PRIVACY UNBOUNDED

www.iappanz.org
TABLE OF CONTENTS

Letter from the President .......................................................................................................................................................... 3
SESSION 1: Finding the Line – Understanding the regulatory landscape.................................................................................. 6
SESSION 2: Managing the Future of Privacy .................................................................................................................................... 7
SESSION 3: The EU GDPR – its effect in Australia and New Zealand and what to do about it? .................................................. 9
SESSION 4: Update from the New Zealand OPC .................................................................................................................................. 11
SESSION 5: Maintaining the line – Facilitating Safe Data Use Through Safe Settings and Ethical Decisions ....................................... 13
SESSION 6: Why I hijacked Privacy Awareness Week to win hearts, not minds ..................................................................................... 15
SESSION 7: De-identification practical: what the privacy professional needs to know ........................................................................ 16
SESSION 8: Ethics of Spyware – What happens when you spy on a thief? ............................................................................................ 17
SESSION 9: Cool or Creepy?: Navigating a safe path to unlock the power of big data, AI and analytics .......................................................... 19
BONUS ARTICLE! (Hot off the press after the recent High Court decision) ......................................................................................... 20
Letter from the President

It is with great pleasure that I write this introduction to Privacy Unbound (Summit edition). In this edition, we wrap up one year of enormous change in our profession and herald the start of an even bigger one. Who remembers when privacy compliance meant advising businesses on filing cabinets and limiting access to reports? The world has changed and the era of the privacy professional is here.

“Privacy and Personalisation – Walking the Line” was the theme of the Summit this year, reflecting the challenges of managing privacy in the digital, international and connected economy. Veronica Scott’s introduction will detail the Summit, so it is my intention here to simply recognise the creativity and drive of the Summit Organising Committee, comprising Richard Kilpatrick, Jacqueline Peace, Daimhin Warner and Katherine Sainty. Thank you to this team for the hours of ideation and action. The Summit would not have happened without your respective input, and here I particularly want to call out my Co-Chair, Richard, who has a way of kicking goals quietly and humbly.

The Summit attracted huge interest from mainstream media, including the ABC Radio National Breakfast program with Matt Wordsworth, Interview with Dr Stephen Hardy on ‘confidential computing’ and why it’s important (airing Tuesday 3 October), Mumbrella: iappANZ to explore the line, ZDNet: Australians made over 2,000 privacy complaints to Commissioner in 2016-17, and ABC Television’s “7:30” airing 16 October, featuring Anthony van der Meer on his story and the ethics and legal implications of using spyware, with iappANZ Vice President Veronica Scott.

We are also expecting the imminent publication of feature articles in Bloomberg on the GDPR and its impacts for Australia and New Zealand, and in the SMH on Anthony van der Meer and the impetus for his film plus thoughts on the implications of privacy and protection considering the current facial recognition debate. We will send links to these items when they are released.

Summit Statistics

Diversity was top of mind in planning the Summit this year and I am pleased to report that we had equal male and female attendance and no “all-male” panels. If you have ideas for further diversity (in ideas and backgrounds) next year, we would like to hear from you. Some of the other feedback we have received on the Summit includes running the AGM and voting in of the new Board separately, to ensure that networking drinks are not disrupted and publishing the detailed program earlier. Our attendees have suggested that next year we cover more case studies, practical tips on keeping staff engaged, more on ethics, the future of the privacy officer and the GDPR in action. If you have not completed the survey, I’d urge you to do so now.

More than 40% of our attendees travelled to Sydney for the Summit from other parts of Australia and New Zealand and further afield. We will be actively promoting iappANZ across the region this year. If you would like to be involved in planning or hosting one of our events or initiatives outside of Sydney, please let us know. On that note, next year’s Summit will take place on 1 and 2 November in Melbourne.

New Board and sub-committees

The 2018 Board was elected at our AGM following the Summit. I’d like to welcome the new Board, comprising:

- **Executive**: Veronica Scott (Vice President), Jacqueline Peace (Secretary), Katherine Sainty (Treasurer)
- **Ordinary Directors**: Daimhin Warner, Carolyn Lidgerwood, Christopher Rogers, Marina Yastreboff, Tim de Sousa, Bronwyn Furse, David Templeton and Lyn Nicholson.

In welcoming the new Board, we also farewell some old friends, Kate Monckton, Emma Hossack, Olga Ganopolsky, Marta Ganko and Richard Kilpatrick. Kate has served the Board tirelessly as President for the last two years. We owe a huge debt of gratitude to Kate for the hours, ideas and effort she has continuously given. Kate is one of the most collaborative and kind leaders we have seen, and has been instrumental in establishing capability which will enable the iappANZ to grow over the coming year. Thank you, Kate. We hope to build on the foundations you have established. Longstanding Board member and former President, Emma Hossack also deserves a special mention, having brought her entrepreneurial drive to iappANZ for many years. A driving force and a change agent of the highest calibre, some of you will also have seen Emma speak in the last year on privacy in the health sector and other topics. Emma, we salute you and will miss you! Now on to Olga, who has brought a wealth of technical expertise and depth of experience to the running of the iappANZ for several years. We
hope to continue to work closely with Olga (and the rest of the outgoing Directors) over the coming year and beyond as a leading light of the Australian privacy community.

We also thank every member of our 2018 sub-committees (names over the page) and invite you to continue in these sub-committee roles — or others — over the coming year. Your time and efforts are greatly appreciated. We will be in contact soon to establish 2018 committees.

Last thank you

The 2017 Summit was made possible by our sponsors. I’d like to thank the individuals who bring privacy to life within our sponsor organisations and thank you personally for choosing to continue to support the work of the iappANZ. We have made some changes over the last year to the way we will work with you in 2018, including better planning to ensure sponsor benefits are taken up in the way that best supports your business strategies. We all look forward to seeing you over the coming year.

2017 Sub-committee members

New Zealand Events Committee:
Kerry Bakkerus RIMS
Tom Bowden HealthLink
Fiona Colman Info by Design
Kathryn Dalziel Taylor Shaw
Annabelle Fordham Office of the Privacy Commissioner New Zealand
Katherine Gibson Gibsons Law
Nicola Hermansson EY
Sandra Kelman Privacy Solutions
Deanne Myers KPMG
Jacqueline Peace Air New Zealand
Emma Pond Southern Cross Medical Care Society
Daimhin Warner Simply Privacy

Australian Events Committee
Olga Ganopolsky Macquarie Group Co-Chair
Christopher Rogers Ernst & Young Co-Chair

Certification Advisory Committee
Carolyn Lidgerwood Rio Tinto Co-Chair
Daimhin Warner Simply Privacy Co-Chair
Charles Alexander Legal Consultant
Kerry Bakkerus Counties Manukau District Health Board
Fiona Colman ACC Info by Design
Marta Ganko Deloitte
Katherine Gibson Gibsons Law
Emma Hossack Extensia
Sandra Kelman Privacy Solutions Ltd
Peter Leonard Data Synergies
Jacqueline Peace Air NZ
Dawn Swan Inland Revenue Department, NZ

Journal Advisory Committee
Carolyn Lidgerwood Rio Tinto Co-Chair
Veronica Scott Minter Ellison Co-Chair
Marta Ganko Deloitte
Katherine Gibson Gibsons Law
Emma Kulnitsch Guildlink

