and held that position from 2008. Mr Green has a Masters in law, majoring in technology law including privacy, regulation of the internet and media.

iappANZ congratulates Mr Green on his appointment.

Carolyn Lidgerwood is a board member of iappANZ and Global Privacy Counsel at Rio Tinto.
Privacy@Work – the 2015 iappANZ Summit
A view from the floor

by Lucy Scott

It’s easy to forget the meaning of work in the day to day of doing. Time out at iappANZ’s Summit is a tonic for workers at the information privacy coalface. Unabashedly focussed not just on the mechanics, but the why of what we do, this was a rare opportunity to learn from the frank confessions of colleagues, the reflections of regulators, and the insights of entrepreneurs using new technologies to make a difference to individual and social well being.

A recurring theme at this year’s Summit was that privacy is about more than compliance; and that effective compliance requires an ethical, not just a risk-based approach. The meaning of privacy matters not least because awareness about the evolution of privacy regulation, including its genesis as human right, provides a touchstone to test our effectiveness as privacy professionals in the rapidly evolving technological and commercial landscapes of work.

Timothy Pilgrim, Australian Privacy Commissioner, fresh from the International Privacy Conference in Amsterdam, kicked off with the ‘elephant in the room’ - the impact of the EU decision in the Schrems case on Australian businesses. Timothy’s short answer was that it is business as usual for cross-border disclosures of personal information (and that APP guidelines on this remain relevant); although he noted that multinationals are likely to feel the direct impact of a shift in EU data protection standards in the wake of Schrems.

A number of expert panellists working in or with multinational corporates took this point further throughout the day, advocating Schrems as a privacy ‘door opener’ at executive level, and advising practitioners to reassess whether existing mechanisms such as model contracts effectively meet their own and their clients’ data protection obligations.

Back home, data breach reporting - with or without the Federal Government’s promised mandatory reporting scheme - and the new metadata retention scheme, will be foci of the OAIC in the coming year. It was interesting to learn that the OAIC has commenced assessments of how the Department of Immigration handles personal information under the Department’s new Foreign Fighters Act powers; and that the OAIC plans to assess whether telcos are adequately protecting metadata retained under the Telecommunications Act (the logical fall out from the OAIC’s determination in Grubb and Telstra).

Timothy’s final message for businesses: assume that so-called anonymous data is personal information, and protect it as such.

The value of metadata lies in how richly it speaks to our ‘web of relationships’, as Moira Paterson noted on the Summit’s diverse opening panel. Drawn from media, Parliament, academia, and the technology and information security industries, the panel generally acknowledged the chilling effect of the new metadata regime on journalism. We heard that work-arounds are being found in old techniques - snail mail and source referrals to colleagues for uncompromised first contact - and in new technologies such as metadata-free instant messaging tools (shameless plug from the panel technologists).

For telcos, panellists pondered how hundreds of micro providers, let alone the big players, will manage and resource their obligations under the metadata regime. And how will the Federal regime expand the capacity of State agencies to obtain personal information, often under enabling legislation which is silent on whether such collections are reasonably necessary or proportionate? What checks and oversight mechanisms will temper indiscriminate, third party collections of metadata? What other unintended consequences will play out as the metadata regime matures?

Marie Schroff, the former New Zealand Privacy Commissioner, treated participants to a strategic overview of the seismic shifts in the ‘privacy power game’ in her irreverent keynote address. State and corporate power relies on mass surveillance and data aggregation to an extent unforeseen in recent memory. At the same time 3 billion individuals currently make use of internet-devices for their own diverse purposes. The challenge for privacy professionals is to engage with the ‘information privacy players’ in ways that enhance personal control in the context of vast, global information networks. These networks are not ethical vacuums, and Marie challenged...
the Summit to ponder the possibilities of bringing balance to the ‘privacy power game’ - through enhanced voluntary customer participation; genuine organisational privacy maturity backed by the kind of auditing applied to monetary transactions; and willingness on the part of privacy regulators to exercise their public mandate.

The business of managing privacy was interrogated by a range of overseas and domestic experts, frankly sharing their best successes and stuff ups. In her keynote speech Hilary Wandall compared the privacy landscape in 2000 with that in 2015, noting the current proliferation of privacy laws around the world. Hilary described the challenges faced by a global company in developing a ‘future proof’ privacy program across 140 countries, and how identification of core values and fundamental privacy principles could be used to form the basis of global procedures and practices (in addition to compliance with specific local obligations). A particular focus was how to get the business to ‘own’ the privacy program and to be accountable in practice. Hilary provided some insights on strategies that had worked in her company, from simplification of communications, to annual compliance sign-offs from people across the business, to ensuring that privacy impact assessments fed into that annual certification.

