Privacy Unbound is the journal of the International Association of Privacy Professionals, Australia-New Zealand (iappANZ),

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

Veronica Scott
veronica.scott@minterellison.com

Carolyn Lidgerwood
carolyn.lidgerwood@riotinto.com

David Templeton
David.Templeton@anz.com

Please note that none of the content published in the Journal should be taken as legal or any other professional advice.
Hi and welcome to the ‘new look’ iappANZ Privacy Unbound. Thanks to our wonderful editors Carolyn, David and Veronica and our new Operations Manager, Jess for their hard work in putting it together. As always, if you have any feedback on the new format or any other element of your membership of iappANZ, we would love to hear it.

Registration for this year’s ‘Trust in Privacy’ themed iappANZ summit, being held in Sydney on November 14th, will be open very soon and we will be offering early bird rates until the end of September so make sure you get in quickly. The full program will be announced very shortly, including details of a half day practical workshop the day after the Summit. On November 14th, after the Summit we will also be holding our AGM, which is when we elect the new Board and executive. This year we have a number of the existing team stepping down after many years of service and we are very excited at the prospect of bring new people onto the Board. We’ll be sending more information out about what it means to be on the Board over the coming weeks but in the meantime, I would be very happy to talk to anyone who is interested in getting to know more, just drop me a line.

Happy reading!

Kate
Our July/August edition of Privacy Unbound is filled with informative and thought-provoking contributions on current privacy related sightings in Australia and New Zealand. While each contribution offers distinct privacy perspectives on recent initiatives and debates, the theme that overlays each of them is Trust in Privacy. Whether we are dealing with a national mandated collection of citizen data or storage of health records or the use of modern apps, integrity and transparency when collecting personal data, using it and protecting it are paramount.

Board Director, Tom Bowden has an insightful editorial on what can only be seen as the great Census debacle of 2016 with useful observations on the UK experience and Kyle Lees examines the political and public furore which unfolded with the mandated collection of personal data and the fruits of the ABS’ labour ... surprisingly richer than one would have expected. The OAIC provides a succinct update on the Ashley Madison report and a case for more robust consumer awareness when disclosing their personal information. Kerry Bakkerus writes on the New Zealand Health Strategy and the challenges for managing and delivering on expectations. The concluding line ‘Trust is everything’ cannot be over-stated. iappANZ members, John Fairbairn, Helen Lauder and Martina Pasqualino provide a great summary of recent determinations involving NRMA on managing disclosures of personal information to a customer. The determinations highlight that where a practice involves the disclosure of a customer’s personal information, even to their family or associates, the privacy impacts need to be thoroughly considered before it is implemented.

Happy reading!
iappANZ is the pre-eminent forum for privacy professionals in Australia and New Zealand. We are affiliated with the International Association of Privacy Professionals (IAPP), the largest and most comprehensive global information privacy community and resource with more than 23,000 members. We work with public and private entities across all industry sectors in Australia and New Zealand as well as the Privacy Commissioners in both countries.

iappANZ offers our members a wealth of opportunities to expand their privacy knowledge, compliance, interests and networks. Our members in Australia and New Zealand represent some of the best minds in the privacy field, from large public companies and the government sector to not for profit, SMEs and individuals.
The hotel clerk fixed me with his beady eye.
A grim expression instantly told me that something was amiss. “You’re going to have to fill in one of these”, he said, pushing a large envelope toward me, “its census night.” “Not I won’t, I am an alien”, I said smugly, having just jumped off a three hour flight from New Zealand. “Doesn’t matter” he responded, “everyone has to do it, resident or visitor”. It was only a matter of minutes before I realized that I had descended into a war zone. On my in-room television I could see that an angry debate was unfolding.

Australia’s national census, which provides a snapshot every five years of the country’s people, from religion to income, had created a headline grabbing furore. Australians (and visitors) were being asked to fill in a host of details about themselves online, for the first time in the 105-year history of the census. The only other change was the fact that names and addresses were being collected and retained for the next four years, instead of 18 months. In protest, some politicians and privacy advocates decided to partially boycott the survey, because of worries over data security. Minor party leader Senator Nick Xenophon and three senate colleagues refused to enter their names and addresses “Rather than being a snapshot of the nation, this census will now morph into a mobile CCTV that follows every Australian,” Senator Xenophon said in a statement. “The Australian Bureau of Statistics (ABS) has failed to make a compelling case why names must be provided, and stored for four years.” He claimed support from across the left, centrist and right-wing minor parties elected to parliament in the recent general election. Xenophon and his three fellow senators have said they will not write their names on the census forms, even on pain of a A$180-per-day fine.

Bill McClennan, Australia’s chief statistician from 1995 to 2000, said the retention of names was “the most significant invasion of privacy ever perpetrated on Australians by the ABS”. Former NSW Deputy Privacy Commissioner Anna Johnston added her voice to the calls of alarm, saying she would be boycotting the Census herself, due to “moral” privacy-oriented reasons. “The short version is this: Yes to a national snapshot. No to detailed data-linking on individuals. That’s not what a Census is for,” Johnston said, outlining the risks as she sees them, “Although there are certainly heightened privacy and security risks of accidental loss or malicious misuse with storing names and addresses, the deliberate privacy invasion starts with the use of that data to create a Statistical Linkage Key (SLK) for each individual, to use in linking data from other sources. Please don’t believe that SLKs offer anonymity. SLKs are easy to generate, with the same standard used across multiple datasets.”