Melanie Marks
iappANZ President
Foreword

If you were able to get to the Summit last month, this edition of the journal will remind you of the fantastic and thought provoking sessions you would have heard. But if you couldn’t make it, we are delighted to be able to bring you a full roundup from our outgoing Board and Committee members of all of the keynote sessions, panel events and breakout workshops that filled the day with the theme ’Privacy & Personalisation: Walking the Line’. Here’s a teaser:

- Katherine Gibson starts us off with the opening of the Summit by New Zealand Privacy Commissioner John Edwards who challenged us as privacy professionals to follow the line between unlocking the opportunities of data and maintaining good privacy practices;
- Timothy Pilgrim did a star turn with his full report on the work of the OAIC this year, ranging from development of the Public Service Privacy Code, to preparing for the introduction of mandatory dare to breach notification in February next year, as well as the effect of GDPR compliance, thanks to Chris Rogers for this review;
- GDPR again: Carolyn Lidgerwood reports on the timely and oh so helpful and clear presentation from privacy guru and lawyer Eduardo Ustaran on the GDPR - those notes will be so valuable as more Australian and New Zealand organisations come to understand the extraterritorial impact of the GDPR on their business;
- The fantastic work of the Office of the Privacy Commission in New Zealand was highlighted by Annabelle Fordham’s presentation (thanks again Katherine Gibson) on what they are doing to make privacy easy for agencies. Look out for the planned privacy trust mark that is being developed;
- Jacqui Peace reports on the expert panel lead by Anna Johnson on the safe use of data. Note we had an astrophysicist (from CSIRO) on the panel. The session was absolutely thought provoking, exploring social licence, the use of a data dial, safe models for privacy and security and balancing the need to benefit from the data we collect to enable innovation, value and growth whilst ensuring a good experience for the individuals going on the data journey;
- Melanie Marks reports on Craig Templeton invigorating and refreshing session on the use of digital tattoos and donuts to get people talking about privacy;
- De-identification is becoming such a critical tool in the privacy professionals’ armoury and Anna Johnson’s workshop, as reported by Olga Ganopolsky, was both practical and timely. (It also tested our maths skills.) Tongue twisters techniques of aggregation, suppression, generalisation, pseudonymisation and perturbation (say these all quickly) were explained;
- The ethics of spyware, as highlighted by Anthony van der Meers, the young Dutch film producer of the film Find my Phone which he created after his mobile phone was stolen, led to some interesting discussion about the ethics of spyware apps and mobile phone tracking. This report is brought to you by Marta Ganko and myself. Anthony’s story was picked up by the Australian media and resulted in some great coverage;
- The closing session of the day took us back to that line we walk all the time as privacy professionals and the question we have to keep asking ourselves the question in this era of big data, AI and analytics – is it cool or creepy?. The delightful and unique Laura Bell from SafeStack challenged the panel on what they and their organisations considered acceptable.

Finally, hot off the press from Anna Johnson, a bonus article on ‘dataveillance’ and the concerns raised by the High Court’s approach to the meaning of ‘statistical information’ which has given the ABS a green light to collect opinions from Australians (in this case whether or not marriage equality laws should be introduced) and the potential for this to be connected with other data sets the Government collects about us. This certainly fits in with the theme of the Summit and challenges us to be alert to that line and data creeping.

Please reach out if you have any comments or questions at any time or wish to submit an article for the journal.

Veronica Scott
iappANZ Vice-President
SESSION 1: Finding the Line – Understanding the regulatory landscape

Speaker: John Edwards - New Zealand Privacy Commissioner

Report author: Katherine Gibson, Director, Gibsons Law Limited

We were welcomed to the Conference by John Edwards, New Zealand Privacy Commissioner (via video link) who introduced the Conference theme by providing some insights into how “Walking the Line” can achieve good privacy and data use outcomes.

Often privacy and data use are considered as trade-offs – you cannot achieve both. The Commissioner does not agree. You can have it both ways and it is not a matter of trading off privacy for better data use, or vice versa. This is what he said is “Walking the Line”.

You walk the line by addressing privacy at an early stage in projects that use information. This will help maintain the trust of those affected by the information use. An added benefit to building good privacy practice from the ground up is ensuring the information is accurate and up to date. In the Commissioner’s view, getting this right represents a huge opportunity for the global economy.

After introducing the program, Mr Edwards commended iappANZ for engaging in the many issues to be discussed at the Summit, bringing smart people together to share ideas and experiences on how we all can “walk the line”.

Finally, the Commissioner challenged us all at the Summit to “knock out” a recording of the famous Johnny Cash song Walk the Line. Something, unfortunately (but probably fortunately!) we failed to achieve.
SESSION 2: Managing the Future of Privacy

Speaker: Timothy Pilgrim - Australian Information and Privacy Commissioner

Having just returned from the Information Commissioners’ Conference in Manchester, followed by the Data Commissioners’ International Conference in Hong Kong, Timothy appeared at this year’s iappANZ Summit to provide attendees with an update on the work of the OAIC and evolving issues in the privacy environment.

Timothy advised that the OAIC has been increasingly called upon by members of the public over the year due to an increased awareness of privacy. This came about by several key events bringing privacy concerns into the spotlight. In particular, the 2016 Census demonstrated how essential it is for the Australian Government to clearly communicate privacy practices, in order to build and maintain the public’s support of data use. In addition, de-identification attracted significant media attention this year when a researcher exposed a potential re-identification risk in published medical and pharmaceutical benefits scheme data. The OAIC’s Annual Report for 2017, due to be released later this month, will show that the increase in public interest continues. In the past year, the OAIC has seen a total of 2494 complaints (a 17% increase from the previous year) demonstrating that Australians are becoming increasingly comfortable in exercising their right to lodge a privacy complaint. The public are also becoming more aware of the privacy rights which are afforded to them under the Privacy Act.

Complaints to the OAIC were typically in relation to: Finance; Health Service Providers; the Australian Government; Telecommunications; Credit Reporting Bodies; and Retail. Timothy advised that the most common issues raised in these complaints were: Use and disclosure; Security; Individuals’ ability to access their personal information; Collection; and Quality of information. Despite a significant increase in the number of privacy complaints received, the OAIC has nevertheless managed to improve the rate in which complaints are resolved by 22% over the last year. In addition, 95% of all privacy complaints were resolved by the OAIC within 12 months of receipt, a tremendous result for the Commission.

Looking at the Freedom of Information (FOI) Act and how it interacts with privacy, Timothy advised that an individual’s right to access information is becoming increasingly important. There has been a significant (24%) increase in the number of requests to the OAIC to review the decisions of government agencies which have not released information under FOI. The Australian public are increasingly challenging agency decisions to withhold information. Despite this increase, 80% of all requests to the OAIC were resolved without a formal decision being made. In one-third of cases, the request was resolved by the government agency taking steps to address the applicant’s concern.

Timothy discussed another link between FOI and privacy which demonstrates the OAIC’s broader role. In the last financial year there were 38,000 requests for access to information made to the government under FOI, however 83% of those requests were from people seeking access to their own personal information held by government.