Expert practitioners from New Zealand and Australia spoke of valuable hard lessons out of their responses to data breaches. The importance of building in a personal response to incident management was a key theme. Since a breach of privacy is felt inherently as personal harm, then our response should as far as practicable be personal. Otherwise aggrieved individuals are likely to feel treated as a number; at worse the response blames the victim (ouch, it really does happen, usually when there is ‘institutional privacy blindness’). This underscores the value of an ethical lens across privacy management practices, and more complex measures of privacy maturity.

We heard from big players that a transparent and personal response to data breaches can in fact build consumer trust and, even in the glare of high profile and high volume incidents, retain relationships with each customer who has suffered harm. We were reminded too (courtesy of Russell Burnard), that swift incident management depends on thorough preparation and is quite different from panic-button mode.

Michael Rivette from the Victorian bar informed us that privacy litigation is alive and well, although it may not be making headlines. Australian privacy litigation is also creative (the Privacy Act and State counterparts being one cause of action among others), and potentially powerful, especially if it involves a class action. However if you are relying on the Privacy Act, Michael implored us to go back and read the preamble (as is his habit for the bench when presenting his client’s case). Right there, we are reminded that the basis of the entire Act is the human right of privacy as protected in the International Covenant on Civil & Political Rights. Michael’s parting tip for businesses? Mitigate the harm caused by your data breach - and your damages bill - as quickly as possible.

In a ‘nerds versus jocks’ breakout, lucky nerds learned about some exciting technological developments and disturbing possibilities. Entrepreneur Ros Harvey is giving oyster farmers and food regulators sustainable production data using the Internet of Things. Aviation expert Ron Bartsch surprised many with the stunning figure of 50,000 drones that currently operate in Australia, including in non-navigable airspace, 250 of which are licensed.

And what better opportunity than a room full of privacy experts to challenge whether the fundamentals of information protection (statutory privacy principles) and current privacy management approaches (privacy by design) actually work? At least one panelist questioned the usefulness of privacy by design and rejected the privacy professional’s mantra, ‘privacy is good for business’. However, the overwhelming view from panellists and the floor was that privacy principles and privacy by design continue to provide flexible and effective frameworks - if they are properly resourced. Just be sure that you’re ‘gutsy’ with your advice - the privacy principles are always open to interpretation, so it may as well be yours (thank you, Bojana Bellamy). Your management may even thank you for it one day, as Hilary Wandall reminded us.

Bojana Bellamy’s keynote view from Europe spoke of mandatory data breach notification as a privacy game changer, going to the heart of organisational risk and reputation. More than ever privacy will be a board-level issue and a measure of accountability. Bojana rejected the concept of consent in the context of big data and technological innovation; and yet challenged us to re-think privacy notices from a company insurance policy to a form of genuine transparency and something meaningful to people asked to read them.

Finally, how very refreshing to close with an all-female panel of experts and chair. This should hardly be remarkable, and yet it is no small achievement when so many conference panels still comprise so few or no women (just talk to anyone who has attended a recent...
start up or tech conference!). It bodes well for the future of the privacy profession that its Summit leads with genuine representation from the ‘other 50 per cent’ of talent across the industry.

Lucy Scott is a Sydney based privacy consultant and lawyer

The Closing Panel from the 2015 iappANZ Summit ‘The Politics of Privacy’
Left to right: Keynote speakers Bojana Bellamy, Hilary Wandall, Marie Schroff with panel chair Greer Harris
We'd like to thanks the members who attended our Annual General Meeting which followed Privacy@Work in Melbourne on 18 November 2015.

Our retiring President, Anna Kuperman, spoke to the key opportunities for iappANZ in 2016, including starting the development of regionally relevant privacy professional certification and producing a parallel New Zealand annual summit.

Our Treasurer James Kelaher presented detailed financial statements.

As we had received more nominations for the Board than places available, we conducted a ballot for the contested officer roles and for our ordinary Director roles.

We are pleased to announce the following Board was elected to lead iappANZ through 2016:

President: Kate Monckton
Vice President: Melanie Marks
Treasurer: James Kelaher
Secretary: David Templeton
Directors: Anna Kuperman, Tom Bowden, Emma Hossack, Veronica Scott, Malcolm Crompton, Carolyn Lidgerwood, Olga Ganopolsky, Alex Webling

We thank Anna Kuperman for leading us through 2015, and welcome our incoming President Kate Monckton.

