PRIVACY UNBOUND

ISSUE 78
PRIVACY AWARENESS WEEK EDITION
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 email: opsmanager@iappanz.org

The Journal Advisory Committee is comprised of the following iappANZ board members and members:

Carolyn Lidgerwood
Kyle Lees
Marta Ganko
Katherine Gibson
Emma Kulintsch

Please note that the content published in the Journal should not be taken as legal or any other professional advice.
Welcome to the post PAW wrap up edition of the Journal. There was such a jam packed schedule in Australia and New Zealand across both PAWs in the last half of May with the theme this year was ‘Trust and Transparency. Don’t worry if you missed any of it – its all here, including the iappANZ breakfast series from IDCare. We were delighted to host Dave Lacey from IDCare who spoke about putting individuals and the damage they may suffer at the centre of an organisation’s data breach response. This can often get lost in a crisis.

There were some major lightbulb moments. iappANZ’s Olga Ganopolsky and Katherine Gibson give us their insights form the series. This consumer centric theme is also found in the new tool launched by the New Zealand OPC that Dame Diane Robertson, Cahir of the Data Futures Partnership spoke about – a framework for deciding whether organisations have a social licence to use and share data. Thanks again to Katherine Gibson for this report. Thanks also to Katherine for her report on Gethan Gunasakera’s presentation of his research on all the decisions of the Human Rights Review Tribunal under the NZ Privacy Act in the last 10 years.

We also have a report on Victoria’s PAW activities which were supported by the Office of the Victorian Privacy and Data Commissioner and the University of Melbourne. Keeping with the customer focussed theme, the OAIC tells us about its report on the results from its latest Community Attitudes survey (what sectors do we trust the most with our data?).

Marta Ganko shares the findings of Deloitte’s third annual assessment of the top 100 brands’ privacy practices in its 2017 Privacy Index, as digital connectivity poses more challenges as well as opportunities.

We have more reports from PAW activities and session in New Zealand and Australia including the role of privacy in the work of Counties Manukau (CM Health). Anna Johnston breaks down the disclosure principles in the Privacy Act. Stephen Wilson talks BlockChain in a way we can finally understand. Start investing in bitcoin everyone.

Finally thanks to Christopher Rogers for his report on the iapp global Summit.

Our Summit Advisory Committee are working hard on developing the program for this year’s Summit which will take place at Dockside, Sydney on Tuesday, 3 October with the theme “Privacy and Personalisation – Walking the Line”. Registration will open early next week.

The iappANZ Board hope to shortly announce the outcome of its search for a CEO to help drive the strategies the Board has set. We will also be reaching out to sponsors with our updated sponsorship packages. Thanks as always for their support which is critical.

Enjoy the Journal.

Veronica Scott
Vice President
iappANZ
The highlight of this year’s Privacy Awareness Week (PAW) was the release of the 2017 Australian Community Attitudes to Privacy Survey (ACAPS) — the longest-running privacy survey in the country, mapping Australians’ privacy expectations and behaviours since 1990. The 2017 ACAPS provides insights relevant across all industries and sectors at a critical time, when data is increasingly utilised as a resource to inform the development and improvement of products and services. The ACAPS found that the majority of Australians remain uneasy about engaging with organisations online, with 83 per cent saying that this is inherently more risky than dealing with an organisation in-person, or through other more traditional channels. People similarly perceived risks in data-sharing, and the secondary use of information. Only one in ten Australians are comfortable with their personal data being shared between businesses. 86 per cent said they considered it misuse of personal information if that information is used for a purpose other than the one it was provided for. There was also a general consensus that personal information being sent overseas was something to be concerned about (93 per cent). These concerns factor into individuals’ decisions on which businesses they interact with. Around six in ten Australians (58 per cent) have decided not to deal with a business because of privacy concerns. And despite Australians’ reputation as early adopters of new digital devices, 44 per cent said they have chosen not to use a mobile app for privacy reasons.

These results highlight the importance of organisations developing and implementing a privacy culture that reflects this year’s PAW theme — trust and transparency.

Through transparent information handling practices, and ensuring individuals are aware of how their personal information would be managed, organisations can build trust and community confidence.

Transparent data handling practices may also be used to address widely shared beliefs that online environments are inherently risky. While the majority believe privacy risks are greater online than off, this does not necessarily reflect actual risk; in fact, many of the privacy breaches the OAIC deals with are offline and low-tech. Given the desirability of promoting the use of digital platforms to improve efficiency and product and service delivery, it is key for organisations to demonstrate, and build public confidence in, their dedication to privacy best practice.

The same may be said for the community’s perception of data-sharing — which is particularly relevant for government agencies and open data initiatives. The ACAPS found that people are more comfortable with agencies sharing personal information (33 per cent), which is significantly more than with the private sector. A new question also found that 46 per cent are comfortable with government data-sharing for “research, service development, or policy development”, and a further 21 per cent hadn’t made up their minds on where they stood on the issue. This suggests that when a clear case is made as to the benefits of the re-use of personal information to the community, there is fertile ground for broad public support.

Significantly, the ACAPS revealed that the health, financial, and government sectors remain the top three most trustworthy in terms of privacy management. The government’s third place position further supported the development of the recently announced Australian Public Service (APS) Privacy Code, which will take effect on 1 July, 2018.

The APS Privacy Code is a binding instrument created under the Privacy Act 1988 that will apply to Australian government agencies — and is designed to establish a single high standard of privacy practices across all agencies. The Code reflects the role of government agencies should take in modelling leading privacy best practice. Commonwealth agencies have unique abilities to collect and hold personal information – as individuals are often required, by law or by practical circumstances, to provide it. It is essential then, for Commonwealth agencies to be viewed and trusted as national leaders in personal information protection. The APS Privacy Code, which will take effect in 2018, will help all agencies build the capacity, capability and advocacy to create a single best-practice standard across the Australian Public Service.

You can read more about the APS-wide Privacy Code on our website.
As part of celebrating Privacy Awareness Week in Australia IAPPANZ hosted events across three Australian capital cities featuring Professor David Lacey, Managing Director of IDCARE[1], a non-profit organisation that helps individuals and organisations manage the outcomes of a data breach and helps mitigate some of the damaging consequences. Starting in 2014, IDCARE has assisted 2000 clients (consumers, government agencies and private sector organisations) to handle data breaches.

**Introduction and Notifiable Data Breach**

In Sydney the session was introduced by Andrew Solomon of the Office of the Australian Information Commissioner (OAIC), setting the scene for the pending discussion by articulating the key features of the Notifiable Data Breaches scheme (NDB), due to come into effect in Australia on 22 February 2018[2]. A Notifiable Data Breach is a data breach that is likely to result in serious harm to any of the individuals to whom the information relates. Examples of a data breach include when:

- a device containing customers personal information is lost or stolen
- a database containing personal information is hacked
- Personal information is mistakenly provided to the wrong person.