The increase in privacy complaints as well as applications for FOI reviews demonstrates a community expectation about how personal information should be properly managed. Timothy emphasised that the key concept here is transparency – “privacy” does not equate to “secrecy”. Australians are open to new technologies and innovative uses of data, provided there is transparency. Data protection processes and systems which are clearly communicated are the building blocks of consumer and community trust, which is vital in the public and private sectors. Transparent data management practices enables individuals to make informed decisions and enables organisations to demonstrate that they take data protection seriously. Timothy advised that without assurance of data protection, the innovation of data based products and services will struggle to gain user trust. The OAIC is aware that privacy concerns are held by the majority of Australians and inform their decision making. The OAIC’s 2017 Attitudes to Privacy Survey found that 58% of Australians have avoided businesses because of privacy concerns. 44% have decided not to download a mobile App for the same reasons.

The OAIC has also seen the potential for broad public support for personal information being used for reasons that benefit the public. The OAIC supports initiatives which align with the principle that government information is a national resource, where appropriate safeguards are in place to protect individual privacy. In its 2017 Attitudes to Privacy Survey, the OAIC included a new question regarding the use of personal information by the government for research and development purposes. Forty-six percent of people responded here that they were comfortable with their personal information being used for these purposes. However, when the OAIC asked the question without any purpose or outcome, only 33% of people responded in support of such use. Accordingly, Timothy indicated that when you give people more information about how you intend to use their information, their approval increases,
emphasising the importance of governments gaining “social licence” before they go ahead and use information. Australians are willing to consider data sharing and use of technologies when a case for public benefit is made. Timothy advised that there is an ongoing need for rights based regulation that governs the use of data, to provide assurance to individuals that their privacy is prioritized. In summary, a successful data driven economy needs a strong foundation in privacy. Timothy advised that over the past year there have been two main developments: firstly, the Notifiable Data Breaches Scheme (“Scheme”); and secondly the new Privacy Governance Code (“Code”) which he discussed in more detail below.

The Scheme comes into effect in February 2018 and requires businesses and agencies with existing obligations under the Privacy Act to notify individuals whose personal information is involved in a data breach that is likely to result in “serious harm”. “Serious harm” is a qualification introduced to avoid overburdening organisations with the cost of compliance and to reduce the likelihood of notification fatigue to individuals. The Scheme requires organisations to evaluate the impact of a data breach and establish a framework supporting transparency and data protection. There are similar breach notification schemes in operation in the UK, Canada, Korea, Mexico and the United States (and also soon in the EU under the GDPR). Timothy advised that the OAIC is currently preparing resources regarding the requirements of the Scheme, which will be available on the OAIC’s website.

All Commonwealth Government Agencies bound by the Privacy Act are preparing for the commencement of the Code, which outlines their requirements for complying with APP1.2. Through the Code, the OAIC is seeking a single high standard of personal information practice and governance, that will apply to personal information no matter where it travels within the public service. The OAIC is requiring “best practice” for Australian public service Agencies to provide assurance around the protection of personal information, which is necessary for building public confidence in the government’s data innovation agenda. Timothy advised that while the private sector will not be covered by the Code, the OAIC nevertheless encourages us to look at the Code as an example of what privacy best practice entails from the Government’s perspective and the OAIC’s expectations around privacy governance and compliance. One requirement within the Code is for government Agencies to undertake privacy impact assessments (“PIAs”) for any “high risk projects” they undertake. PIAs are a process that all organisations across industry can implement to minimise risk. Timothy advised that in the event the OAIC performs an investigation of an organisation, it will be looking to see what steps the organisation took to build in privacy by design and whether PIAs have been conducted. The Code also requires the designation of a data champion within an agency. A data champion fosters a culture of privacy and provides high level oversight to the organisation’s privacy management framework. The OAIC will be releasing resources dealing with the Code in the coming months.

With both the Scheme and the Code, the OAIC has given the most significant boost to privacy protection and governance since the 2014 reforms to the Privacy Act. Both these initiatives will be implemented in 2018, which is the 30th anniversary of Privacy Act (1988). Timothy advised that the OAIC will continue to work with all government agencies and businesses to realise Australia’s economic and social potential from the ever increasing data driven economy, where privacy plays a fundamental role. The OAIC will achieve this by continuing to provide expert support and guidance on the regulatory landscape and engaging with both the public and private sectors on privacy matters.

Reflecting on the past year, Timothy advised that the OAIC’s Data Privacy Asia Pacific Conference was a great success in stimulating new conversation about data privacy and ethics. Timothy hopes that the OAIC will be able to host a similar event every few years. As previously advised, Timothy has just returned from the 39th International Conference of Data Protection and Privacy Commissioners in Hong Kong (which he referred to as the “UN of Privacy”). The Commissioner’s conference provided discussion and debate on complex issues such as the nexus between data innovation, ethics and discrimination. The GDPR was also a topic of conversation at the Conference as it would also be at the iappANZ Summit. Timothy was pleased to see this, as the GDPR is an issue which impacts on Australian and New Zealand organisations dealing with the EU. The OAIC has developed resources (available on its website) which show the similarities/differences between Australian law and the GDPR.

Timothy concluded his presentation to the Summit by saying that the identification and implementation of processes and systems that safeguard data to the highest possible standard will be a continual challenge as new technologies are developed. At the same time, community expectations in data protection and the use of data continue to change. The sharing of knowledge between industries and regulators is the key to advancing data protection, something which occurred at this year’s iappANZ Summit.
SESSION 3: The EU GDPR – Its effect in Australia and New Zealand and what to do about it?

Speaker: Eduardo Ustaran - Partner, Global Privacy & Cybersecurity Practice, Hogan Lovells, UK

Report author: Carolyn Lidgerwood, iappANZ board director and Head of Privacy, Rio Tinto

Eduardo Ustaran of Hogan Lovells is a big name in EU data protection law, and iappANZ Summit attendees were fortunate to be able to hear him speak about the EU General Data Protection Regulation (GDPR) and how it will impact businesses in our region.

While Eduardo was speaking, there was much furious note-taking around the room – it is clear that this topic generates a lot of interest! In this report, I’ve summarised Eduardo’s key points - for those iappANZ members who couldn’t make it to the Summit or who are now wishing that they had written more down!

Eduardo commenced his presentation by outlining what the GDPR aims to achieve. The current EU Data Protection Directive (dating from 1995) has been implemented by EU member states in different ways – resulting in different approaches in different countries, and a sometimes confusing maze of laws to apply in practice. The GDPR aims to simplify all that, and to put people in control of their personal data.

The Big Ticket Items

Eduardo highlighted some of the ‘big ticket items’ under the GDPR that people need to be aware of:

- **Extra-territorial reach:** No longer will the reach of EU data protection laws be limited to EU ‘establishments’ or to the use of processing equipment in the EU. The GDPR will have an extended reach, including to organisations who offer goods and services to EU citizens, or who monitor the behaviour of EU citizens (including through cookies). As Eduardo put it, if you are looking into the life of someone who is normally based in the EU, the GDPR will apply;

- **Consent:** While consent has always been a pillar of EU data protection law (as a legal basis for personal data processing), what actually amounts to consent will change under the GDPR. The days of implied consent have gone; under the GDPR consent has to be demonstrable, freely given, involving a clear affirmative action and able to be withdrawn. That means no more pre-ticked boxes or assumptions based on inactivity;

- **Legitimate interests:** The ‘legitimate interest’ test is another potential basis for personal data processing (eg as an alternative to consent).

However the legitimate interests of a data controller (ie the organisation or entity that determines the purposes and means of the processing of personal data) must be balanced against the rights of the individual.