We welcome Alex Webling of Resilience Outcomes to the Board. Alex will be known to readers of Privacy Unbound as a former winner of the writing prize, and we have worked with Alex before, and we know he’ll have a lot to contribute.

We’d like to acknowledge Peter Leonard’s decision to retire from the board. Peter served as director since November 2012 and brought a tremendous depth of knowledge and a wonderful sense of humour. We thank Peter for his enormous contribution and look forward to working with Peter and Gilbert + Tobin where we can. We’d also like to say a special thanks to Peter’s assistant Carina Murray for her help with hosting iappANZ events at Gilbert + Tobin.

Kate Monckton closed the meeting by expressing our appreciation to the nominees who missed out. They were all very strong candidates. We strongly encourage them to nominate again for 2017, and want to emphasise Kate’s encouragement to them to join the ‘extended board’ to help us deliver an exciting 2016, whether through joining our subcommittees or on other initiatives. This invitation is open, of course, to all members. If you are keen to participate, please let Emma Heath know at emma.heath@iappanz.org or on 043 767 588.

/
Introducing new iappANZ board member – Alex Webling

Alex has been a Director of Resilience Outcomes Pty Ltd since 2012.

Resilience Outcomes is a consultancy specialising in identity, biometrics and information security. Prior to this, Alex was a senior executive in the Australian Federal Government in national security for two decades. Alex is deputy chair of Security Professionals Australasia, a member of the Standards Australia Board on Security and Resilience (MB-025) and Associate of the Australian Risk Policy Institute. He is a registered security professional in the area of Enterprise Security.

He lives in Brisbane with his partner, two children and a standard poodle called Cleaver.
The Wrap: Observations from Privacy@Work

1. New technologies and future privacy

By David Templeton

The panel: Ben Carr (Chief Privacy Officer, Telstra), Ron Bartsch (Managing Director AvLaw, Chairman AvLaw International), Ros Harvey (Founder and Managing Director, The Yield) and Stephen Wilson (Analyst and Adviser, Digital Identity and Privacy, Lockstep)

This was the popular choice, attracting about 90% of delegates. I am assured, though that it was matched for content value by the parallel session built around privacy in sport.

There were a number of high points, starting with the very able, brisk and entertaining chairing by Carolyn Lidgerwood (iappANZ Director and Global Privacy Counsel, Rio Tinto). The only low points were the flight patterns of unregulated drones – but I’ll come to that.

Stephen went first, with sobering observations on data science. Citing the now famous case of Target’s impressively accurate art of pregnancy detection from purchasing patterns and social media’s ability to attribute names to facial images from which biometric parameters can be drawn, Stephen challenged the notion that drawing inferences on data based observations is merely a use of data. Stephen made a strong argument that analysis can cross the line to constitute an entirely new collection, potentially requiring notification.

Ros, an entrepreneur and innovator, spoke to the enormous value that can unlocked via smart, linked devices and analytics, aka the ‘internet of things’. She gave the practical example of a product her firm is about to commercialise. The product maximises oyster harvesting opportunities by tracking salinity. Low salinity indicates dangerous rainwater run-off, presenting an infection risk. Salinity monitoring for runoff, rather than reliance on weather and rainfall observations, gives a far more precise and wider window for safe harvest.

There are many more examples of cases where connectivity can be harnessed to build valuable data, and Ros predicts rapid proliferation of smart devices and significant increases in their utility in coming years.

Ben Carr described some of the great work Telstra is supporting in the area of start up incubation and reported on the excitement of working with innovators and entrepreneurs.

Ron Bartsch, partway through his doctorate on Unmanned Aircraft Vehicles (UAVs) and their impact on society, pointed out that there are about 50,000 potentially privacy-invading drone aircraft in Australia of which about 50 are regulated by CASA. The rest have avoided regulation by remaining below 400 feet and thereby staying out of regulated airspace. Ron asks how long that will remain the case, given the range of risks drones present, and cautions that the sheer utility of drones coupled with their cost-effectiveness calls for balanced regulation.

David Templeton is a board member of iappANZ and its recently re-elected Secretary.

2. The Politics of Privacy

By Carolyn Lidgerwood

The closing panel featured the Summit’s three accomplished keynote speakers – Marie Schroff, Hilary Wandall and Bojana Bellamy, with insightful chairing by Greer Harris from Astra Zeneca. The topic – ‘The Politics of Privacy’ - was a good way of bringing together many of the themes that had been discussed during the day.