Later in the evening, the system was hacked. Amidst much discussion about cyber security and privacy risks and a number of official statements about how robust and secure the system is, it received a series of sustained attacks. Finally, late in the evening, the ABS took down the online survey “after a series of distributed denial-of-service events.”

So what was all the fuss really about?
Names and addresses have always been collected and presumably for a number of years, the information has been manually entered into a computer somewhere? To some extent the issues politicians and other detractors
have raised are questionable and potentially groundless, 
because the same information has been gathered on 
paper records for many years. Holding the data on a 
computer system hardly seems like a major change to a 
long-established process. Extending the duration that 
records are kept from 18 months to four years does not 
seem to be something earth shattering either. It seems 
as though the Australian public has reached a point at 
which it wishes Government to understand and 
acknowledge that it will not accept ongoing incursions 
into its privacy without proper discussion and debate. 
This opinion might well be labelled as presumptuous, 
however I firmly believe that the minor changes to the 
2016 Australian Census may well have been the straws 
that broke the camel’s back.

If this is so, how then can government recover the 
situation and get back into a position from which it can 
continue to use information technology to reduce the 
costs of governing and to improve the lives of its 
citizens?

**Compare the UK Care.Data experience**

A good example of a government doing just that is the 
United Kingdom’s recent withdrawal of the highly 
controversial ‘Care.Data’ service which had been 
tended to gather patient data and use it for multiple 
purposes. What is interesting is that on the same day 
Care.Data was cancelled, the UK’s healthcare data 
guardian Dame Fiona Caldicott tabled her third report - A 
*Review of Data-Security, Consents and Opt-Outs – June* 
2016. In presenting the report Dame Fiona commented 
that she had been prompted to write it because the UK 
National Health Service (NHS) had made insufficient 
progress in automating the NHS’ IT systems, a lack of 
progress that in her view had been caused by a lack of 
clarity surrounding patient privacy issues. The essence of 
Dame Fiona’s report was a call for greater openness and 
clarity and more explicit dialogue with individual patients 
over their rights and wishes.

Dame Fiona’s overall conclusion was:

> “That information is essential to support excellent care, for 
> running the health and social care system, to improve the 
> safety and quality of care, including through research, to 
> protect public health, and to support innovation. But for 
> the majority of purposes personal confidential data is not 
> required. High quality, linked data that is anonymised will 
> often be sufficient”

Clearly the Australian Government could consider taking 
a similar, much more open approach and being 
completely ‘up-front’ about what data it is collecting and 
why? While this might be viewed by some in government 
as ‘taking the long way round’ it is becoming clearer and 
clearer that citizens want their governments to be open 

and transparent about why they are seeking information 
and what they intend to do with it.

In the meantime, I have made a diary entry for early 
August 2021 “Check privacy situation in Australia before 
making plans to visit”.

Tom Bowden is co-founder and CEO of HealthLink and a 
Board Director of iappANZ
August was another busy month for the OAIC with the release of the high-profile report into the 2015 Ashley Madison website data breach which affected approximately 36 million people.

The investigation provided a leading example of how privacy issues can be resolved on an international level, and the report provides valuable lessons for individuals and businesses.

Privacy and data have become global challenges, with personal information crossing international borders as people sign-up to use websites hosted overseas. While Ashley Madison is the first “joint jurisdiction” OAIC has engaged with, we expect to collaborate increasingly with other offices to find solutions to privacy breaches affecting Australians – as was the case with the Ashley Madison investigation. The Ashley Madison website, operated by Avid Life Media (ALM, recently rebranded as Ruby Corp) and based in Toronto, Canada, offered users a space to organise a discreet extramarital affair at the time it was breached. Millions of users across Australia and Canada had their personal information published online, including their account information, email addresses, security questions and, in some cases, billing and geolocation information. The OAIC worked with the Office of the Privacy Commissioner of Canada (OPC) on the investigation that followed.

The final report on the breach is highly critical of the privacy and personal data security frameworks ALM had in place. It was found that ALM’s privacy and security practices were inadequate; encryption keys were stored as plain, clearly identifiable text on ALM systems, key and password management practices were poor and ALM failed to adequately ensure the accuracy of user email addresses – which potentially meant people who never signed up to the website were included in the database.

In a positive step forward, ALM has committed to large-scale changes outlined in an enforceable undertaking in the report, to be completed by mid-March next year. The public interest in the report meant that OAIC was present in numerous publications from the ABC to the New York Times, and to promote what business leaders and individuals can learn from Ashley Madison. For businesses, ALM’s story provides a case-study in how not to approach privacy. Best privacy practices can be built into businesses from the beginning and developed as a business grows to better ensure data security. The report also serves as a reminder that privacy is not simply about ‘IT issues’, but relies on the proper training of staff, policies, oversight and clear lines of authority for decision making.