Eduardo emphasised that reliance upon ‘legitimate interests’ can provide a stronger case for personal data processing if it is ‘done right’. What I took from that observation was that if you can satisfy the balancing test, and your processing of personal data is also necessary and proportionate to the relevant business purpose, you may be on more certain ground (as opposed to a situation where consent is relied upon, and the consent is withdrawn by the data subject);

- **Transparency:** Under the GDPR, there are no less than 11 items of information that need to be provided to individuals about the processing of their personal data – Eduardo noted the potential for this to lead to very long privacy statements. Certainly, this will mean that GDPR-regulated organisations will need to update their existing privacy statements;

- **Putting People in Control of their Personal Data:** The GDPR provides individuals with broader rights, including rights to information and rights of access, rectification, erasure; plus rights of data portability, objection and the right to restrict certain types of processing;

- **Accountability:** Data controllers will be subject to a broad range of accountability obligations. As Eduardo outlined these, there were some nodding heads around the room (as at least some of these are familiar to Australian-based organisations who are complying with APP1 of the Privacy Act). The GDPR accountability obligations include documentation of data protection policies, undertaking data protection by design and by default, keeping internal records of data processing (replacing most of the current requirements to notify data processing to national supervisory authorities) and co-operation with regulators.

Other areas of accountability include the obligation to keep personal data secure (with
more prescriptive requirements than what exists now) and to notify certain types of breaches to regulators (within 72 hours!) and impacted individuals. There are also obligations to undertake data protection impact assessments (DPIAs) for ‘higher risk’ data processing, and depending on the outcome of those DPIAs, this can require consultation with regulators about the proposed processing activities. Appointment of a Data Protection Officer (DPO) will also be mandatory in some circumstances, with Eduardo noting that it was not mandatory that DPOs be located in Europe;

• **Use of Vendors:** Vendors (generally ‘data processors’) will be more directly regulated and accountable under the GDPR than they are at present; their obligations will extend beyond data security. Critically, data processing agreements must be put in place by data controllers with their data processors, and these must contain specific terms, including in relation to processing in accordance with documented instructions, confidentiality measures, security obligations, sub-processing, providing assistance to the data controller and deletion and return of personal data at the end of the contract and audit rights. Addressing these requirements will be likely to involve a lot of work. If your organisation is going to be regulated under the GDPR — Eduardo’s message is to focus on updating the most important contracts first;

• **International data transfers:** Under the GDPR, there are a range of available mechanisms to protect transfers of EU personal data from the EU, including binding corporate rules, the EC’s standard contractual clauses and approved codes of conduct. For EU to US transfers there is also the Privacy Shield, but Eduardo noted that could be relatively weak (noting the risk of further legal challenges, as occurred with the former EU-US Safe Harbour scheme). It is also worth noting that Eduardo’s presentation occurred before the news broke that the Irish High Court has referred the validity of the EC’s standard contractual clauses to the Court of Justice of the European Union (see the iapp Privacy Advisor for more details);

• **Risks of non-compliance:** The risk of ‘not getting it right’ under the GDPR are more severe; fines can potentially be massive, national regulators can be expected to be active and will co-operate on an international level.

**What to do?**

Eduardo’s key messages were ‘don’t panic’ and to have a plan of action, including:

• **Determine the extent that the GDPR applies** to your business;

• **Review what will be the ‘lawful basis’ for processing.** That is, will you rely on legitimate interests (as balanced against individual rights)? Or will you rely on consent (and if so, how will you obtain that consent?) or on one of the other grounds?

• **Review your transparency mechanisms** (that includes your privacy policy and privacy statements/collection notices) so that people know what personal data is being used for what purpose/service;

• **Develop a Data Protection Impact Assessment (DPIA) process** – this is an important mechanism to show compliance;

• **Prevent and prepare for data breaches.** Consider where and how you are vulnerable?

• **Think strategically about data flows** and where it makes sense for personal data to be processed;

• **View this as an opportunity** – that is, to show you are using personal data fairly and openly and for the benefit of people.

With just over 7 months until the GDPR commences (on 25 May 2018), the countdown is on, and Eduardo made it clear that organisations in our region can and will be regulated.

**Author note:** For Australian organisations, further guidance can be found on the OAIC website (see Privacy business resource 21: Australian businesses and the EU General Data Protection Regulation, as mentioned in the presentation at the Summit from Australian Privacy Commissioner Timothy Pilgrim).
SESSION 4: Update from the New Zealand OPC

Speaker: Annabel Fordham - Office of the Privacy Commissioner, New Zealand

Report author: Katherine Gibson, Director, Gibsons Law Limited

As signalled by John Edwards in his Welcome, his Office Walks the Line by making privacy easy for agencies. In her presentation, Annabel Fordham expanded on this by recapping on what the NZ OPC had achieved in the last 12 months and what was ahead for 2018.

EU Adequacy – work to ensure this is maintained

Following on from Eduardo Ustran’s insightful presentation on the EU GDPR, Annabel Fordham reminded us that New Zealand has EU adequacy status, having been formally recognised by the European Commission (EC) in 2012. This is a significant advantage for New Zealand facilitating the free flow of information from EU countries to New Zealand for processing.

However, questions have arisen on the adequacy status, particularly in light of the delay in New Zealand’s privacy law reform.

Ms Fordham gave us an update on the current status of New Zealand’s adequacy:

- The adequacy status will be continued but is subject to periodic review.
- The NZ OPC understands work is needed to maintain the status and the EC must continue to be satisfied that the NZ law meets the EU standards.
- The EC wants to ensure that any country who has adequacy must continue to meet the standards.
- There is no absolute assurance from the EC that New Zealand will retain adequacy.
- The EC and the NZ OPC has informally agreed a process for ongoing monitoring by supplying update reports.

Law Reform NZ Privacy Act – what is happening?

Many of the New Zealanders in the room were reminded of the current uncertain political future with the recent General Election failing to deliver a Government and presently there is no clear “winner”. Hopefully by the time this article is published a new Government will be formed.

Despite this uncertainty, Ms Fordham confirmed the widely held view that updating the Privacy Act (nearly 25 years old) is overdue, particularly in light of the rapid changes in information technology and data science and the international developments, including the GDPR. The New Zealand privacy professionals in the room have been waiting for some time for traction on this reform and we learnt that:

- A new Bill is being drafted which the NZ OPC is involved in – particularly in working through the operational implications of some of the recommendations.
- There is no news to report on when the Bill will be introduced but it is still expected that there will be an exposure draft of the Bill circulated for wider consultation.
- The new legislation is likely to include more enforcement powers for the Privacy Commissioner: access determinations, enforcement notices and mandatory breach notification for material and serious data breaches.

New recommendations for Privacy Act reform

The Privacy Commissioner has proposed six further recommendations to the Minister of Justice for law reform:

- Data portability.
- Controls on re-identification.
- A new power to require agencies to demonstrate compliance with the Act.
- Civil penalties.
- Narrowing defences available for obstructing the Commissioner.
- Public register reform.

MSD – OPC Report on inquiry into proposal to collect client level data

Described by Annabel Fordham as “one of the most high-profile privacy debates we were engaged in during the year”, this is an example whereby the failure to “Walk the Line” at an early stage of a change in policy involving data resulted in significant public mistrust of a Government agency’s proposal.