From the challenges of cross-border data flows around the globe (particularly in the wake of the Schrems decision), to dealing with similar but not identical legal regimes, to developing practical compliance frameworks that need to pass muster with different national regulators – it is important to understand the political overlay.
Marie Schroff observed that the European Court of Justice (CJEU) decision invalidating the US Safe Harbour scheme (as a basis for authorising EU to USA personal data transfers) has the potential to disrupt global business. When we also consider the questions arising from the ‘Snowdon affair’, we are in unchartered legal and economic territory.

Marie noted that the CJEU decision suggests that EU member states can also review previous ‘adequacy’ decisions of the European Commission. In that context, it is possible that questions could arise about the ‘adequacy’ of New Zealand privacy law because of its security arrangements (again, the spectre of Snowdon appears ...). While the current expectation is that the existing adequacy decisions will be ‘carried over’ under into the new regime under the new EU Data Protection Regulation, those decisions can be reviewed at any time. That introduces an air of uncertainty – which is unfortunate given the heavy labour involved in obtaining EU adequacy!

Bojana Bellamy talked about the need to build ‘privacy bridges’ between the different schemes authorising trans-border data transfers. Binding Corporate Rules and the EU Model Clauses are not the same as US Safe Harbour, but this needs to be explained and understood. Bojana discussed the current state of play following the CJEU decision, and that with respect to EU to US personal data transfers there is effectively an enforcement ‘moratorium’ prior to 31 January 2016 (following an announcement by the European Commission). Bojana noted that the European Commission has undertaken to complete the ‘Safe Harbour 2.0’ negotiations by that date, but even so, countries such as Spain are not honouring the moratorium, and are asking questions of companies that have previously notified data transfers in reliance on US Safe Harbour. So much for the moratorium!

Hilary Wandall emphasised that we need to focus on those things that we do have control over – that is, protecting personal data and building compliance frameworks. We should be reviewing our data flows and considering key risks and what we can address now to make them compliant (including ‘model contracts’ for EU personal data flows). It was observed that the CJEU decision has unfortunately diverted resources to data flows and away from more important things like developing privacy by design and growing accountability. In light of the Schrems decision, going forward, we will need to be able to explain our processes for considering requests for access to personal data – particularly by Government agencies. As Marie noted at the outset, that is something that is not a US-specific issue.

It was a treat to hear from this excellent international panel and to learn from their experience.

Carolyn Lidgerwood is a board member of iappANZ and Global Privacy Counsel at Rio Tinto.
The EU General Data Protection Regulation

Reprinted from the Hunton & Williams Privacy & Information Security Law Blog
(Thanks to Bojana Bellamy, keynote speaker at iappANZ’s recent Privacy@Work Summit).

On December 17, 2015, after three years of drafting and negotiations, the European Parliament and Council of the European Union reached an informal agreement on the final draft of the EU General Data Protection Regulation (the ‘Regulation’), which is backed by the Committee on Civil Liberties, Justice and Home Affairs.

The Regulation replaces Directive 95/46/EC (the ‘Directive’), which was enacted in 1995, and will significantly change EU data protection laws. Once officially adopted by the European Parliament and the Council of the European Union, it will apply in EU Member States after a period of two years.

The Regulation will significantly affect businesses in all industry sectors. Below is a summary of key changes to the EU data protection landscape under the informal text published on December 17:

**Harmonization of Legislations**

- **One-Stop-Shop**. Where a business is established in more than one EU Member State, the data protection authority (‘DPA’) of the main establishment of the business will act as the lead authority for the business’ cross-border processing. In addition, each DPA will have jurisdiction over complaints and possible violations of the Regulation.

- **Reduction of Administrative Burden**. National registrations and prior authorization registrations will be abolished by the Regulation. Each controller will have to maintain a record of its data processing activities, however.

- **Legitimate Interest**. Under the Regulation, throughout the EU, legitimate interest will become a legal ground for lawful processing and in certain circumstances, for international transfers of personal data.

**Wider Scope**

- **Territorial Scope**. The Regulation will apply to the processing of personal data by controllers or processors established within the EU. The Regulation also will apply to controllers and processors established outside the EU, where their processing activities relate to the offering of goods and services to individuals in the EU or to the monitoring of such individuals’ behavior.

- **Definition of Personal Data**. The definition of personal data will cover a wider range of data types, including online identifiers or any factors specific to the individual’s physical, physiological, genetic, mental, economic cultural or social identity.

**Increased Obligations**

- **Consent**. Under the Regulation, consent must be freely given, specific, informed and constitute an unambiguous indication of the data subject’s wish to, either by a statement or by a clear affirmative action, agree to the processing of his or her personal data.