Attention quickly turned to the key features of the NDB scheme which will require organisations[3] to:

- Carry out a reasonable and expeditious assessment of whether there are reasonable grounds to believe that the circumstances amount to an eligible data breach and take all reasonable steps to ensure that the assessment is completed within 30 days after the entity becomes aware of the suspected breach[4];
- Notify affected individuals and the OAIC of eligible data breaches[5].

At the heart of the dilemma is the fact that organisations are called upon to assess what ‘harms’ are likely to befall an individual (now or in the future) arising out of the particular breach as known to the organisation at the time. While the law on the subject is clearly driven by an objective standard[6] the types of factors that may cause harm (let alone serious harm) for one individual or a set of individuals may vary greatly depending on the circumstance highly unique to that person or persons and not necessarily known or let alone well understood by the organisation experiencing the breach event.

This is where the experience that IDCARE in handling data breaches is so vital and helps shed light on what is often a delicate factual balance between objective and reasonably well understood and known factors versus the less obvious and possibly highly subjective factors.

**Risky practices and inevitable crisis events**

David Lacey explained that that the key to dealing with a data breach starts with accepting two important propositions. Firstly, that the data breach event is a crisis event and, secondly, that a data breach is inevitable. A crisis is defined as a ‘perception or experiencing of an event or situation as an intolerable difficulty that exceeds the persons current resources and coping mechanisms... crisis has the potential to result in severe affective behavioural and cognitive malfunctioning’[1]. This elicits a fight or flight response in participants. The fight or flight dynamics impact on the psychological factors affecting the response of all participants or stake-holders in the data breach event and therefore its effective management. Accepting that data breaches are inevitable impacts how one prepares for the situation. The key is planning and understanding the so called ‘risky practices’ and their impact on individuals in the event of a breach.

IDCARE has identified a number of such risky practices. These typically include a combination of technical and human factors and apply to large and small organisations alike. Some examples includes failure to install anti-virus/firewall protections for remote working arrangements, absence of information management controls that prevent or detect bulk data uploads, poor disposal practices, uncertainty as to who is responsible for cyber security and downplaying or underestimating the risk involved to the individuals.

The damage to individuals can be far reaching and difficult, if not impossible, to fully mitigate or resolve. For example, in a case involving identity takeover (which may have been prevented if the client was notified promptly of a Malware attack) the client’s superannuation funds were severely compromised due to identity takeover and fraud. The client is now prevented from retiring because a substantial part of their superannuation savings has been lost. Some types of damages are purely psychological. For example, genuine fear arising out of an unauthorised disclosure of contact details of a victim of violence and their dependents. Both examples demonstrate the far-reaching impacts on individuals, albeit for different reasons.
Lessons learned?

If data breaches are indeed inevitable, then what is the role of the privacy professional and what are the lessons learned to date? The presentation by David Lacey in some ways seems to de-stigmatise the breach itself and focuses the attention on the response post the discovery of the breach event. Clearly, it is important to take steps to secure the personal information and avail yourself of the tools available, be they data loss prevention tools, secure handling and disposal of information and other preventative and detective controls available in the market. However, regardless of the technical cause of the given breach, the IDCARE presentation reminded privacy professionals that their respective organisations will be ‘judged’ by the quality of the response to the affected individuals not simply its causes. Many factors relevant to an effective response are in the realm of ‘soft skills’ and the ability to understand the human factors involved in the crisis event, both within and outside the organisation.

IDCARE’s approach proceeds on the basis that notification is a positive public step and not notifying or delaying notification is a high risk strategy, especially where the breach is more serious.

David Lacey said that ‘default position should be to notify unless there is a very good reason not to’. In IDCARE’s experience, elements of a ‘good’ response are:

- **Communicating well and, if need be, often**: It will be important to inform individuals of what occurred and do so in a factual manner, avoiding supposition and assumptions. Be the point of ‘absolute truth’ said David Lacey. Sometimes, this could be as simple as explaining that you are investigating particular aspects and that you will be in contact again in a given period. If you have a call centre it, use it and if need be set up a domain or sub-domain to address the breach. If there is something that you would like your customers to do or not do, tell them! For example, to change their passwords or not to respond to certain types of messages or messages from certain sources.

- **Be Quick**: Don’t wait for all the facts to be fully tested and reconfirmed. The first 72 hours will be key. Leaving things for more than 4 to 5 days after your organisation becomes aware of the data breach is perceived as too long.

- **Clear roles**: Define the roles (in advance) especially as these relate to stakeholder management and make sure that all actions are logged. The response will inevitably require a multi-disciplinary approach so make sure that roles such as IT, Security (physical and IT), Legal, Compliance and Governance, and Communications (internal and external) are part of your planning and the response. A key aspect of the plan is connecting these roles and helping to co-ordinate their activities.

- **Focus on the individual**: The overarching theme in the approach taken by IDCARE is the centre stage that the individual plays and the impact on that individual, regardless of the precise nature of the relationship your organisation has with that person. The response to the data breach should not be driven by whether they are a current or former client of your organisation or the nature of the services or the longevity or history of the relationship. They key is what harm the individual is exposed to as a result of the breach and your role in seeking to prevent or mitigate the harm.

Conclusions

Handling a data breach response well will help build trust. A poor, badly co-ordinated or delayed response erodes or destroys trust. The key is to plan and to put the individual affected in the centre of that plan. Thanks to Professor David Lacey, and our venue hosts Minter Ellison in Sydney and Melbourne, and Corrs Chambers Westgarth in Brisbane.

Olga Ganopolsky is General Counsel, Privacy and Data at Macquarie Group and an iappANZ Board Director

[1] David Lacey is also a Professor of Cyber Security, USC
[2] The Office of the Australian Information Commissioner is developing guidance and organising events to help organisations understand their obligations under the NDB scheme, and prepare for commencement.
[5] Section 26 WE (2) of the Privacy Act 1988 (as amended by the Privacy Amendment (Notifiable Data Breaches) Act 2017)
When there is a data breach, the main priority for the organisation is almost always protecting their brand and minimising damage to their reputation. They often forget that a privacy breach involves a person who will be experiencing harm - on many levels.

During his presentation hosted by iappANZ Rights, Responsibilities, and Roller-Coasters: The Inevitability of a Data Breach, Professor David Lacey provided us with insights into the roller-coaster ride experienced by organisations and affected people when a data breach occurs. He stressed organisations must resist the temptation to desensitise their response to a data breach. They must consciously take steps to translate what has happened into the human experience of the individuals that are suffering the data breach.