This involved NGOs in the social sector, including those dealing with psychological counselling and family violence. As part of new funding contracts with NGOs, the Ministry of Social Development (MSD) proposed to require NGOs to provide to the MSD client level data (such as name, address, date of birth, ethnicity and dependents). The NGOs were very concerned about the impact this policy would have on their clients and ongoing service viability.

The Privacy Commissioner undertook an inquiry under the Privacy Act and the report prompted an urgent debate in Parliament. The Commissioner concluded that the policy,
as implemented, “is inconsistent with the principles of the Privacy Act and should therefore be amended”. ¹

The Commissioner found that MSD had not clearly explained its purpose for requiring individual client information from NGOs. While the objectives of the underlying policy were sound (being the Government’s social investment strategy), the Ministry had not given adequate consideration to whether it could meet those objectives without collecting such granular personal information. The Commissioner recommended the Ministry use less privacy invasive means of achieving the Government’s objectives of social investment.

Soon after the delivery of the Commissioner’s report, the MSD announced it would no longer be requiring NGOs to pass on client level data.

Making Privacy Easy

We were then provided with details of how the NZ OPC helps agencies to "Walk the Line" by making privacy easy:

- The Commissioner can issue an Advisory Opinion to give agencies greater certainty about the law and how the OPC would respond to an issue. One Advisory Opinion was issued during the year for the NZ Fire Service relating to whether the addresses of fire incidents were “personal information”.
- The Trusted Sharing Consultancy Service aims to help agencies use the Privacy Act to enable information sharing. This service has supported the Police, DIA NZTA and Immigration NZ.
- Free training modules on the OPC website.
- AskUs - the OPC interactive bank of online FAQs. We were told that the most asked questions are: “what is personal information?” and “can I record someone without telling them?”

So what is ahead for 2018

After such a busy 2017, we were treated to what was on the horizon for the OPC in 2018:

- Law Reform – “We hope” said Ms Fordham, and I think that sentiment was echoed by many (if not all) the New Zealanders in the room.
- LIVE CHAT function to come on the OPC website.
- 25th anniversary of the Privacy Act.
- Hosting APPA in late 2018 – and the IWGDPT (Berlin Group) in late 2018

Privacy Trust Mark

Finally, we heard about a new development at the OPC, a Privacy Trust Mark. This will be an endorsement from the OPC for 2 years. It is intended that this will create a way for consumers to know if they are using a product or service that has been designed with privacy in mind. This initiative is still at an early stage, but we were told that early responses have been positive.

¹ Privacy Commissioner Inquiry into the Ministry of Social Development’s Collection of Client-Level Data from NGOs 4 April 2017.
SESSION 5: Maintaining the line – Facilitating Safe Data Use Through Safe Settings and Ethical Decisions

Panellists:
Anna Johnston – Director, Salinger Privacy
Dame Diane Robertson – Chair, The Data Futures Partnership
Stephen Hardy – Leader Confidential Computing and N1 Analytics, CSIRO’s Data61
Geof Heydon – Principal, Heydon Consulting

Report author: Jacqueline Peace, iappANZ Secretary and Senior Manager Data Protection & Chief Privacy Officer
Air New Zealand

My remit, write an article summarising the panel on ‘Safe data, trusted data use: what it means and how to get there’. Sure, I can do that. After all, isn’t ‘safe data, trusted use…’ what we are all about and what we are all striving for? So, all I need to do is identify the three easy actions the well-informed panellists agree need to be taken to support the ‘… how to get there?’ part of this statement. Actually, all I really needed to do was record Anna Johnston’s well-articulated summary at the end of the panel, however, I was engrossed in the panel and forgot to write this summary down. So, from memory and with a little bit of help when my memory failed me from Dr Google, here we go:

1. Dame Diane Robertson, Chair of The Data Futures Partnership in New Zealand, noted we needed to obtain “social licence and that de-identification isn’t always the answer”. Let’s not underestimate these wise words. It’s complex. Instead of, “what can we do with data?” as guided by the privacy principles, we should be thinking about “what should we do?” Whose data is it and how should we use it? That’s really what we are talking about with ‘Social Licence’. The aim of Social Licence is to obtain community acceptance by getting people to come along with us on the data journey. Do communities think what we want to do with their personal data is ok? If we are de-identifying data are we truly anonymising it and getting the best out of the data for the community?

Dame Diane talked about the ‘data dial’ which enables conversation and transparency about data and data sharing, with the aim being to let individuals have their say about whether they are prepared to share their data and in what form. The topics that were explored using the data dial included sharing of health data (even if it has been anonymised), the internet of things (smart cities, driverless cars) and social investment (sharing data across agencies about identifiable individuals to better target the help they need).

The ‘data dial’ is a set of eight questions that communities wanted organisations to answer transparently to explain what the organisation intends to do with the data they collect and why. Here’s a snapshot of the questions that can help you articulate a transparent summary of intended data use with the aim of achieving social licence. If you want more information you can refer to http://datafutures.co.nz/our-work-2/talking-to-new-zealanders/

Value questions:
What will my data be used for?
Who will be using my data?
What are the benefits and who will benefit?

Choice questions:
Will I be asked for consent?
Could my data be sold?

Protection questions:
Is my data secure?
Will my data be anonymous?
Can I see and correct my data?

The communities Dame Diane talked to in New Zealand, ultimately all agreed that they wanted every organisation to answer these questions before seeking their trust. If you are planning on doing something new or novel with personal data and if it affects marginalised groups and you don’t have their trust, (some Government agencies have fallen foul of being trusted by their communities) then you need Social Licence. The ‘data dial’ can help you gain that trust and ultimately the community approval to proceed.

2. Dr Stephen Hardy, Leader confidential Computing and N1 Analytics at CSIRO’s Data61, talked about a continuum of highly identified personal data through to highly de-identified. He mentioned the need to look for the associated risk, work out what we want to do with the data (purpose) and who is best placed to do it (access and trust). Considering these factors will help us to balance how much data
we share and what level of protection (de-identification) does it need. How then do we know what sort of project involving personal data should sit where on this ‘identification continuum’?.

Stephen wisely advised us to consider placing projects that involve de-identified and sensitive personal data in the hands of internal, trusted staff and not to share it by default. Technology is there to support the different levels of data sensitivity and comfort. Technology advancements have resulted in the cost of electronics going down and the ability to put sensors on more and more items (even the common electric toaster), therefore increasing our ability to collect data sensing the things we are doing (is data about my propensity to burn the toast really worth collecting?). Every one of these sensing devices is connected to some default password by the organisations manufacturing them, which isn’t easily changed.

Rather than allowing the collection of sensitive personal data by default (could my household insurance premiums go up because of my ability to regularly burn the toast and set off the fire alarm?), Stephen suggests that the organisations selling the sensor driven devices, should be encouraging individuals to set the password before starting the device. This would then enable individuals to determine their own comfort levels about what data is or isn’t shared. Does this mean potentially another password to remember should I inadvertently “lock” the toaster?

De-identification is seen as the new panacea ... first we labelled personal data as confidential, then we upped it a notch to encrypt it, now we are talking about de-identifying it so that it can be used “anonymously”. At this point of the panel, as all good techies do, Stephen “wandered off” and talked keenly about k-anonymisation and differential privacy. Clearly he knows his stuff, and I’m not capable of remembering his well-made points, let alone capable of trying to explain what they meant. I suggest you refer to the session later in this journal that Anna Johnston led at the Summit, she explains it beautifully and she had us practising these techniques with enthusiasm! What I did surmise from Stephen was that relying on your personal data to be safely de-identified isn’t failsafe.