- **Consent for Children’s Data Processing**. Parental consent is required for the processing of personal data of children under age 16. EU Member States may lower the age requiring parental consent to 13.
• **Mandatory Data Protection Officer.** The designation of a data protection officer ('DPO') will be compulsory where (1) the processing is carried out by a public authority or body, (2) the core activities of the controller or processor require regular and systematic monitoring of individuals on a large scale, or (3) the core activities of the controller or processor include processing certain types of data on a large scale, including data relating to criminal convictions and offenses. In other situations, a DPO may be appointed by the controller or processor on a voluntary basis, or must be appointed where required by EU Member State law.

• **Privacy Impact Assessments.** Controllers will be required to perform a data Privacy Impact Assessment ('PIA') where the processing of personal data likely involves high risk to the rights and freedoms of individuals. In particular, a PIA will be required for automated data processing activities, including (1) profiling leading to decisions that produce legal effects for the individual, (2) where the processing includes large scale processing of certain types of data, or (3) systematic monitoring of a publicly accessible area on a large scale.

• **Privacy by Design and by Default.** Controllers will be required to establish and maintain appropriate technical and organizational measures (e.g., such as pseudonymization) to implement data protection principles in an effective way and to integrate necessary safeguards for data processing. In addition, appropriate technical and organizational measures also must be implemented so that, by default, only data necessary for each specific purpose of processing is collected.

• **Data Breach Notification.** In the event of a data breach, controllers must notify the competent DPA without undue delay and, where feasible, no later than 72 hours after being aware of the breach, unless the breach is unlikely to result in risk to individuals’ rights and freedoms. Where the breach likely involves high risks to individuals’ rights and freedoms, controllers also must communicate the breach to the individual without undue delay.

• **More Obligations on Data Processors.** The processing of personal data by a processor must be governed by a contract between the processor and the controller. Furthermore, the processor will directly be liable for the security of personal data during its processing activities.

• **Accountability.** Controllers must implement ‘appropriate technical and organizational measures in order to ensure and be able to demonstrate that the processing of personal data is performed in compliance with the Regulation.’

**Strengthened Individuals Rights**

• **Information Notices.** Controllers must take appropriate measures to provide information regarding the processing of personal data to individuals in a concise, transparent, intelligible and easily accessible form.

• **Right to Object.** Where a controller relies on the public interest or legitimate interest as legal basis for the data processing, individuals will be allowed to object to that processing ‘unless the controller demonstrates compelling legitimate grounds for the processing,’ which override the rights of the individual. The individual also will be allowed to object to the processing of his or her personal data for direct marketing purposes, including profiling.

• **Profiling.** Individuals will have the right not to be subject to a decision based solely on automated processing, including profiling, that produces legal effects for them or otherwise significantly affects them. However, profiling will be allowed, if necessary, to enter into a contract between the controller and the data subject, if authorized by the law of a Member State that provides measures to safeguard the data subject’s rights, or when based on the data subject’s explicit consent.

• **Data Portability.** The Regulation will allow individuals to receive personal data concerning them in a structured, commonly-used and machine-readable format. Individuals also will be able to request, where technically feasible, that the controller send his or her personal data to another controller.
• **Right to Erasure.** Subject to certain exceptions, individuals will be able to request the erasure of their personal data without undue delay.

**Increased Enforcement, Fines and Liability**

• **Right to a Remedy.** The Regulation grants data subjects the right to seek judicial remedies against DPAs, controllers and processors.

• **Right to Compensation.** Individuals will have the right to obtain compensation for damages resulting from violations of the Regulation by a controller or processor.

• **Sanctions for Non-Compliance.** Depending on the provision of the Regulation that is violated, companies may be sanctioned with fines up to € 20 million or 4% of annual worldwide turnover.

• **Supervisory Authorities Enforcement Powers.** DPAs will be given wide-ranging powers to enforce compliance with the Regulation, ranging from the power to order the controller or processor to comply with a data subject’s request, to the power to impose a ban on data processing.

• **European Data Protection Board (‘EDPB’).** The Regulation grants the EDPB the authority to issue opinions, adopt binding decisions on the application of the Regulation, and issue guidelines, recommendations and best practices.

**Cross-border Data Transfers**

• **Data Transfers.** Transfers of personal data outside the EU will be allowed where the European Commission has issued an adequacy decision regarding the level of data protection provided in the jurisdiction where the data is transferred. Previous adequacy decisions issued under the Directive will remain in force. In addition, transfers of personal data will be allowed based on legitimate interest if the transfer is not repetitive and concerns only a limited number of individuals.