About IDCare

IDCare is a national identity and cyber support service for New Zealanders and Australians. It provides free and anonymous support to people who believe their personal information has been put at risk in any way (online or physical).[1] IDCare aims to empower the individual with knowledge and a pathway to reduce the harm they experience as a result of a data breach. It also assists organisations prepare for and manage data breaches.

The lighter side of the presentation

A couple of interesting Trans-Tasman comparisons were made by Professor Lacey (who happily resides on the Sunshine Coast in Queensland):

- New Zealand experiences more data breaches per year than Australia. For the 2016 reporting period, voluntary notifications were New Zealand - 148 to Australia - 107. Professor Lacey wondered whether this was actually the case, or whether “New Zealanders were more honest that Australians”, much to the amusement of the Kiwi audiences in Wellington and Auckland.
- The time taken for an impacted individual to respond to a data breach is, on average, 4.3 hours faster in New Zealand. New Zealand - 13.1 hours to Australia - 17.4 hours. An explanation offered was that Australia has significantly more bureaucracy than New Zealand - he was really appealing to the New Zealanders in the audience!

The harm

All jokes aside, this presentation was about a serious topic. Organisations must not forget that there is a human side to a data breach and organisations must acknowledge this and take steps to reduce the harm. Professor Lacey also stressed the focus needs to be on all individuals. Organisations should not forget that former and prospective clients matter too. Three types of harm following a data breach were discussed:

1. Direct Harm.

The likelihood of the harm to the impacted individuals of a direct misuse of the information that has been breached. This is usually the focus of the organisation and they often assess the risk from their business perspective. We were reminded that “risk is in the eye of the beholder” - it is the risk of harm to the individual (and not just the organisation) that must be assessed.

2. Indirect Harm. The likelihood of a person suffering harm indirectly. For example receiving spam, phishing emails or phone calls.

3. Response Harm. The harm suffered by the individual in responding to the data breach.

It was this last form of harm that most organisations simply fail to consider, yet the response harm can be significant to the individual. This is the harm suffered in having to take steps to prevent identity theft, such as reporting to the Police, checking your credit file and requesting your credit file be suppressed, changing contact details, checking bank accounts and replacing a drivers licence or passport.

Professor Lacey spoke about the recent data breach experienced by the New Zealand Nurses Organisation. As a result of a spear phishing scam, all of the organisation’s members’ names and email addresses were accidently disclosed. IDCare carried out an independent review of the cyber incident. He said that the organisation’s focus was very much on helping its members and urged us to read the report.[2]

Adding to the response harm is that there are multiple actors in a response and this leads to the inefficiency of the response. In Professor Lacey’s view, it is the responses of the other organisations that the harmed person must deal with - such as the Police, the credit reporting bureaux, the banks and telcos - that will influence the perception of how the person feels about the organisation who caused the data breach. Also, there is no one central agency to report to who can then act as the lead agency in assisting the individual when they have suffered a data breach.
Professor Lacey laid down a challenge for us - he said if any place could create an agency for this very purpose, it was in New Zealand. The audience was left pondering how this could be achieved.

The first 72 hours - it’s important, so have a plan and practise it.

We were reminded that a data breach is often a crisis situation for an organisation and unless the response has been rehearsed and prepared, decisions can be made dominated by emotion, leading to poor decisions. Crisis is particularly acute where the media is the first to notify the public of the breach, where the organisation is a small business or a government agency or where the breach is high risk. In his view, the first 72 hours will be the big test and how an organisation responds in this time will often dictate how well their response is perceived. IDCare can assist agencies in their response when a data breach occurs.

This was a presentation packed with plenty of new information - a data breach through the lens of the impacted individual. Lots of valuable takeaways for the privacy professional. Thanks to Professor David Lacey, iappANZ and our hosts Ernst Young in Wellington, Buddle Findlay in Auckland.

Katherine Gibson is the Director of Gibsons Law Limited in Auckland
www.gibsonslaw.co.nz

In addition to the fantastic session from Prof Dave Lacey about IDCare hosted by Minter Ellison, Victoria also enjoyed a number of other events for PAW 2017 co-hosted by the University of Melbourne and the Commissioner for Privacy and Data Protection.

There was a public forum on surveillance with a panel of speakers debating the tensions between privacy, civil liberties and national security in the surveillance state.

This was followed by a seminar on Look what they’ve done to my data: issues in privacy, security and data protection. An interesting panel from the fields of big data, information security and artificial intelligence.

There was also an event hosted by the Commissioner’s Youth Advisory Group (YAG) which explored how different generations perceive the concept of privacy and what it means to them.

Here is a takeaway on CCTV Surveillance in Victoria

Julianne Brennan who is the director of Community Crime Prevention Unit at the Department of Justice and Regulation talked about delivering Government policy in support of crime prevention in the context of providing grants to enable Councils to establish CCTV in public places.

Key takeaways:

- CCTV was not a panacea to stop crime but is one tool that should be used as part of a holistic strategy;
- what was important was the cohesion of community and a holistic approach to crime prevention and solutions;
- the approach should address community safety, as well as perceptions of safety which are as important;
- as a guiding principle, just because you can install CCTV, doesn’t mean you should;
- councils need to look at what safe guards are required and balance reasonable expectations of privacy in public places against concepts of safety and what a community needs to feel safe including law enforcements. It is a matter of proportionality.

Interesting fact – the increase CCTVs have mostly been sought by Traders Associations. However, Unit only funds local government because it is local government that is subject to privacy laws and not local traders.

Application process

They Unit has a very robust application process and requires evidence of the need for CCTV to address an existing problem including how the Council will manage CCTV. They ask questions such as what is the Council’s code of conduct and the standard operating methods and the purposes for which they collect CCTV. The maximum period CCTV recordings can be kept is 30 days unless an offence has occurred. The local area commander also has to provide a letter of support and the footage can only be shared for law enforcement in crime prevention issues.

Privacy protections

The Unit has developed a standing Memorandum of Understanding between Victorian Police and local government in relation to the management of CCTV cameras. Local government has no access to the footage – it is transmitted directly to the Victorian Police where it is subject to limited access and appropriate controls. VicPol are also subject to law enforcement and protective data security obligations in the Privacy and Data Protection Act 2016

The Victorian Privacy and Data Protection Commissioner has also issues guidelines on public sector use of CCTV.

Veronica Scott is Special Counsel at Minter Ellison Lawyers (Melbourne)

Dushan Stevic is a Graduate at Minter Ellison Lawyers (Melbourne)
NEW ZEALAND'S SOCIAL LICENCE TO SHARE DATA
OPC PRIVACY WEEK, PRIVACYLIVE SPEAKER SERIES
DAME DIANE ROBERTSON, CHAIR DATA FUTURES PARTNERSHIP
Katherine Gibson

Shortly a significant resource will be added to New Zealand’s privacy toolbox: a framework for Government and businesses to use when considering whether they have the "social licence" to use and share data. By following these guidelines, agencies can gain confidence that they have the acceptance and trust of people to use and share their data in the way they want to. This framework will not only be valuable to privacy professionals, but to all who are involved in data use and sharing decisions.