Stephen referred to the 5 Safes Framework from the UK which he thinks can offer a safe model for privacy and security teams to weigh up the balance of: benefits, value and community derived benefits. This echoed the data dial questions Dame Diane had referred to also. Wikipedia (not my memory) advised me that the 5 Safes for projects are: Is this use of the data appropriate?; Can the researchers be trusted to use it in an appropriate manner?; does the access facility limit unauthorised use?; Is there a disclosure risk in the data itself?; and are the statistical results non-disclosive?

3. Geoff Heydon, Principal at Heydon Consulting, further supported the concepts of social licence and identifying community derived benefits throughout his input to the panel. He explained that he’s seen many councils gathering personal data in silos within their own departments and that “the most value for communities would only be obtained when this data is shared appropriately”. Geoff was wholeheartedly supportive of organisations taking a data journey that involved drafting data policy and providing a data sharing ‘playbook’ that outlines risk assessment profiles combined with analytics. Such an approach in a council environment for example, would enable departments to test what personal data can be shared and to identify when it’s appropriate to do so. To reach a playbook scenario would require councils to engage with their population or as Dame Diane puts it, engage with our communities to obtain Social Licence to the transparent use of their data.

In summary, the panellists all appeared to be in agreement (data dial = 5 safes = data sharing playbook). They provided their well-considered interpretations of the importance of taking individuals (whose personal data is being used) on a data journey in order to get the best out of the data in an appropriate way for the individuals concerned. Furthermore, a common theme across the panellists was that if we over protect and de-identify everything, then we run the risk of stifling and preventing innovation, value and growth. We should be looking for ways to appropriately and transparently drive the value of data and use it to develop better services and products for individuals at the heart of the community.

Privacy Impact Assessments might tick all the right boxes against the privacy principles we adhere to, however, the real impact on privacy is whether or not the initiative in question is “the right thing to do”. If we can’t explain what we want to do in a simple conversation with the communities it impacts and with their support, then we shouldn’t be doing it. My takeaway? Just because we can, doesn’t mean we should.
SESSION 6: Why I hijacked Privacy Awareness Week to win hearts, not minds

Speaker: Craig Templeton - Chief Information Security Officer, REA Group

Report author: Melanie Marks, iappANZ President and Principal, Eleven M

When Craig Templeton says he “hijacked” Privacy Awareness Week (PAW) at REA (aka www.realestate.com.au) he means it. Usually the domain of lawyers, risk and compliance people and maybe a rare Chief Privacy Officer, it’s rare for a CISO to take the reins (and dedicate budget) to win hearts and minds on privacy - yet that is exactly what he did with a campaign about digital tattoos.

Craig’s presentation had us all paying attention not only for the sense it projected but because Craig on stage is like combining Danny Bhoy with your favourite TedTalk presenter. Danny had the crowd taking pictures of his slides for their loved ones at home.

Craig’s thesis
- Evidence suggests that attitude beats compliance, as a lead indicator of cyber resilience.
- All personnel, our peers and colleagues in the businesses within which we work have been subjected to fear mongering about privacy consequence rather than empowerment.
- If we want to maximise the capability of our people and peers to be an effective first line of defence for privacy risks and cyber threats, we must empower them.

Focussing on the importance of using a positive ‘nudge’ rather than cyber fear to get results, Craig’s Digital Ink program for staff at REA included inviting staff to visit the security team to review their social media privacy settings.

Whilst there they were given digital tattoos and donuts, creating a lure for other staff to come down and a lot of buzz on REA’s internal social media platforms.

The digital tattoo campaign used the concept of a tattoo as an analogy for a digital footprint – that is, hard to remove, and essentially forever.

Success
- Staff were given materials to take away, driving home the message about maintaining personal privacy online.
- Success came in the form of an exceptional “sentiment” rating on internal platforms, with people sharing content and wanting to know more about security topics and increased requests for engagement.

One of the last questions Craig was asked during his presentation was what is in store for REA’s PAW in 2018. No doubt Digital Ink will be a tough act to follow within REA just as Craig was a tough act to follow at the Summit.

Craig’s presentation will be available in the ‘members only’ area of the iappANZ website along with other presentations from the Summit.
SESSION 7: De-identification practical: what the privacy professional needs to know

Speaker: Anna Johnston - Director, Salinger Privacy

Report author: Olga Ganopolsky, General Counsel - Privacy and Data at Macquarie Group

If you thought that identifying what is personal information and what is not was an easy task, think again!

Anna Johnston’s presentation reminded us that information when managed can go through various stages and processes, some highly mathematical and statistical in nature.

Anna focused on the five de-identification techniques and the maths behind them. These techniques are: aggregation, suppression, generalisation, pseudonymisation and perturbation.

1. Aggregation refers to a process in which information is gathered and expressed in summary form. It is commonly used to derive more information about specific variables such as, age, profession or income.

2. Suppression refers to a process of withholding or removing selected information.

3. Generalisation is a bottom-up approach in which two lower level entities combine to form the higher entity. The process involves extracting a shared characteristic. These can be different attributes.

4. Pseudonymisation is the separation of data from direct identifiers so that linkage is not possible without additional information that is held separately. Typically, actual information is replaced with artificial identifiers or pseudonyms and the information is not anonymous.

5. Perturbation involves the 'disturbing' or perturbing the data by adding or multiplying a factor. This can be structured or unstructured. The technique is commonly used in electronic health records and can be reversed provided the method used is known or can be ascertained.

The presentation reminded us why de-identification matters and how we as privacy practitioners can navigate through the maths driving the data science of turning personal information into de-personalised or de-identified data and, in some cases, back again.

The key to selecting the right technique is the need to know the data and the risks one is trying to avoid. The ability to properly de-identify data that was previously personal data is a key mitigation for most privacy related risks. This is because, when the techniques are properly applied, the data ceases to relate to an individual or to identify the individual, thereby:

- removing the key risk for the individual of any misuse of information about him or her; and
- no longer attracting compliance obligations imposed on the organisation holding the data.

Also, considering that the activity of unlawfully re-identifying data is fast emerging as a new crime or offence under a number of privacy related statutes, the ability to draw a clear line in the sand and be clear and precise about the process and its outcomes is now critical in so many instances.

Anna stressed that the risk being managed are various and not always binary. For example, with the risk of identification, one is trying to avoid the disclosure of identity. This risk is ever present in structured data sets containing identifiers and is common in industries such as health and financial services where the actual identity of the individual is typically intertwined with the very service being received. Another risk is the risk of attribute disclosure. This risk is that the identity of the person is known but not the key confidential attribute such as their tertiary entry score, salary level or medical test results. Individuation is the risk of disclosure of a set of characteristics about a person but not their identity per se. Individuation can enable targeting for marketing or other purposes, for example a particular age group such as retirees, or individuals in higher income brackets.

In addition to participating in a lively maths lesson, the session helped demonstrate that whether one can identify or ‘individuate’ a person from once identified information is both an art and a science. The demonstration was timely, given that many of us are grappling with these very issues daily, either in various security programs (APP 11 under the Privacy Act 1988 (Cth)), data analytics led projects designed to improve the efficacy of regulatory reporting or law reform programs such as the EU General Data Protection Regulation where the ability to minimise data and do so on a systematic basis will soon be an express legal requirement (Article 5 (1)(c)).
SESSION 8: Ethics of Spyware – What happens when you spy on a thief?