For individuals, the Ashley Madison report was a reminder to take privacy into their own hands by making informed choices on where they share their personal information online. While the possibility for a privacy breach may appear evident as outlined in the report, it was perhaps not evident to, or carefully considered by, the millions of users that signed up. When providing personal information online, people should be clear on what information they are providing and keep in mind that no organisation is ‘breach-proof’ regardless of how discreet the website promises to be.

For more information contact Richard O’Neill – Director Stakeholder Relations and Communications richard.oneill@oaic.gov.au
SAVE THE DATE!

iappANZ PRIVACY SUMMIT
TRUST IN PRIVACY

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

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

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

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

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

+ Half-day workshop
Designing Privacy Controls into Projects
Featuring Salinger Privacy’s Anna Johnson
Tuesday, 15 November 2016, 9.00am - 1.00pm
Limited spaces available

iapp ANZ
international association of privacy professionals
CONNECTING PRIVACY PEOPLE, ENHANCING PRIVACY PRACTICE

Platinum Sponsors ___________________________ Gold Sponsors ___________________________

Commonwealth Bank Microsoft NAID ANZ

Silver Sponsors ___________________________

BINDER GILBERT + TAMBIN HL Health Law

www.iappanz.org
The Office of the Privacy Commissioner (OPC) has launched a new interactive online resource. Its an FAQ called 'AskUs' at privacy.org.nz/ask that provides answers to more than 300 high-level privacy questions such as ‘can I get my information from my employer’ and ‘can I record a conversation’.

The resource has been launched in response to the thousands of enquiries that the OPC receives each year on a broad range of privacy related topics. It is aimed at both public and private sector entities as well as the general public and covers a broad range of topics such as data breaches, surveillance, credit reporting, children's privacy, complaints ... The answers are practical, in plain English and connect you to answers to other related questions. The search function offers you a range of suggested questions much the same way Google does.

This will be a developing resource which the OPC will continue to update and refine according to feedback and the frequency of new questions it receives. It is therefore interested to have any feedback from our members via the comment box at the bottom of each answer. So if you can't find the answer to a question you have, then please do leave a comment or you can contact Annabel Fordham, Public Affairs Manager, Office of the Privacy Commissioner on annabel.fordham@privacy.org.nz
AN ELECTRONIC HEALTH RECORD FOR EVERY NEW ZEALANDER BY 2020: WHAT DOES THIS REALLY MEAN?  
KERRY BAKKERUS

The New Zealand Health strategy, released in April 2016 ‘sets the direction of health services to improve the health of people and communities.’ Part of the strategy includes provision for the delivery of a national electronic health record.

The strategy will impact how and where health records are stored and used by health practitioners and how patients will be able to access their health information. One can see the value and efficiency of a single record; however history has shown degrees of success and some failings from others that have attempted to achieve this.

The iappANZ’s event on 8 August 2016 (hosted by Chapman Tripp in Wellington and via video conference in to Auckland) sought to start a conversation, identify the learnings and key considerations from a variety of viewpoints - initiating thoughts and reflections to ensure that privacy remains the default setting – embedded through design. Speakers provided a multitude of perspectives, thoughts and lessons for consideration and a number of questions that need to be answered.

Is the benefit of a national electronic health record about ‘big data’ and the value this delivers? Malcolm Crompton (Australia’s Privacy Commissioner from 1999-2004, who led the ACC data privacy breach review) reflected on global scenarios where there has been improved learnings and patient outcomes with the aid of extensive health information. Documented evidence exists to support the benefits of a single health record – so why has Australia not delivered comparable benefits? For Australia, the motivation to move to a single record was to facilitate improved research outcomes and was not centred on improved health results. The model to deliver on this strategy was for individuals to opt-in, the resultant effect was that uptake was poor. This model has been revised and adjusted for greater gains. However, changes have been made without a corresponding variation to the governance model. This could potentially affect public trust. According to a survey from California in 1999, results indicated that a proportion of individuals would defend privacy at the expense of their health. According to Mr. Crompton, trust is about ‘saying what you do and doing what you say.’ Transparency is the key to maintaining trust. It is acknowledged that a great amount of benefit can be gained if it is done right.

According to the Ministry of Health, the national electronic health record will ensure that, ‘Privacy is assured’. For Dr Bernard Robertson-Dunn (Chair of the Health Committee of the Australian Privacy Foundation) privacy can never be assured. Dr Robertson-Dunn, who has specialised in developing models, highlighted that systems can only be respectful of privacy as the biggest risk to personal information is people. If the biggest risk to personal information is people, how does a national electronic health record ensure that information is restricted based on the ‘need to know’ principle? Reference to Dame Fiona Caldicott’s review of the United Kingdom’s National Health Service highlighted this too – how do we ensure that only the minimum amount of information required to deliver appropriate care is shared? A good governance framework is the starting point to manage privacy.