The Social Licence Framework

The framework is currently being developed by the Data Futures Partnership, an independent group created by the New Zealand Government to develop innovative solutions to data-use issues. The Partnership considers a social licence to use data will be given “when people trust that their data will be used as they have agreed, and accept that enough value will be created.”[1] Their aim is to develop a set of guidelines to help organisations (both public and private agencies) in their efforts to build and maintain the trust of people whose data they wish to use and share.[2] Dame Diane Robertson, Chair of the Partnership, shared with us the work they have been doing in developing these guidelines as well as some learnings along the way. Dame Diane said that we are entering into a new era of data use. Data is not just the new oil, it is “faster than oil”. We are chasing to keep up with technology, analytics and capability and organisations need to establish a safe and trusted environment for using and sharing data. She warned us that to do this, the focus must not be on just individual rights, privacy, ethics and human rights. Driving trusting data is about genuine engagement with people. It is not stopping at the question "can we use and share the data this way?". It is going further and asking "should we use and share the data this way?" These are the new rules for this "new world".

Integral to the development of the guidelines has been finding out the views of New Zealanders. This was achieved by 27 face to face workshops (about 400 people) and on-line questionnaires (about 4,000 people) where people were asked about how they feel about their data being used and shared in different situations. The themes that have emerged that will form the basis of the guidelines are:

- **Purpose**: what is the data being used for?
- **Value**: what is the value to both the organisation and individual?
- **Use**: when will the data be used and will it be reused?
- **Control**: who controls the data?
- **Security**: how secure is the data?
- **Transparency**: people being able to “see” purpose, value, use, control and security.
- **Governance**: what is the governance framework?

Arisings from this is the question of whether there is a need for a Data Commissioner to govern the use of sharing of data.

Views of New Zealanders

Through the public engagement process, there were some other learnings, many of which reinforce views currently held:

1. Organisations generally do not have protocols on sharing data.
2. Data is not always in good condition.
3. Organisations forget data is about people and that data is not an "innate thing"
4. New Zealand’s have a very high level of trust that their GPs will look after their health data.
5. Comparatively, there is a high level of mistrust in sharing educational data.
6. Older people are information savvy too. While they may not be technologically savvy, they have experienced life events that influence their views on data use and sharing.
7. Younger people generally have no idea who they are giving their data to.
8. People accept data can never be 100% secure but they do not like it when there is a data breach and the organisation will not be accountable and fails to take steps to make it right and make changes to their processes and systems.

Re-identification issues

Dame Diane also commented on the issues encountered when considering re-identification of information. A fundamental issue here is the lack of common terminology: what is “anonymised”, “de-identified” and “re-identified” data? The Partnership considers there needs to be an agreement on these important terms. In carrying out their work they have found people were sceptical about anonymisation and the more people are involved with Government the less they trust them. A question was also posed: is there a need for legislation on re-identification and how is this to be achieved?
in specific legislation (for example, privacy, statistics and justice legislation) or in overarching legislation?

Avoid the negative – focus on the value

Finally we were challenged to avoid a "deficit approach" to data use and sharing and focus on its benefits to the organisation and individual. A deficit approach is where the organisation simply considers "negative" uses of data. For example, the data will be used to make decisions on whether a person receives a social benefit. Organisations will need to widen their lens and consider the ways in which the data can be of value to the organisation as well as the people. Dame Diane asked us: "Many of you will have risk registers but how many of you have value registers?". It was an information packed presentation and we look forward to the publication of the guidelines - which are due to be released in June. Thanks to Dame Diane Robertson, the Office of the Privacy Commissioner and Southern Cross Health Society as venue hosts.

Katherine Gibson is the Director of Gibsons Law
Limited in Auckland
www.gibsonslaw.co.nz

[2] Ibid.
“Organisations are under increasing pressure from an ever evolving digital, connected and innovating world. When it comes to privacy practices they can no longer have a set and forget mentality. Policies and procedures and behaviours must align. We have reached a point where the introduction of new digital technologies requires active monitoring of consumer information risk exposure.”

- 91% of organisations believe their organisation could be more transparent with consumers about how their information is used.

- 59% of organisations believe they are neglecting to build trust with their employees.

- 58% of employees believe that regulatory compliance is more important to their organisation than building trust with customers (36%)

- Financial services have the best privacy governance and least risk taking followed by Government.

In Deloitte’s third annual assessment of the privacy practices of the top 100 brands in Australia, both listed on the ASX 100 as well as non-listed, there is some disconnect between what organisations do and what their employees want them to do. We surveyed more than 1000 employees of these top organisations, asking for their opinions of their organisation’s privacy practices, in particular their expectations of trust, complaints and information handling.

In this index we wanted to see if there was any difference between what organisations and what staff members believe is occurring when it comes to protecting data and honouring customer privacy.

Why from within?

This year’s focus on employees as the consumers was because most organisations in Australia have reached a level of maturity in their website privacy and security controls and policies. The reality is that mobile apps are now more open and transparent to consumers, so we wanted to discover if there was any dichotomy between organisational governance practices and actual operations. And we found that there was. An organisation may feel for example, it has all the requisite boxes ticked, and all its policies and procedures in place. Yet it appears that many staff members own up to circumventing these processes (21% of respondents may have let someone at work use their work password and 35% use the same password across multiple sites). So our findings show that employees do find what they consider to be easier ways of doing things, even if adequate monitoring processes are in place.

A key finding was that 91% of organisations believe their organisation could be more transparent with consumers about how their information is used. And almost 60% of organisations believe they should do more to build trust with their employees. “When there is transparency in how personal information is used, it gives individuals clarity, choice and confidence that their privacy rights are being respected” Timothy Pilgrim, Australian Privacy Commissioner.