Speaker: Anthony van der Meer - Director, Researcher, Concept Developer & Filmmaker

Report author: Marta Ganko, National Privacy Lead, Risk Advisory, Deloitte and Veronica Scott, Special Counsel, MinterEllison

Marta: We often hear that data can be used for good and evil. The same notion can be applied to spyware. Spyware is software that collects data from devices without the knowledge and or consent of a user. Data can include taking a photo, text messages and files. On the surface, it may appear this is completely wrong, but, what if spyware is being used to track down a thief - of your mobile phone? Does this make it ok?

Anthony van der Meer, a filmmaker from the Netherlands has created a film that explores exactly this. Find my phone, a movie created by van der Meer, sets out on a mission to determine what kind of individuals would steal a phone and learn what is done with one when stolen. He configured a phone with spyware, and after some trouble in encouraging getting his phone stolen – it finally does. Anthony sets out on a journey to learn about the thief, his life, and by the end, he even questioned whether he felt sorry for the thief.

van der Meer quickly learns that not all phones are pulled apart to resell parts. Phones can be stolen and then reused for other purposes. Data including texts, photos and contact lists are not wiped and can be accessed by the thief or person to whom phone is sold. More concerning is that the activities performed by the thief, could lead the original owner of the phone to be associated with illegal activity. The data on the phone is not removed and treated like junk mail and offered no respect or protection.

While there may be a right to privacy, Anthony spoke about how the question of whether spyware is legal or not is a question for each jurisdiction to answer. Due diligence needs to be performed on spyware users to ensure activities are not overstepping the mark – and he did exactly this.

It is worth noting that there are applications of spyware in the modern world – organisations may receive information about individuals without their knowledge, customer behaviour may be tracked and assertions made, and parents may track their kids for safety reasons.

So where is the line drawn?

In some countries it may be illegal to buy and/or use such software. Use of such software can put you on the wrong side of the law. In the movie, van der Meer has his own phone stolen, but when it falls into another’s hands, should one be allowed to look at another’s activities on their own device? Even if they are doing the wrong thing? Is this taking the law into your own hands. How would the perpetrator feel? It is also tempting to use this evidence as a result of using spyware to monitor devices other than your own – in some jurisdictions, evidence needs to be provided as to how information was obtained.

It is evident that the question of whether the use of spyware is lawful is not always clear. The context could mean there are varying perspectives on the same scenario as is demonstrated in the ending of Find My Phone. What is being seen is that spyware is becoming unlawful in more countries.

Do you think you should be able to track your own phone’s activities once stolen?

Veronica: In Australia, there are a range of laws that would apply to the installation on computers or devices and use of apps with these software features at a State and Commonwealth level. These include surveillance devices legislation, the Telecommunications (Interception and Access) Act 1979, privacy and consumer laws and computer offences. Some of these were discussed during the Q&A with Anthony and are outlined below to place Anthony’s interesting presentation in an Australian context.

In Australia anti theft and find my phone or devices manager apps are increasingly popular. They are available to be downloaded depending on the operating systems. These apps are not necessarily illegal and may have some legitimate personal uses when an individual downloads and uses it on their own device, for some limited purposes. They are intended for personal use on authorised devices only where the user knows and consents to their installation and the collection of their information. The app’s service provider will require users to agree that they will not use the services for any unlawful purposes and that they will only install the app for personal use on their own devices.

Privacy laws in Australia generally apply to businesses and government agencies, not to individuals collecting and handling the personal information of others in their individual capacity. However individuals will be subject to State and Territory surveillance devices laws which generally prevents the recording of private conversations and activities or tracking without consent, and the publishing of information collected through this kind of surveillance, subject to some limited exceptions (which differ from State to State, for example, depending on where you are, if is in the public interest or is for the protection of the lawful interest of the person).

An individual could argue that a thief who steals and uses their smart phone should expect the phone may have
location services turned on and the use of the app they have installed is for the protection of their lawful interests as an owner. But don’t be a test case. The best and safest option is first keeping the phone and data on it secure and in a worst case scenario when stolen, reporting it to the police and letting them investigate the crime.

Users also need to be aware not only of who they might be collecting data about through the apps, but what the app provider can collect about them. These apps are usually free and therefore their data will be the price for the service. The app service provider may be overseas and not subject to local privacy laws. If users want to install and use an app of this kind themselves, they should ensure their purpose is legitimate and read the terms and conditions and privacy notices to ensure they understand what the app can access, how and when their information, and what information will be collected, who it will be disclosed to and where it is stored.

If these apps are installed on someone’s device without their knowledge and/or are used to record and collect information about the user and pass on their information, without the user’s consent, these activities would be unlawful. Also anyone who uses them to stalk or to harass a person, for fraud or blackmail or to commit computer-related crimes which are prescribed under the various Criminal Codes, could be prosecuted. There are a number of steps that device owners can take to ensure these spyware apps cannot be surreptitiously installed, including ensuring the device has up to date and strong privacy and security settings and following the advice of the operating system they are using.

Of course spyware apps are not to be confused with the many common types of mainstream legitimate spyware which people will be familiar with, such as adware and tracking cookies (which is becoming almost the default for many apps). They can be used for location based tracking, storing our movements as we browse the internet and access websites and serving up pop-up ads or push notices. Users should still be informed of these features and their agreement obtained to allow these activities and the collection of their data.
SESSION 9: Cool or Creepy?: Navigating a safe path to unlock the power of big data, AI and analytics

Panellists:
Laura Bell – Chief Executive Officer and Security Cat Herder, Safe Stack,
Linden Dawson – Digital Transformation and Business Strategist,
Jodie Sangster – Chief Executive Officer, Association for Data Driven Marketing and Advertising (ADMA),
Anne-Marie Allgrove – Partner, Baker & McKenzie

Report author: Daimhin Warner, iappANZ board director and Director, Simply Privacy

The 2017 Summit was concluded with a thought-provoking panel discussion on navigating a safe path to unlocking the power of data, and particularly Big Data, AI and analytics.

The panel was part of the final session of the day, where panel members were invited to reflect on the many excellent presentations and provide insights on questioning the line our speakers had grappled with during the Summit. This was about taking a practical and ethical approach to data use and the perspectives of our panel members - from a data governance rather than legal or compliance approach - were refreshing.

The panel members were ably herded by Laura Bell, CEO of security consultancy Safe Stack. Joining her on the panel were Linden Dawson (Digital transformation and business strategist who led stakeholder engagement for the Digital ID platform at Australia Post), Anne-Marie Allgrove (partner at Baker & McKenzie focusing on technology, media and healthcare), and Jodie Sangster (CEO of the Association for Data Driven Marketing & Advertising). As such, the viewpoints expressed were diverse and fascinating.

A few high-level observations:

- The panelists were excited about the technological evolution we are witnessing, including self-driving cars and artificial intelligence, and there was a sense that privacy should not stifle this innovation. However, there was an equal sense that such innovation needed to be managed with care and respect, and with public buy-in.

- Data Governance Australia has developed a code of practice designed to promote the responsible and ethical use of data through nine core principles: No harm; honesty and transparency; fairness; choice; accuracy and access; accountability; stewardship; security; and enforcement.