So how do we ensure that the focus is better patient outcomes and that the value is delivered? Sebastian Morgan-Lynch (Office of the Privacy Commissioner - Senior Policy Advisor: Health) indicated that to be successful we need to understand the critical elements of control, to manage the ever advancing technology developments. Mr. Morgan-Lynch reiterated and confirmed that for New Zealand as with other nations, ‘Privacy is all about trust.’
New Zealand has a number of successful regional shared records, however there is greater complexity at a national level. If privacy is to be maintained for the national electronic health record, stringent governance and security will be required to preserve trust – people need to believe that their information will be kept safe. The individuals managing our personal information can’t be seen to be ‘changing the deal’, where they say they will use the information for a particular purpose but ultimately do something else. Transparency, governance, security and control needs to be embedded within the frameworks for the protection of our personal information. A ‘culture of privacy’ is central to the success of the national electronic health record.

As with technology, the way in which people access the health system and the services they require is changing according to Dr Stephen Child (Chairman of the New Zealand Medical Association). Individuals are opting for convenience and reduced cost. It is however not clear whether the risk to the patient is clearly understood by those making these decisions. When compared to the free market of consumerism, health care still does not fall within this realm. A consumer has the ability to make informed decisions for themselves, this freedom is however limited for the patient. Individuals requiring health care generally still trust their general practitioner to provide guidance and decision support. Patients trust in their doctors because of their commitment to the Hippocratic Oath, that the patients’ interests are placed above those of their own. According to Dr. Child, the patient’s trust is based on the honesty, competence and reliability of their doctor.

Reflecting on a privacy breach at Auckland Hospital in September 2012, Dr. Child highlighted that the loss of patient trust was substantial, with consequences for staff severe. Notwithstanding the above, for Dr. Child the challenge is that 13-17% of the population is still not engaged with the health care system – often due to cost. These are generally the most vulnerable individuals potentially with the greatest health care needs. How can a national electronic health record influence greater outcomes for these individuals?

Ultimately, privacy is about the consumer. Barbara Robson (an experienced health consumer advocate) highlighted that it is about managing and delivering to expectations. There is an expectation that health information should not be shared, that there will be transparency and consultation. The approach for the national electronic health record needs to be taken carefully and with respect. Current concerns include future and secondary uses of the information, the agenda of multi-agency teams and cross sector sharing of information.

Although reservations are significant, individuals accept and acknowledge the benefits of a single patient record. Key themes need to be discussed and formalised to ensure the consistency and sustainability of privacy protection. Ms. Robson reaffirmed, as with other speakers, that this includes robust protocols for the privacy and security of personal information, designated authority to monitor governance with strong consumer representation, frameworks for the sharing of information, access rights and related audit procedures.
From a privacy perspective, it is clear that a number of considerations and learnings need to be taken into account for the national electronic health record to be a success. Key considerations and insights include:

- The motivating factor to proceed with the national electronic health record must be on the grounds that it will deliver improved health care outcomes for the patient. The value must be measurable.
- A good governance framework, underpinned by a culture of privacy, is required to manage and be responsible for the protection and security of personal information. The governance framework needs to be transparent and provide the individual with control of their information, an opt-out option needs to be incorporated. Privacy must be embedded as the absolute minimum – by default.
- Individuals involved with privacy and security of the information must be transparent and deliver according to the deal - ‘Say what you’re going to do and do what you say.’
- The transition of the patient to a health consumer is dependent on the increased health knowledge and maturity of the patient – opportunities to improve health literacy need to be identified and implemented.
- Consumer input should be included in all stages of the process to ensure that the expectations of the public are central to the process and incorporated as appropriate.
- Ultimately, patients are going to their doctors to be cared for, this involved listening; understanding and empathising – this can never be replaced with technology. This care is based on trust.

**Trust is everything.**

Special thanks to Katherine Gibson for her extensive involvement in the event. The speakers at the event were: Malcolm Crompton AM (Managing Director IIL Consulting and Board Director of IappANZ), Jill Bond (Executive Director, Office of the Director General of Ministry of Health), Sebastian Morgan-Lynch (Senior Policy Advisor, Office of the Privacy Commissioner, New Zealand), Dr Bernard Robertson-Dunn, (Chair, Health Committee of the Australian Privacy Foundation)

**ABOUT THE AUTHOR**

Kerry has recently joined Counties Manukau Health in South Auckland as their Risk and Privacy Manager, responsible to drive privacy maturity across the organisation. Prior to this Kerry, worked in a number of professional services firms including Ernst & Young and Deloitte for a total of 22 years helping clients manage different strategic and operational risks. Kerry has worked in a number of industries and sectors delivering projects ranging from fraud investigations, IT projects, assurance, data privacy and enterprise risk management. Privacy is paramount in the health sector, to maintain patient trust and confidence. Kerry is passionate about delivering solutions for the District Health Board that are fit for purpose and practical, making privacy easy to understand and embedding this as business as usual.

C
THE EYE OF THE BEHOLDER: ANALYSING THE RECENT “NRMA DETERMINATIONS”
HELEN LAUDER, JOHN FAIRBURN & MARTINA PASQUALINO

Two recent Australian privacy determinations highlight two situations where the OAIC took a different view to a business on the extent and the purpose for which personal information can be disclosed to customers.

The determinations concerned disclosures by an insurer to (a) a spouse and (b) a joint insurance policy holder of the respective complainants, which at least in some situations, could or would be entirely appropriate. However, in each case the disclosures were found to contravene the Privacy Act 1988 (Cth) (Privacy Act).