Given the current situation of “could do better”, plus the future direction for organisations both here and around the world, where individuals are being offered greater control over the collection and sharing of their data[1], our organisations have a big challenge ahead to maintain and/or build trust. They need to focus on developing resilience and creating an environment of real consumer and business confidence.
The most trusted industries in the Deloitte Australia Privacy Index 2017 overall are:

<table>
<thead>
<tr>
<th>Sector</th>
<th>Ranking 2017</th>
<th>Ranking 2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial services</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Government</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Telecommunications &amp; media</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>Energy &amp; utilities</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>Industrials</td>
<td>5</td>
<td>N/A</td>
</tr>
<tr>
<td>Health care</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>Consumer/retail</td>
<td>7</td>
<td>10</td>
</tr>
<tr>
<td>Real estate</td>
<td>8</td>
<td>13</td>
</tr>
<tr>
<td>Information technology operations</td>
<td>9</td>
<td>7</td>
</tr>
<tr>
<td>Materials</td>
<td>10</td>
<td>N/A</td>
</tr>
<tr>
<td>Education</td>
<td>11</td>
<td>6</td>
</tr>
</tbody>
</table>

Each of the top three sectors in this year’s Deloitte Privacy Index have employees who said they would be comfortable being consumers of their own employer’s brand (91%).

That speaks volumes for the importance of privacy awareness.

Marta Ganko is a Director and Privacy & Data Protection Lead at Deloitte and board director of iappANZ

We believe one of the reasons the financial sector ranked at the top of the index again this year, followed by Government and, for the first time in the top three, telecommunications and media, is because all three sectors are highly regulated. Financial services conduct frequent privacy training (nearly 40%). Their employees can more often correctly identify a need for a privacy impact assessment, and they know the process to follow in the event of a data breach and they require their third parties to notify them in the event of a likely breach (75%). They also have appointed a Privacy Officer within their organisation, and conduct formal privacy impact assessments for each significant change.

We surveyed individuals employed across these 11 industries to see if behaviours outside work translated to roles within their organisation.

<table>
<thead>
<tr>
<th>Government</th>
<th>Health care</th>
<th>Education</th>
</tr>
</thead>
<tbody>
<tr>
<td>12%</td>
<td>2%</td>
<td>12%</td>
</tr>
<tr>
<td>Consumer/retail</td>
<td>Financial</td>
<td>Information technology organisations</td>
</tr>
<tr>
<td>12%</td>
<td>1%</td>
<td>10%</td>
</tr>
<tr>
<td>Industries</td>
<td>Telecommunications and media</td>
<td>Energy and utilities</td>
</tr>
<tr>
<td>5%</td>
<td>1%</td>
<td>6%</td>
</tr>
<tr>
<td>Materials</td>
<td>Real estate</td>
<td></td>
</tr>
<tr>
<td>5%</td>
<td>5%</td>
<td></td>
</tr>
</tbody>
</table>

The participants we surveyed held the following roles:

- Board member
- Chief executive group
- Director
- Manager
- Professional services provider
- Analyst/Developer/Policy officer
- Customer service
- Support services
- Other

[1] The Australian Federal Treasurer announced the potential for greater controls for consumers to both manage access to and the sharing of their data as enacted in other parts of the world, including the European Union. They are the Revised Payment Services Directive (PSD2)[1] and the General Data Protection Regulation (GDPR)[1].
UPPING THE ANTE: NEW ACTORS AND THE CONSEQUENCES OF BREACHING NEW ZEALAND’S PRIVACY ACT 2017 PRIVACY WEEK PRESENTATION BY ASSOCIATE PROFESSOR GEHAN GUNASEKARA
Katherine Gibson

Associate Professor Gehan Gunasekara kicked off New Zealand’s Privacy Week with a thought-provoking question to those attending his presentation entitled “Upping the Ante - New Actors and the Consequences of Breaching the Privacy Act”. Was the change in the chairperson of the Human Rights Review Tribunal a reason for the significant increase in the amount of damages being awarded for an interference with privacy under New Zealand’s Privacy Act? This was not a novel question, having its genesis in a submission by the Ministry of Social Development to the High Court in its appeal on an award of damages granted by the Tribunal against the Ministry.[1]

“*The appellant’s argument is that since the appointment of Mr. Haines QC as the new chair of the Tribunal it has lifted its award of damages. The appellant says this lift is inconsistent with the High Court authority, and that it is beyond the Tribunal to do that.*”

With that background, Professor Gunasekara presented us with some fascinating draft findings of research undertaken by himself and Niveet Singh (University of Auckland Business School) examining emerging trends in recent Tribunal decisions. All 69 substantive decisions[2] under the Privacy Act jurisdiction over a 10 year period from 2007 had been reviewed. Decisions for the five years preceding the appointment of the current chairperson of the Tribunal were contrasted with the decisions in the five years after his appointment. The draft findings were:

2. Damages awards have risen during the current chairperson’s tenure. The mean of damages awards (excluding *Hammond*) has doubled during this time: from $5,812.50 (2007 - 2011) to $13,181 (2012 - 2016).
3. Whilst damages awards have increased since 2012, the research could not support a finding that the chairperson was the reason for the increase.
4. There has been a recent growth in the number of private sector defendants who over the last 5 years made up 46% of defendants: compare 21% for the 5 years to 2011. This could be a reason for the increase in damages awards.
5. Significant damages have been awarded in the last 5 years against private sector defendants who failed to respond to access requests on time.
6. The authors found that one of the most revealing aspects of the research was the success rates since 2011 of claimants who had legal representation[4] - being as high as 85%.
7. The number of cases being taken by the Director of Human Rights Proceedings is declining, with only two being brought in each of the past two years (2015 and 2016).
8. The current Tribunal will make orders for specific performance and training. There were no such orders made in the 5 years preceding the current chairperson.

A summary of the draft findings are:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Chairperson</td>
<td>Mr Royden Hindle</td>
<td>Mr Rodger Haines QC</td>
</tr>
<tr>
<td>Number of cases</td>
<td>28</td>
<td>41</td>
</tr>
<tr>
<td>Public Sector defendant</td>
<td>79%</td>
<td>54%</td>
</tr>
<tr>
<td>Private Sector defendants</td>
<td>21%</td>
<td>46%</td>
</tr>
<tr>
<td>Claim linked to pre-existing dispute</td>
<td>81%</td>
<td>81%</td>
</tr>
<tr>
<td>Successful claims</td>
<td>32%</td>
<td>54%</td>
</tr>
<tr>
<td>Unsuccessful claims</td>
<td>68%</td>
<td>46%</td>
</tr>
<tr>
<td>Success rate - represented litigants</td>
<td>42%</td>
<td>85%</td>
</tr>
<tr>
<td>Orders for specific performance</td>
<td>None</td>
<td>7</td>
</tr>
<tr>
<td>Training orders</td>
<td>None</td>
<td>4</td>
</tr>
<tr>
<td>Damages Awarded – Range</td>
<td>$3,500 - $10,000</td>
<td>$400 - $25,000</td>
</tr>
<tr>
<td>Damages Awarded – Mean</td>
<td>$5,812.50</td>
<td>$13,181</td>
</tr>
<tr>
<td>Damages Awarded – Median</td>
<td>$6,000</td>
<td>$15,000</td>
</tr>
</tbody>
</table>