- No-one on the panel felt that they had ever been required to accept a project that had crossed the line, or to set aside their ethics for some greater business goal. Most were of the view that they had been consulted early enough to influence change and swing the project back into cool territory.

- The term “creepy” was challenged as downplaying the real harm that could be done where an agency crossed the line. While no alternative was decided upon by the panel, it was agreed that where data use was exploitative or harmful the term creepy might not accurately reflect the risk.

- Agencies need to do better at being open and transparent with their customers, to ensure that customers understand the value their data can deliver and feel that they can engage with the ways their data is used.

Overall, the panel concluded that there is no hard and fast line where cool becomes creepy. Rather, it is the context that matters. In advising our clients or employers on projects or innovations that might come close to this line, we as privacy professionals must be pragmatic - remembering that agencies must be able to do business - and must encourage openness and transparency to build trust.
Dataveillance and the power of the ABS: Government overreach highlighted by the marriage equality survey
By Anna Johnston

I have written elsewhere about why marriage equality is a privacy and freedom of speech issue, but in this article I want to highlight the significant implications of the postal survey for government power.

The privacy issue that has me concerned is the potential power of the Government to use the ABS as a population-wide data-collection tool, for political purposes. The High Court case of Wilkie v The Commonwealth; Australian Marriage Equality Ltd v Cormann [2017] HCA 40, which attempted but failed to stop the same-sex marriage survey, did nothing to assuage my concerns. Here’s why.

The ABS is operating under a Ministerial Direction “to request statistical information” from all Australians on the Commonwealth Electoral Roll, as to their views on whether or not the law should be changed to allow same sex couples to marry.

This phrase ‘statistical information’ is critical, because the ability of the Australian Bureau of Statistics (ABS) to be directed by the Government, and its power to collect data, is limited under the Census & Statistics Act to ‘statistical information’. The meaning of that phrase is not defined, but for surveys other than the Census, the ABS can only collect statistical information on a list of topics prescribed in the regulations, which include “births, deaths, marriages and divorces”.

Prior to the High Court case, some legal experts questioned whether opinions could be ‘statistical information’, in the way that facts are. Constitutional lawyer Anne Twomey for example described ‘statistical information’ as “numerical data concerning facts”. So it would be one thing for the ABS to collect data about the numbers of people who are in same-sex relationships, or the number of married versus unmarried couples – but another thing entirely to ask about people’s opinions about marriage.

Therefore the issue that was tested in the High Court was whether or not asking for people’s opinions on marriage equality is ‘statistical information’ about marriage. The High Court found that “information about personal opinion or belief, including information as to the proportion of persons holding a particular opinion or belief, is and always has been ‘statistical information’” (at [146]).

The High Court also rejected an argument that some direct connection was required between the data to be collected, and the list of topics prescribed in the regulations. The Court stated that the Act does not require “anything more than the existence of a relationship, whether direct or indirect, between the information to be collected and the subject-matter prescribed” (at [147]).

The result of the High Court decision was to increase my fear that the Government could use the ABS as a tool of surveillance.

That might sound ridiculous, but consider this: last year the ABS decided that it had the power to use our names and addresses to generate statistical linkage keys (a type of pseudonym), to enable it to link our Census answers with other data about each of us, from datasets given to it by other arms of government.

So if the ABS can link our Census answers, at an individual level, to our educational records, criminal records, tax records and whatever else it is hoovering up, why not also survey data it collects about our opinions? The ABS has released a statement saying that it won’t do that with our marriage equality survey answers, but I see nothing in the High Court’s judgment that would have stopped the ABS doing so if it so wished.

So here’s where we are at. The Government has the power to direct the ABS to collect ‘statistical information’ about any or all of us. ‘Statistical information’ can mean anything with only the most tenuous link to one of a long range of topics, the list of which can be added to by the Government by way of a new regulation at any time. The ABS has the power to make its surveys compulsory. Individuals face daily criminal penalties if they refuse to answer a compulsory survey. The ABS also claims it has the power to link data about us at an individual level for its own purposes, so long as they don’t disclose our data in identifiable form. The ABS claims this includes data collected from us via the Census, from us via other surveys, and indirectly from other government administrative datasets (like Medicare, Centrelink and income tax records).

By now hopefully you are starting to see the scope of the ultimate privacy issue at stake here. There is nothing to stop the ABS compiling dossiers on every single one of us – and using their compulsion powers and threat of daily criminal penalties to do so. They could do so off their own bat, or they could be directed to do so by the Government of the day.

Why stop with our views on same-sex marriage? Why not also ask where everyone stands on other topics conceivable within scope of the prescribed list of topics on which the ABS can conduct surveys, like how we feel about abortion (‘births’ is one of the prescribed topics), euthanasia (deaths), or who should win The Bachelor (marriage)?
The ABS could just as easily ask how we feel about whether Barnaby Joyce should be sent home to New Zealand (migration), gun control (fishing, hunting and trapping), climate change (conservation and the environment), wind farms (energy), or whether peanut butter should be crunchy or smooth (food preparation and food consumption).

And the ABS could, if it so wished, link our answers to those questions to any other data it holds about us.

As long-time privacy advocate Graham Greenleaf has said, “If ABS can now collect opinions on anything, what limits its collection methods? One more step toward the Australian Bureau of Surveillance”.

I am one of the many who never wanted this wasteful, hurtful, unnecessary survey in the first place, because affording equal legal rights and protections to a minority should not be subject to the opinions of the majority.

But regardless of where you sit on the marriage equality question, as citizens we should all be alarmed that the High Court decision has paved the way for the ABS to become the tool, whether willing or not, of future governments intent on population-wide dataveillance.

Anna Johnston is Director, Salinger Privacy

Salinger Privacy provides specialist privacy consulting services, Learning modules and eBooks on privacy law. Find us, read our blog or sign up for our newsletter at www.salingerprivacy.com.au
EVENT INVITATION

Artificial intelligence in Health: Balancing the use of data with privacy

Healthcare has become a key focus for the application of new artificial intelligence (AI) technologies. Certainly there are many opportunities and also challenges surrounding the use of AI in health.

Join us for this breakfast workshop where we will explore how AI can be used with health data to empower health clinicians and improve health outcomes while still responsibly protecting patient privacy.

Date: Friday 17 November 2017
Time: 7:30am - 9:30am
Venue: The Maritime Room - Princes Wharf, Corner Quay and Hobson Street, Auckland
Cost: Free to attend

PANELISTS INCLUDE:

Dave Heiner
Vice President, Microsoft Corporation, Corporate, External and Legal Affairs

Kevin Ross
Director of Research at Orion Health / Precision Driven Health Partnership

Dylan Mordaunt
Physician, Waitemata District Health Board

TOPICS INCLUDE:

- Ethical and legal considerations around the use of AI
- Health information, AI and privacy - the challenges and opportunities therein
- What is the right balance between ensuring personal privacy and enabling the benefits of AI in health?
- Should health information be treated differently than other types of data? How can we cure disease and save lives if we do not enable access to the data?
- What are the benefits and limitations of District Health Board privacy policies regarding use of data from an artificial intelligence perspective?
- When AI is used to make a consequential decision about people, what types of information should the AI system owner make available to help people understand how the system makes decisions?

REGISTER HERE

REGISTER HERE FOR 2018!