It is clear that decisions on the interrelationship of purposes of collection and disclosure, or whether sufficient steps have been taken to protect information, will vary depending on the facts. However, what the determinations highlight for all organisations is how upfront explicit notifications about potential information flows prior to implementing business practices is the best safeguard against privacy disputes. A thorough assessment of personal information flows in an organisation will inform these notifications. The determinations also provide useful guidance on the approach to the assessment of damages where there has been a breach.

Background

In the first determination, ‘IQ’ and NRMA Insurance, Insurance Australia Limited [2016] AICmr 36 (Determination 1), the complainant held a number of insurance policies with NRMA. The complainant’s spouse attended an NRMA office to inquire about CTP insurance.

In the process of calculating the no-claim bonus for the spouse, an NRMA staff member disclosed to the complainant’s spouse details of the complainant’s car insurance policies (which were not joint policies), including by turning the computer monitor around so that it was visible to his spouse, his daughter and (the complainant alleged) possibly others in the room.

In the second determination, ‘IR’ and NRMA Insurance, Insurance Australia Limited [2016] AICmr 37 (Determination 2), the complainant held an NRMA home building insurance policy jointly with another individual (Ms X). The complainant also held a number of other policies with NRMA, which were jointly held with the complainant’s husband and not Ms X. The renewal certificate that the complainant and Ms X (as joint policy holder) received contained details of all the complainant’s policies and assets insured with NRMA, including assets not related to the policy with Ms X.

In both determinations, the complainant alleged that NRMA interfered with the complainant’s privacy by:

1. improperly disclosing the complainant’s personal information; and
2. failing to take reasonable steps to protect the complainant’s personal information.

These allegations are discussed in turn below, followed by a consideration of the damages awarded in the determinations.

The timing of the acts the subject of the determinations meant that Determination 1 was based on the National Privacy Principles (NPPs), whilst Determination 2 was based on the Australian Privacy Principles (APPS). However, the differences between these principles does not impact the discussion below.
Disclosure of personal information

Under APP 6 (formerly NPP 2), an organisation is permitted to disclose personal information for a purpose other than the primary purpose of collection (secondary purpose) without consent if:

1. the secondary purpose is related (or directly related in respect of health information) to the primary purpose of collection; and
2. the individual would reasonably expect the organisation to disclose the information for that secondary purpose.

In both determinations, the Acting Australian Privacy Commissioner (Commissioner) determined that NRMA had improperly disclosed the complainant's personal information, thereby breaching NPP 2 or APP 6.

In Determination 1, NRMA argued that the disclosure was permitted under NPP 2 because the complainant would have reasonably expected NRMA to disclose his personal information for the related secondary purpose of calculating the no-claim bonus his spouse was entitled to.

Findings – Determination 1

The Commissioner found that:

1. it was not clear that information contained in the complainant's motor policy was necessary to calculate the no-claim bonus on the spouse's motor policy, and consequently, the requisite relationship between the disclosure and primary purpose of collection was not established; and
2. in any case, even if arguably the disclosure was made for the related secondary purpose of assessing the spouse's no-claim bonus, the complainant would not have reasonably expected the disclosure. In reaching this conclusion, the Commissioner focused on the documentation NRMA made available to its customers at the time. He emphasised that the relevant privacy policy did not state that customer information may be disclosed to family members. The Commissioner noted that, although NRMA's current privacy policy states that customer information may be disclosed to family members for purposes including pricing a policy, the act must be assessed at the time it occurred.

In Determination 2, NRMA argued that it was standard practice for a certificate of insurance to list all eligible policies that contribute to a customer's loyalty discount and to disclose this information to the joint policy holder. NRMA argued that the practice arose in response to customer feedback and enabled customers to check the accuracy of the policies listed to ensure their loyalty discount rate was correctly calculated. NRMA pointed to the fact that insured persons are informed:

1. via their product disclosure statement that their certificate of insurance will contain information to assist them in ensuring they are receiving the correct discounts; and
2. via NRMA's privacy policy that their personal information may be disclosed to a joint insured.

Based on these factors, NRMA contended that insured persons would reasonably expect NRMA to disclose their personal information on the certificate of insurance for the related secondary purpose of ensuring they receive the maximum discount they are entitled to.

The Commissioner accepted that using the complainant's policy information to calculate the loyalty discount could be for a related secondary purpose, and that disclosing policy information on certificates of insurance is associated with calculating a correct discount for the customer.