Professor Gunasekara challenged the jurisdictional basis of the training orders which often require the defendant and its staff to undergo a training programme, at its own expense, in conjunction with the Privacy Commissioner. Whilst the Tribunal is not always clear in the decisions on its power to make such orders, it may be doing so under the power to require a defendant “to perform any acts specified in the order with a view to remedying the interference” as well as the catch-all “other relief as the Tribunal thinks fit”. [6]

Unlike the Human Rights Act 1993, there is no explicit provision in the Privacy Act for the Tribunal to make training orders. A concern was noted: despite a High Court ruling that the Tribunal has no jurisdiction to make such orders[7] it continues to make training orders, and these remain unchallenged by those agencies ordered to do so. But as explained, this is the commercial reality of not wanting to incur further costs in an appeal as well as adverse publicity what responsible agency would refuse to undertake privacy training where the Tribunal has found its processes and systems are deficient?
A thoroughly enlightening hour. We came away with plenty of useful information to support a case for those yet to be convinced that privacy must be taken seriously - damages are on the increase for an interference with privacy.

Professor Gunasekara and Naveet Singh have written a paper discussing the research and their findings as well as the authors’ insights into some of the Tribunal decisions. They hope it will be published shortly. A must read for all privacy professionals. Thanks to Professor Gunasekara and Naveet Singh and the Office of the Privacy Commissioner and the University of Auckland Business School for hosting us and providing lunch.

Katherine Gibson is the Director of Gibsons Law Limited in Auckland
www.gibsonslaw.co.nz

[1] Chief Executive of the Ministry of Social Development v Holmes [2013] NZHC 672 at 126. The appeal was dismissed.
[2] This excluded preliminary and interlocutory rulings, strike-out applications and applications for costs where claims were discontinued. A case that was appealed to the High Court or the Court of Appeal was counted once.
[4] Including legal representation, “MacKenzie-friends and cases brought by the DHRP.
[5] This excludes the Hammond decision.
Auckland Council – New Zealand’s largest local government agency and one of the country’s biggest employers – celebrated Privacy Week with a panel discussion entitled Privacy Exposed. Trust and Transparency is the theme for Privacy Week in New Zealand and trust came through as the clear theme for this session.

New Zealand’s Privacy Commissioner John Edwards led the discussion with a presentation on some of the key risks facing local government agencies - CCTV, employee browsing and human error. Mr Edwards was careful to note that openness and transparency were key to getting privacy right and reminded the audience about the various resources his office had made available for that purpose.

Fiona Colman (Privacy Officer, Accident Compensation Corporation) followed with an illuminating summary of ACC’s privacy programme in response to its 2011 privacy breach. Echoing the theme, Fiona noted that ACC’s significant efforts to improve (which have moved the organisation well up the privacy maturity scale) had resulted in heightened trust in the organisation.

Daimhin Warner (Director of Simply Privacy) completed the panel, with an update on the current privacy environment - including New Zealand law reform and the impact of the upcoming GDPR - and a suggestion that Auckland Council should reframe the privacy brand to get better traction. Daimhin suggested that privacy should be viewed as an enabler and not a barrier, and that it should be viewed through the lens of... you guessed it, trust. The session was facilitated by the Council’s COO, Dean Kimpton. Marguerite Delbet, GM Democracy Services had time to ask panellists to state their one key message for the audience to take away (“privacy is about people”, “privacy is an enabler, not a barrier”), before Governance Director, Phil Wilson closed the session with a strong call to action. All were clear to note that privacy mattered to them and to the organisation.

All in all, the session was a great example of Privacy Week’s purpose. Thanks especially to Mary Birch, Privacy Programme Manager, and her colleagues in the Democracy Services team for organising the event and having an enthusiastic approach to doing privacy right at the Council.

**Fiona Colman is Principal Advisor, Privacy Team at Accident Compensation Corporation**

**Daimhin Warner is the Director of Simply Privacy**
COUNTIES MANUKAU HEALTH PRIVACY WEEK
PRIVACY – IT’S ABOUT PEOPLE!
Kerry Bakkerus

ABOUT US:
Counties Manukau Health (CM Health) provides health and disability services to an estimated 570,000 people who reside in the local authorities of Auckland, Waikato and Hauraki District. CM Health looks after 11% of the total New Zealand population with a workforce of around 7,000 staff. Our workforce includes 48% nurses, 8% medical, 20% allied health and 7% of care and support workers. Our vibrant multicultural community attracts new immigrants - we have over 100 spoken languages. Counties Manukau Health is one of the largest employers within the Counties Manukau region.

CM Health has one of the busiest emergency departments with 110,000 patients receiving emergency care annually. It is one of the largest providers of paediatric and adult primary, secondary and tertiary health care in Australasia. We provide a full range of primary, secondary and tertiary care services, and we are known for investing and growing community and primary care services that integrate and connect with secondary and tertiary care. CM Health is internationally renowned for orthopaedics, burns and spinal injury rehabilitation. We also provide other specialist services such as neonatal intensive care, renal dialysis, plastics, reconstructive and maxillofacial surgery together with general surgery, medicine, acute care, paediatric, emergency care and mental health.

OUR PRIVACY WEEK:
As with all health sector organisations, privacy plays an important role in providing care. Trust is an integral part of why patients share their personal information with us – and if they don’t, clinical outcomes could be dire. Our privacy journey includes raising awareness within the organisation that staff information is just as important as that of our patients. With this in mind, Privacy Week was a great opportunity to remind our staff that we need to be mindful and respecting of personal information entrusted to us.

When thinking about how we effectively communicate and raise awareness about privacy and our obligations, we took a multi-channel and multi-pronged approach during privacy week. This year we have followed the Government Chief Privacy Officer’s theme where the concept was to have ‘real people’ from public sector agencies provide their thoughts regarding privacy. To make this more relevant for CM Health, we asked a number of staff to provide their thoughts on privacy and developed posters to support this. We had a number of posters, including one from a nurse, staff member from human resources and an allied health worker. We used these posters within the hospital on our notice boards but also on our Facebook page. Hear what our Charge Nurse had to say. We had a great hit rate with our social media campaign with this particular post reaching 5,109 people. This would predominantly be staff but includes our patients too.