• **EU Model Clauses.** Under the Regulation, no specific authorization from DPAs will be required with respect to EU Model Clauses. In addition, EU Model Clauses approved by the European Commission under the Directive will remain valid under the Regulation.

• **Binding Corporate Rules (‘BCRs’).** The Regulation officially recognizes BCRs as a valid mechanism to transfer personal data outside the EU.

**Next Steps**

The informal agreement will be discussed at the Council level, in the Committee of Permanent Representatives on Friday, December 18, 2015. The Regulation still has to be voted on by the European Parliament in plenary during spring 2016, or if no further discussion is required, by early 2016.

See the European Parliament press release.

A ‘Gladiator’ Bill for children: More reforms proposed to Australian privacy laws

by Veronica Scott and Perry Singleton

Before Federal Parliament called time on 2015, Bob Katter MP introduced his own proposal to amend the Privacy Act 1988 (Cth). In full, the title of the Bill is the Privacy Amendment (Protecting Children from Paparazzi) Bill 2015. Katter in short calls it the ‘Gladiator Bill’.

The Bill would insert a new criminal offence provision into the Privacy Act for anyone who, without consent, harasses children of celebrities or of any other person due to that person’s vocation or occupation, who are aged under 16. The harassment of such a ‘victim’ could be in the form of taking or attempting to take a photograph or other recording of the child’s image or voice, following or lying in wait for them. The offence will be committed if this conduct actually causes the child, or would cause a reasonable person, to be annoyed, alarmed, tormented, terrorised, or to experience emotional distress.

Breach of the offence could mean a penalty of up to 200 penalty units. With the recent increase in the value of penalty units, that means a fine of up to $36,000.

Why the Bill?

The professed motivation for the Bill is to prevent the families of those in the public eye becoming the subject of unwanted and unwarranted public scrutiny solely by virtue of the identities of their relations. Although the law would apply to the children of any person, Katter’s second reading speech suggests a concern to protect the families of politicians. Speaking to the house, he said ‘There are a lot of people in this place who would like the protection of this Bill... [who] have at one time or another had their families dragged into things that it is very unfair that they be dragged into’.

Problems with the Bill

While the motivation for the Bill is clear, its provisions are less so.

It is uncertain whether the conduct of recording or trying to record a ‘victim’s’ image or voice must include following or lying in wait for them to do so or whether it would simply be an offence to follow or lie in wait for your victim without the intention to photograph or record them. The Explanatory Memorandum doesn't help. The Bill is substantially based on a Californian equivalent, which expresses the conduct as cumulative. However, a summary of the offence provision in the Explanatory Memorandum expresses the two forms of conduct as alternative which means the Gladiator Bill imposes a very low threshold for what makes an offence. At its lowest a person could commit an offence if they follow, without consent, a person under 16, because of the occupation of the child’s carer or guardian, and this is likely to cause a reasonable person in the child’s position to be annoyed, even if the actual victim is not. This contrasts with the requirement in the Californian equivalent for ‘serious annoyance’.

Despite its apparent low threshold, the Bill does not provide any defences to the conduct where it has a legitimate purpose such as being in the public interest. Although a reason in the public interest may mean the child has not been photographed because of the job, vocation or occupation of a relative, the Bill gives no guidance as to where to draw this line.

Implications of the proposed reforms: another restriction on the media?

While the Bill may be yet another example of an attempt to restrict the media and protect individual privacy, its practical implications could prove limited given that small businesses (with an annual turnover of less than $3 million), the media and political activities are
exempt from the Privacy Act. It is for this reason that in recommending a statutory cause of action for breach of privacy, the Australian Law Reform Commission proposed it be a stand-alone law rather than an addition to the Privacy Act.

It is also unclear to what extent the Gladiator Bill would add to the already substantial regulation of media standards in Australia. The commercial radio and television industries are required to observe codes of practice monitored by ACMA which cover either the privacy interests of children or privacy more generally. For print media, the Australian Press Council has its Privacy Standards and in addition, the Media and Entertainment Arts Alliance includes privacy protections in its Code of Ethics. Although these codes do not specifically cover the conduct described in the Gladiator Bill, they would extend to such activities if the media was following, photographing or recording a child.

Veronica Scott is a board member of iappANZ and Special Counsel at Minter Ellison. Perry Singleton worked as a vacation clerk with Minter Ellison. Perry is currently undertaking the Juris Doctor at the University of Melbourne.
Winner of the 2015 Writing Prize

At the 2015 iappANZ summit, Anna Johnston’s article ‘Bradley Cooper’s Taxi Ride’ was awarded the 2015 Writing Prize. Originally appearing in the September-October edition of Privacy Unbound, we are happy to bring it to you again below.