Findings – Determination 2

However, the Commissioner found that:

1. NRMA's disclosure to Ms X went beyond that by including details about the complainant's assets and that the link between that information and NRMA's calculation of the discount was tenuous; and
2. the complainant would not have reasonably expected the disclosure. Similar to the approach taken in Determination 1, the Privacy Commissioner considered whether the complainant would reasonably expect the disclosure by examining NRMA's privacy policy and a particular customer guide (Guide). It was clear that NRMA had notified its customers that their certificates of insurance would show a list of the policies that have contributed to their loyalty discount. However, the following factors led to the conclusion that the complainant would not have reasonably expected the full extent of the disclosure made to Ms X:

a) there was no explanation as to why personal information that contributes to the loyalty discount offered to joint policy holders, but that is otherwise unrelated to the policy being issued, is disclosed to a joint policy holder who has no connection with the information;

b) there was no information to suggest that customers would expect disclosure of their asset details to a joint policy holder who is unconnected to those assets;
c) there was no reason why a joint policy holder could not simply be advised that they are eligible for a loyalty discount because of the number of policies held by the other policy holder;

d) there was no explanation as to why policy numbers alone (rather than, eg. car model and property location) were not sufficient for the purpose of checking the accuracy of the data; and

e) the Guide only suggested that limited information would be included on insurance certificates (eg 'Third Party Fire and Theft'). In particular, the Guide did not inform customers that a detailed description of insured assets would also be disclosed on the certificates.

As such the Commissioner found that NRMA had breached APP 6.

**Reasonable steps to protect personal information**

Under APP 11.1 (formerly NPP 4.1), an organisation is required to take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. NPP 4.1 did not contain the reference to 'interference', although this is not material to the determinations.

The Commissioner came to different conclusions in each determination, finding in Determination 1 that NRMA had met its obligations under NPP 4.1, but finding in Determination 2 that NRMA had breached APP 11.1.

In Determination 1, the complainant alleged that NRMA breached NPP 4.1 by failing to take adequate security measures when the NRMA staff member:

1. failed to ask the complainant's spouse for proof of identification before discussing his policies with her; and
2. turned the monitor around towards the complainant's spouse and daughter, thereby also making the screen visible to passers-by in the NRMA office.

The Commissioner found that NRMA had met its obligations under NPP 4.1. In respect of the first allegation (failure to ask for identification), NRMA informed the Commissioner that:

1. NRMA uses a three-point identification process to confirm who it is transacting with; and
2. NRMA staff have access to 'Online Help' which is a tool utilised by staff to confirm the verification process that should be used, including when dealing with third parties and spouses.

The fact that NRMA had a policy in place, and the fact that staff could confirm the steps to be taken under this policy through the Online Help tool was sufficient for the Commissioner to find that NRMA had taken reasonable steps to protect the personal information. In respect of the second allegation (turning around the monitor screen), NRMA claimed that the practice of turning around monitor screens is only undertaken after the three-point identification check and staff are trained to ensure that adequate care is taken when sharing monitor screens (such as monitoring the distance from the waiting area to the screen to ensure those in the waiting area cannot see the screen). The Commissioner found that the staff training was a reasonable step to secure the personal information NRMA holds.

In Determination 2, the complainant contended that NRMA had breached APP 11.1 by including a description of her insured assets on the certificate of insurance, including those assets which were not insured jointly with Ms X. The determination again noted that this was an intentional practice of NRMA done to assist customers to easily confirm their information is accurate, up-to-date and complete. NRMA had made a considered decision as to the extent of asset information to be included on the certificate.

NRMA contended that some impact on an individual's privacy may be justified to ensure customers receive the benefit of any discounts to which they are entitled and to provide a way customers can check the accuracy of their information. The Commissioner stated that 'NRMA's contention that disclosure in this instance is a standard business practice is not an alternative to it meeting its obligations under the Privacy Act.'

**Factors for determining reasonable steps to protect data**

The Commissioner then considered the following factors in determining what were reasonable steps to protect the personal information (which are some of the factors listed for this purpose in the OAIC's Guidelines to the APPs):

The **sensitivity of the information**: The Commissioner noted that, although financial information is not 'sensitive information' (as defined in the Privacy Act), it is 'more sensitive' than other kinds of information, and individuals expect it to be subject to a higher level of protection.

The **possible adverse consequences for the individual**: NRMA argued that the disclosure on the certificate of insurance could not result in any adverse consequences for the complainant because Ms X could not obtain any additional personal information about the complainant from those policy details. However, NRMA conceded the possibility of Ms X fraudulently using the information. After referring to this concession, the Commissioner also noted that the more information disclosed about a person, the more vulnerable they become to misuse of, interference with, or inappropriate access to, their information.
The practicability of implementing a security measure:
The Commissioner found that a practicable step NRMA could have taken was providing less information. Alternatively, the Commissioner was of the view that notice of the extent of the disclosure to policy holders at the time of joining or policy renewal would provide policy holders with an opportunity to raise any concerns they had on the proposed disclosure. The Commissioner made it clear that notice may be a reasonable and practicable step to protect personal information.

Based on these considerations, the Commissioner determined that NRMA failed to comply with APP 11.1 by not taking reasonable steps to protect the personal information.

Assessment of damages
Under section 52(1)(b)(iii) of the Privacy Act, the Commissioner has a discretion to make a declaration that the complainant is entitled to a specified amount by way of compensation for any loss or damage suffered by reason of the act or practice the subject of the complaint (including injury to feelings or humiliation suffered).

In Determination 1, the complainant claimed that he experienced huge stress and anxiety as a result of the breach (resulting from concerns about the security of his vehicles), and the Commissioner accepted that this fell within the ambit of injury to feelings.