Privacy related communication was also included in our internal newsletter for staff - the ‘Daily Dose’, which included a message from the Acting Chief Executive Officer, specific privacy messages and a privacy quiz with prizes. We have recently updated our Privacy intranet site – the quiz required respondents to get the answers from the new intranet site, tripling the number of page views. We included a ‘twist’ within our privacy quiz which required the respondent to include their driver’s licence ID as part of their details. Individuals who questioned whether this was relevant were included in a separate draw for another prize. It was interesting to see how many individuals included this information without questioning. A guest speaker, Samantha Finch presented to our Privacy Committee on the findings of her thesis titled ‘Expectations and Trust Crucial in Information Sharing for Primary Care Patients’. We included an extract of her thesis in our E-Update Newsletter distributed to General Practitioners in our area. Our most significant activity for privacy week was the updating of our Patient Information Brochure. This is used to communicate our privacy responsibilities to our patients – why we collect their information, what we do with it and how we protect it. A total of 5,000 copies have been printed and distributed across the organisation. Improving privacy maturity is about ensuring that all staff have a consistent understanding of their obligations. It is a journey, with constant communication, raising awareness and training initiatives required. Privacy Week is only the start.

Kerry Bakkerus, Risk & Privacy Manager, Counties Manukau Health
“Our patients and colleagues trust us with their personal information. I take that very seriously.”

SIUPOLU TAVUI
CHARGE NURSE

Privacy Week 2017
IT’S ABOUT PEOPLE
JUST BECAUSE YOU CAN DISCLOSE DOESN’T MEAN YOU SHOULD
Anna Johnston

Let’s talk about discretion and trust. And perhaps also the public interest.

These are not the usual words I would use when introducing a discussion of the Disclosure principles in privacy law, but right now they seem apt. Because right now I am hopping mad about the disclosure by our government of one woman’s personal information to the media.

The matter I am talking about involves a single mother, but at a deeper level it involves all of us. We are all citizens, we are all “clients” of government agencies at various times throughout our lives, and we all entrust our personal information to those government agencies. We expect that our privacy will be respected in return. This is the story of what happens when it isn’t. This is the story of Andie Fox, but it could just as easily be the story of you or me.

So the story is this: About a month ago, single mum Andie Fox wrote an opinion piece about her experiences dealing with Centrelink, which was published in Fairfax newspapers. A few weeks later, a journalist with the Canberra Times, Paul Malone, wrote an article about Centrelink, also published in Fairfax newspapers. That article included details about Ms Fox’s criticisms of Centrelink, but then also says “there are at least two sides to every story”, and in particular that “Centrelink has a different story”. Mr Malone’s article went on to reveal details about Ms Fox’s financial affairs and personal affairs, as well as quotes from Centrelink general manager Hank Jorgen about Centrelink’s dealings with Ms Fox.

(Just who gave Ms Fox’s information to the journalist is unclear. The article attributes comments to Mr Jorgen, but officials claimed the information was collated by DHS officials and approved for release by the Minister’s office. Later it was revealed that two responses were given to the journalist, one from the department and the other from the Minister’s office.)

The personal information about Ms Fox disclosed to the journalist, and revealed by the journalist to the world, included:

“The agency says Ms Fox’s debt is a Family Tax Benefit (FTB) debt for the 2011-12 financial year which arose after she received more FTB than she was entitled to because she underestimated her family income for that year.

The original debt was raised because she and her ex-partner did not lodge a tax return or confirm their income information for 2011-12.

Centrelink says that after Ms Fox notified the department that she had separated from her partner, the debt due to her partner’s non-lodgement was cancelled.”

and

“Centrelink made numerous attempts to get in touch with Ms Fox via phone and letter but many of these attempts were left unanswered. Between November 16 and January 17 Centrelink made four phone calls and sent six letters to Ms Fox.

Centrelink says it was not until 2015 that she informed them that she had separated from her partner in 2013.

Mr Jorgen said the experience described by Ms Fox could have been avoided if she had informed the department she had separated from her partner in a timely way, and if she had lodged her tax returns in a timely way.”

Wow. So much for privacy.

How exactly does a government agency get away with disclosing this kind of deeply intimate information about a person’s relationship history, tax affairs and social security benefits?

Let’s break it down.

Australian Privacy Principle (APP) 6 governs the disclosure of personal information by federal government agencies like Centrelink and the Tax Office. There are various grounds under which personal information can be disclosed, but let’s skip straight to the grounds that might possibly be relevant in this case. (BTW we have “untangled” the Disclosure rules for you under NSW privacy legislation, but haven’t yet tackled the APPs.)

1. **Consent (APP 6.1(a))**
   Clearly not. Ms Fox wrote a follow-up blog detailing the “disturbing experience” of having her personal information distributed to the media, and asked “Is this what happens when you criticise government?” I think we can safely say that Ms Fox did not authorise the release herself.

2. **Individual should reasonably expect the disclosure for a secondary purpose which is related to the primary purpose for which it was collected (APP 6.2(a))**
   OK, this one is trickier. Let’s say that the primary purpose for which Ms Fox’s personal information was collected was to administer her social security payments. Is providing that information to a journalist a purpose that is somehow related to the administration of her payments? Debatable. Even if it is related, is the disclosure to the journalist something Ms Fox should have reasonably expected?
The guidelines from the OAIC on APP 6.2(a) actually have this to say on the topic:

“Examples of where an individual may reasonably expect their personal information to be used or disclosed for a secondary purpose include where ... the individual makes adverse comments in the media about the way an APP entity has treated them. In these circumstances, it may be reasonable to expect that the entity may respond publicly to these comments in a way that reveals personal information specifically relevant to the issues that the individual has raised”.

And in 2010 the OAIC handled a privacy complaint from someone in a similar position to Ms Fox, and found that the agency had met this test (albeit under an earlier version of the privacy principles). The Privacy Commissioner in that case noted that:

“The information provided by the agency was confined to responding to the issues raised publicly by the complainant. The Commissioner considered that the complainant was reasonably likely to have been aware that the agency may respond, in the way it did, to the issues raised.”

First, I would query whether in this case, the information provided to the journalist was “confined to responding to the issues raised publicly by the complainant”. Most of Ms Fox's original piece was about the bureaucratic nightmare of dealing with Centrelink processes: queues, being on hold on the phone, being pushed to use an online system which didn't cater for her circumstances. These experiences were not refuted by Centrelink.

Ms Fox had also written about the phenomenon known as sexually transmitted debt in the context of our tax and social security system, in which a legitimate payment of the Family Tax Benefit to one parent can later be described as an over-payment and thus a ‘debt’ because the other parent simply has not yet lodged their own tax return for the relevant financial year – something over which you might have little control at the best of times, but which can become impossible if the relationship has since broken down. Her original piece was about the traumatic experience of having to prove to the government that her relationship with the other parent had ended, before she could demonstrate that the 'debt' should be cancelled. Again, Ms Fox's description of the way in which our tax and social security system operates (in particular, to the detriment of newly-single parents) was not refuted.