Bradley Cooper’s taxi ride: a lesson in privacy risk

by Anna Johnston

Hollywood heartthrob Bradley Cooper is a bad tipper. That was the conclusion drawn by media – though denied by his PR rep – when data about 173 million New York taxi trips became public.

But I drew a different and more disturbing conclusion, which was how easy it is to get privacy ‘wrong’, when a government official is trying to get transparency ‘right’. Here's what happened.

In March 2014, the New York City Taxi & Limousine Commission (known by the rather sweet acronym TLC) released under FOI data recorded by taxis’ GPS systems. The dataset covered more than 173 million individual taxi trips taken in New York City during 2013. The FOI applicant used the data to make a cool visualisation of a day in the life of a NYC taxi, and published the data online for others to use.

Top marks for government transparency, useful 'open data' for urban transport and planning research ... but not, as it turns out, great for Bradley Cooper.

Each trip record included the date, location and time of the pickup and drop-off, the fare paid, and any recorded tip. It also included a unique code for each taxi and taxi driver.

In theory the identity of each taxi and taxi driver had been ‘anonymised’ by the use of ‘hashing’ – a one-way encryption technique which replaced each driver licence number and taxi medallion number with an alphanumeric code, that can’t be reverse-engineered to determine the original information.

However as a computer scientist who found the published dataset pointed out, hashing is not a good solution when you know what the original input might have looked like. So if you know what taxi numbers look like (and that’s not difficult - they are printed on the side of the taxi), you can run the ‘hash’ against all possible taxi numbers. It took a software developer less than an hour to re-identify each vehicle and driver for all 173 million trips. So anyone can now calculate any individual driver’s income for the year, or the number of miles they have driven, or where they were at any given time. So much for their privacy.

But what’s this got to do with Bradley Cooper, you ask?

Geolocation data exposes behaviour

While the computer science community started debating the limits of hashing and how TLC should have ‘properly’ anonymised their dataset before releasing it under FOI, an astute postgrad student found that even if TLC had removed all the details about the driver and the taxi, the geolocation data alone could potentially identify taxi passengers.

To demonstrate this, Anthony Tockar googled images of celebrities getting in or out of taxis in New York during 2013. Using other public data like celebrity gossip blogs, he was able to determine where and when various celebrities got into taxis. Using the TLC dataset, Anthony could then identify exactly where Bradley Cooper went, and how much he paid. (Mind you, cash tips are not recorded, hence the debate about whether or not he is a bad tipper.)
Anthony also developed an interactive map, showing the drop-off address for each taxi trip which had begun at a notorious strip club. I imagine the same could be done to easily identify the start or end-point for each taxi trip to or from an abortion clinic, a drug counselling service, or the home address of an investigative journalist, suspected whistle-blower or partner suspected of cheating.

As Anthony notes, ‘with only a small amount of auxiliary knowledge, using this dataset an attacker could identify where an individual went, how much they paid, weekly habits, etc … ‘I was working late at the office’ no longer cuts it’.  

**Open data or open sesame?**

The publication of the NYC taxi dataset illustrates a particular challenge for privacy professionals: how easily an individual’s identity, pattern of behaviour, physical movements and other traits can be extrapolated from a supposedly ‘anonymous’ set of data, published with good intentions in the name of ‘open data’, public transparency or research.

Other recent examples have included the re-identification of ‘anonymous’ DNA donors to the ‘Thousand Genomes Project’ research database, and the re-identification of bike riders using London’s public bicycle hire scheme. As the blogger who turned the publicly available bike trips dataset into interactive maps noted, allegedly ‘anonymous’ geolocation data, even when months old, can allow all sorts of inferences to be drawn about individuals – including their identity, and their behaviour.

Closer to home, the NSW Civil & Administrative Tribunal has shown they are willing to challenge, rather than blindly accept, assertions by government agencies about the identifiability of data, by accepting that if a ‘simple internet search’ links the data in question back to an individual’s identity, the published data will meet the definition of ‘personal information’, and its publication or disclosure becomes contestable under privacy law.

For privacy professionals, the goalposts are shifting. An assumption that data has been ‘de-identified’, and is thus not subject to privacy restrictions, may no longer hold true.

Privacy Officers would do well to engage with their colleagues who might publish or release datasets, such as people working in FOI, open data, corporate communications or research, to ensure they understand the risks of re-identification, and know about their disclosure obligations under privacy law.

You don't want your 'open data' to become 'open sesame'.