In Determination 2, the complainant stated that she experienced anxiety and distress as a result of the disclosure of her investment property location and car ownership details. The Commissioner accepted that disclosure of this information to persons unrelated to those assets may cause some distress or concern (particularly given that financial information is 'more private' than other kinds of information).

In assessing damages, the Commissioner considered the amounts awarded in previous privacy and discrimination cases, as well as the following principles on awarding compensation:

1. where a complaint is substantiated and loss or damage is suffered, the legislation contemplates some form of redress in the ordinary course;
2. awards should be restrained but not minimal;
3. in measuring compensation, the principles of damages applied in tort law will assist, although the ultimate guide is the words of the statute;
4. in an appropriate case, aggravated damages may be awarded; and
5. compensation should be assessed having regard to the complainant's reaction and not to the perceived reaction of the majority of the community or of a reasonable person in similar circumstances.

Based on these factors, the Commissioner awarded damages to the complainant in the sum of $2,000 in Determination 1 and $3,000 in Determination 2, both for non-economic loss.

In respect of Determination 1, the Commissioner expressed the view that, while distressing for the complainant, the breach did not command damages in the higher range because it was a one-off incident, it was not intended to upset the complainant (or his wife) and it was likely that the disclosure was limited to the complainant's wife and daughter. In respect of Determination 2, the Commissioner found that a modest, but not insignificant, amount of compensation should be awarded. In coming to this conclusion, he noted in particular that financial information is 'more sensitive' than other personal information and that the disclosure was an overt disclosure to a known third party.

Aggravated damages were not awarded in either determination as NRMA's conduct was not high-handed, malicious or oppressive and NRMA had been conciliatory in its approach.

Lessons learnt – privacy considerations in business practices
The determinations highlight the weight that needs to be given to privacy considerations when developing business practices. Practices that may make sense from a business perspective or customer service perspective, can still give rise to adverse privacy impacts. Where a practice involves the disclosure of a customer's personal information, even to their family or associates, the privacy impacts need to be thoroughly considered before it is implemented. For new projects, privacy impact assessments (PIAs) need to be part of the planning process.

PIAs can help organisations to address privacy risks, including by identifying those practices which can be changed to reduce privacy risks (such as disclosing less personal information to achieve a business aim) and identifying those uses and disclosures for which a 'reasonable expectation' needs to be raised. The latter will enable organisations to ensure their privacy policies and collection notices raise this expectation through the inclusion of relevant information. Determination 1 is a good example, where NRMA now has a privacy policy that the Commissioner suggested would have raised the required reasonable expectation had the Commissioner not been making
Mitigation - steps taken by NRMA

Although the Commissioner found that there were privacy breaches, the determinations also describe a number of positive actions taken by NRMA which affected liability and quantum. Organisations can learn from NRMA’s experience by:

1. documenting privacy practices and procedures, training staff on these practices and procedures, and making tools available to staff to enable them to easily follow the practices and procedures; and
2. taking a conciliatory approach to privacy complaints. The use of tests of reasonableness mean that privacy is by no means a black and white area. Judgment calls need to be made. Consequently, complaints and possibly breaches can sometimes be difficult to avoid. However, a conciliatory approach will both mitigate the effects on the complainant and potentially damages.

John Fairbairn, Helen Lauder and Martina Pasqualino are members of iappANZ
What certifications are available? Are they relevant to my work here?

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

To achieve either of these credentials, you must first successfully complete the Certification Foundation. The Certification Foundation covers basic privacy and data protection concepts from a global perspective, provides the basis for a multi-faceted approach to privacy and data protection and is a foundation for the distinct iapp privacy certifications.

What about testing?

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

FOR FURTHER INFORMATION
www.iappanz.org | +61 2 9431 8684
admin@iappanz.org
THE RECKONING: CENSUS FAIL
HOW BUREAUCRATIC AND POLITICAL
CHAUVINISM IN THE CENSUS DEBACLE LEAD TO
A MARVELLOUS RENDITION OF THE
EPONYMOUS AUSSIE BOYCOTT

KYLE LEES

Almost as soon as the Census 2016 campaign began, political, public and professional opposition to the national survey erupted, citing a lass of privacy issues and vocal opposition seeking to limit the kind of data the census could collect and keep. The Australian Bureau of Statistics bureau (ABS) is now facing reproach from both privacy and civil liberties groups over changes to the 2016 census – specifically around those manoeuvres which involve the acquisition and retention of people’s names and addresses.

Security, Surveillance and Trust

The current climate of mistrust around the ABS and government accountability generally, does not give credibility or confidence in the 100-year history of maintaining community belief in the way ‘[the ABS] collects, uses, discloses and stores your personal information collected in the Census.’¹ By its own admission, almost 20% of Australians don’t trust the ABS in protecting their data.² With over fourteen data breaches in the last three years, whilst the ABS ‘is committed to upholding the privacy, confidentiality and security of the personal information it collects’³; it has not done an exceptional job of this in the last month.⁴

² Media Release: Trust in ABS and ABS Statistics - A survey of informed users and the general community, 20 October 2015. See:
http://www.abs.gov.au/AUSSTATS/abs@nsf/be6aa82cd8c7f7f7ca2570d60013da27776f7c1ec02ef2b2dca257ee3000f5a40fOpenDocument
⁵ Timothy Pilgrim PSM, Census 2016 website incident, August 9, 11 August 2016, available at:
What's the Drama?