Anna Johnston is Director, Salinger Privacy

Salinger Privacy provides specialist privacy consulting and training services.  Salinger Privacy publishes a blog, as well as eBooks on privacy law, including an annotated guide to the NSW privacy laws.  Find Salinger Privacy at [www.salingerprivacy.com.au](http://www.salingerprivacy.com.au)
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).

Privacy Consultant – Sydney

Would you like to work in one of the most challenging interdisciplinary areas of our information driven age and help grow the region’s largest privacy consultancy?

Your role in the future

Information Integrity Solutions Pty Ltd (IIS) has a well established reputation in the niche but growing field of information management, privacy and data protection. It was established in 2004 by a former Privacy Commissioner of Australia.

Our clients value IIS for its:

- Significant dedicated experience in the privacy space, including regulatory experience – IIS staff have over 60 years of combined experience in privacy, its Managing Director was the Privacy Commissioner of Australia between 1999 and 2004
- Practical recommendations and solutions – Our analysis takes into account the needs and concerns of both our client and its customers and goes beyond mere compliance with the law and looks at broader issues including trust and reputation
- Independence and world class reputation – IIS helps its customers get privacy right so as to enhance trust with customers while avoiding unwanted regulatory scrutiny.

Reporting to the Head of Sales and Operations/Deputy Managing Director, the Consultant provides expert privacy advisory services to private and public sector clients locally and globally.

The role requires the possession or ability to rapidly develop excellent knowledge of the practical application of privacy and exceptional stakeholder management to ensure client needs are met. The Consultant will work in close collaboration with the existing and well-established Privacy team.

We can provide you with

- A flexible and collaborative work environment
- Development opportunities to grow your skills as a privacy professional
- A remuneration package that can grow as the company grows

You can help us

- Conduct privacy impact assessments and audits
- Provide written strategic and practical advice
• Conduct research on privacy trends and laws globally
• Prepare presentations
• Contribute to the sustainability and growth of the business

Your skills

This is an excellent opportunity, one that requires a flexible approach to work. You must bring initiative and be self-motivated and bring energy and enthusiasm to the Privacy team to help deliver and continually improve a business with a first class reputation.

• First rate written and verbal/presentation skills
• High level analytical skills
• Autonomous worker, but can work closely with an established team
• Understanding of privacy and its applicability in business and government environments
• Client facing experience
• A background in law, risk, information technology or related discipline would be desirable - Tertiary education in a related field preferred

With these skills you can help us transform businesses and governments as we move to a society where the key assets of business and governments are the intangible information assets, and how they are managed, shape expectations of us all.

To submit an expression of interest in this role, please include a cover letter with your resume, sharing what you can bring to this role to Annelies Moens, at amoens@iispartners.com.
Senior Manager, Data Protection

Auckland job#112199

As Airline of the Year* we have been acknowledged for our in-flight innovations, financial performance, operational safety and motivation of our staff. It is our investment in customer experience, product innovation, operational excellence and people culture that drives our success. The business has set a clear and compelling strategy to deliver improved business performance resulting in sustainable, profitable growth across the Air New Zealand Group. A key Air New Zealand priority is to continuously improve our approach to data privacy and data protection across the organisation to ensure it is aligned to our ambitious digital strategy.

Reporting to the GM Governance, Risk and Compliance, this is a position where you will manage strategic and tactical efforts to deliver the Privacy Roadmap to reflect global best practice. The role is responsible for supporting the Group’s adherence to applicable privacy laws and regulations across multiple global jurisdictions.

As the Senior Manager, Data Protection, you will also be expected to maintain a commercial focus and to facilitate a pragmatic approach to privacy and data protection to support commercial goals ensuring compliance with global privacy and data protection is maintained. As a senior leader in the industry, you will promote organisational culture that respects data privacy and ensure that privacy and data protection is considered in business processes and in the development of new products and services. Overseeing the ‘virtual privacy office’ you will play a key role in managing Air New Zealand’s privacy risk as we embrace digital transformation whilst working in collaboration with key stakeholders across the business to achieve key business objectives. Commercially pragmatic, you will help to shape key decisions and bring Privacy policies and processes to life.

With high visibility at the Executive level on all privacy and data security matters, you will be an expert in this field with well-connected networks and proven experience across global jurisdictions in a complex, commercial environment working with big data.

Make your mark as we embark on a journey of change and innovation, and take Air New Zealand Data Privacy towards a world class approach.

Applications close Wednesday 20th January 2016. Click here to apply now or register online at www.careers.airnz.co.nz.

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/](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.