At the most recent Privacy Awareness Week (PAW), Privacy Commissioner Timothy Pilgrim noted:

‘Privacy is not secrecy. It is about giving individuals control over how their personal information is handled; creating customer confidence and trust. As such, good privacy practices and great innovation directly support each other.’

The key sticking point of the census this year appears to be the perception of the loss of control over the use of personal information, the inclusion of which - for the first time - has been mandated.

At first glance, and according to former Australian Statistician Bill McLennan, the ABS approach seems to be a direct and deliberate breach of the Australian Privacy Principles in the Privacy Act 1988. This denial of convention, statute and law, is a surprising action for an entity such as ABS to be taking. Moreover, McLennan highlights the broader risk here – that by forcing the collection of people’s names and addresses, the ABS has put the very success and value of the 2016 Census at significant risk. It is also clear from a plethora of study into this question over the years, including the Law Reform Commission Report: Privacy and the Census – that more than ever before, Australians are very concerned about the collection and use of their names and addresses, alongside their privacy generally.

Perhaps in 2016, this paranoia is more valid than in preceding times. The smacking irony is that the ABS didn’t engage with, consult, or try to speak to, the very same people it was attempting to gather information from. An approach which has now become clear, wasn’t transparent, and didn’t beguile the Australian public to any great levels. On this note, the ABS did present a Privacy Impact Statement (PIS) in 2015. What it failed to mention was that a similar proposal for the 2011 Census wasn’t allowed to proceed because of privacy concerns and the possibility of significant public backlash. McLennan questions: If this matching proposal was rejected in 2006 and again in 2011 for privacy and respondent reaction reasons, what has changed in 2016 that makes such a proposal acceptable? He also argues that under the Census enabling legislation, the ABS doesn’t have the authority to collect ‘name’ in the 2016 Census on a compulsory basis. Anna Johnston, a former Deputy Privacy Commissioner (NSW) echoes this interrogation, making a moral standpoint to not complete the Census over the very real fear of privacy intrusion. “Yes to a national snapshot. No to detailed data-linking on individuals,” she says. Like McLennan, Johnston was assuming that a vocal cacophony of public and political pressure would force the ABS to drop the proposal. Alas, the ABS has pushed ahead regardless – a move which may forebode the failure of a decidedly Sisyphean task.

10 The Law Reform Commission Report, Privacy and the Census, 1979
13 Ibid., See also: The Census and Statistics Act (1905) — Sections 8(3), 9.

Sisyphus (1548–49) by Titian, Prado Museum, Madrid, Spain
The Great Political and Social Boycott?

Greens senators Scott Ludlam, Janet Rice, Sarah Hanson-Young, Lee Rhiannon and Larissa Waters have joined fellow crossbenchers Nick Xenophon and Jacqui Lambie in saying they will refuse to give their names when they fill the census out. Ludlam paraphrases the thinking behind this partisan approach. “By ploughing ahead despite well-founded warnings by privacy experts, digital rights organisations and security professionals, the ABS has invoked a growing campaign of civil disobedience that will inevitably compromise the whole rationale for the census.” If we imagine the census itself as the focal point of vision, what and who remains outside delivers an interesting platform upon which to view the population – and demographical ideologies - of Australia. Sailing on this tack for a moment, the census debacle could deliver a view of Australians as a society cognisant of complex issues around privacy, technology, security and surveillance. That is, in the face of a myriad privacy, technology, and security concerns, many Australians have chosen to boycott the census. A move replete with politicism. The number of Australians making the decision not to complete the Census over privacy and security concerns remains monumentally unclear. In and of itself, the sheer taskforce of the census as a whole - is similarly as gargantuan. A metropolis, it employs close to 40,000 workers with which to cleave information from Australian households and gift it to the futurists behind the resource planning of Australia. Despite the political and public furore over the humiliating website outage on census night, it appears about 1.5 million more completed census forms than expected at this stage of the collection process. Of that, over 6 million of Australia’s 9 million households have now submitted a census form online or by post, a figure well above the 4.5 million responses the ABS had expected to receive. At a cost forecast at $470 million over five years to deliver the Census, this writer wonders if the call to try and mandate the names and addresses of Australia’s public, was worth it.

Kyle Lees writes in a personal capacity as a member of iappANZ

---

16 Ludlam, Scott, The Census should be delayed to restore trust and confidence, Guardian Australia, 4 August 2016. Available at: https://www.theguardian.com/commentisfree/2016/aug/04/scott-ludlam-the-census-should-be-delayed-to restores-trust-and-confidence
17 De Kerckhove, Derrick, “The Skin of Culture,” in Marshall McLuhan: Theoretical elaboration”, Volume 2, Taylor & Francis 2005. p 157. (In Japanese, ma, the word for space, suggests interval. It is best described as a consciousness of place, or the simultaneous awareness of form and non-form deriving from an intensification of vision).
19 Ibid.