Instead, we got finger-wagging editorialising about how Ms Fox should have updated her records in a more timely way, and how often Centrelink had tried to contact her. The inferences to be drawn from those comments – perhaps, that Ms Fox is disorganised or disengaged and thus has herself to blame for the 'debt' being raised – are in turn disputed by Ms Fox in her follow-up blog. And in any case, they are hardly examples of correcting 'false statements', as the Minister later suggested had been made by Ms Fox.

But even if the information provided to the journalist had been a more direct correcting-an-error-of-fact, should Ms Fox have 'reasonably expected' Centrelink to brief a journalist in response to her opinion piece? Judging from the outcry on social media and across politics, it would seem that plenty of people did not expect a Centrelink customer's personal information to be splashed about in the way experienced by Ms Fox. (Apart from anything else: don't they have anything better to do?)

Despite the OAIC's guidelines on interpreting this exemption, I think Centrelink would be drawing an extremely long bow to argue that their disclosure was either a related purpose or within reasonable expectations, let alone both.

Authorised by another law (APP 6.2(b))

Now here is where it gets interesting – this is what Centrelink and the Minister are publicly using to justify the disclosure. Though which law has been harder to pin down.

On 28 February, Minister Alan Tudge told Parliament that “We are able under the Social Services Act (sic) to release information about the person for the purposes of, as I quote, ‘correcting a mistake of fact, a misleading perception or impression or a misleading statement in relation to a welfare recipient’.” However the Minister was quoting not from the Act itself, but from cl.11 of statutory guidelines which constrain the power of the Secretary of the Department of Human Services, of which Centrelink is a part, to disclose personal information under section 208 of the Social Security (Administration) Act 1999. In such a case, a public interest certificate must first be issued by the Secretary. The Department later confirmed that no such public interest certificate had been issued in relation to Ms Fox's personal information.

Instead, the Department claimed that the disclosure was actually made under section 202 of the same Act, which governs the routine collection, use and disclosure of personal information. Because it is about routine matters necessary “for the purposes of the social security law”, disclosures made under s.202 do not require the Secretary's authorisation. This is a standard, operational provision, about the normal functioning of Centrelink, and what the 35,000 staff employed by the Department can and can't do with our personal information as they go about their work.

So the Department has effectively claimed that its disclosure of Ms Fox's details to a journalist was lawful on the basis that the disclosure was made “for the purposes of the social security law”. What purpose of social security law was being served by the disclosure to the journalist? A Departmental spokesman is quoted as saying:

“Unfounded allegations unnecessarily undermine confidence and takes staff effort away from dealing with other claims”.

The Department doubled-down on this rationale a few days later, with the Secretary of the Department Kathryn Campbell telling an Estimates committee in Parliament that the disclosure of personal information about clients to the media does not even need a public interest certificate from the Secretary under s.208, if it is released under s.202 “for the purposes of maintaining the integrity of the system”.

PRIVACY UNBOUND | ISSUE 78
Ms Campbell is also quoted as saying: “That’s why we felt that it was appropriate to release the information, so that people knew it was important to file their tax returns and tell us about changes in their circumstances.”

Just let that sink in for a moment…. so the Secretary of the Department is saying that Ms Fox was made an example of, to remind the rest of us to lodge our tax returns on time?

One journalist summarised the problem thus: “Campbell ... described an interpretation of social security law so broad that it effectively adds up to a license for the Department to disclose information against any citizen criticising government policy”.

In fact, if you interpret s.202 that broadly, there is very little limit to what federal public servants could start doing with your or my personal information, regardless of whether we have publicly criticised Centrelink.

Next time it might not be the PR unit releasing the personal information; it might be a limelight-seeking junior Centrelink staffer who decides to tweet about named ‘welfare cheats’ – for the purposes of maintaining the integrity of the system, of course. Or a staffer might decide to tell the media about a celebrity who was late filing their tax returns - as a way of reminding the public about the importance of filing their tax returns on time, clearly. Or perhaps a staffer could get away with telling a mate who pays child support that his ex-wife has a higher income than his mate suspects – “for the purposes of maintaining the integrity of the system”, obviously.

However this interpretation of s.202 is being questioned. Legal academic Darren O’Donovan has questioned whether the Department has read its ‘discretion’ too broadly, as has Legal Aid Victoria. In particular, since s.208 creates a specific mechanism for disclosures of personal information to ‘correct the record’, but which requires a public interest certificate to be issued by the Secretary in compliance with statutory guidelines, can s.202 really be read as also allowing an alternative pathway to disclosure, one which is predicated on broader, vague purposes and which does not require the Secretary’s authorisation at all?

(And even if you believe s.202 is that broad, surely it cannot authorise the disclosure of personal information that was released by the Minister’s office in error?)

So if the Department’s interpretation of the breadth of s.202 is wrong, what then? Well then, a disclosure of information that was not authorised or required by or under the social security law is a crime, punishable by up to two years’ imprisonment for the individual who made the disclosure.

Also, Centrelink would not be able to claim the ‘any other law’ exemption under APP 6.2(b), and therefore could be looking at a possible breach of the APPs. Labor has asked federal police to investigate, and the OAIC is looking into the matter. The OAIC can apply to court for a civil penalty order up to $1.7M, and Ms Fox could seek a remedy for herself, if it is found that there has been a breach of APP 6.

Of course, it is not just legal concerns which have been raised about the department’s decision to publicly respond to Ms Fox’s opinion piece by releasing her personal information. There are plenty who have questioned the ethics of the decision, even if it is found to be lawful. Some have raised the potential chilling effect on free speech and political discourse, while others have noted the power imbalance between a single parent blogger and the might of the government. Where was the concern for Ms Fox’s well-being? Where was the discretion? Did no-one think this might be a bad idea, to go pick a fight with a single mum? Did no-one say: just because we (think we) can disclose, doesn’t mean we should.

I spoke with ABC Radio’s Jon Faine about this case, and described Centrelink’s actions as legally arguable, but morally reprehensible. Paul Shetler, former head of Australia’s Digital Transformation Office, described Centrelink’s actions as “pretty shocking”. And that was before it was revealed that the Minister had asked for extra information about Ms Fox … or that the Minister’s office had sent ‘For Official Use Only’ material to the Canberra Times journalist … or that the Minister’s office is regularly receiving updates on Centrelink clients who have made public complaints on social media.

This case just compounds the effect of #censusfail and #notmydebt on a cynical and weary public. We are so often compelled, either by law or by financial need, to hand over details about our private life to government. In return, we expect government agencies to actually mean it when they say “we take your privacy seriously”. Otherwise, that phrase becomes a joke, up there with “your cheque is in the mail”, and “your call is important to us”.

The way the bureaucracy has dealt with Ms Fox has shown to be hollow the privacy promises made by Centrelink. Worse, it also undermines the privacy promises made by other agencies which share personal information with Centrelink, such as the Tax Office. The ATO has confirmed that once tax information about an individual is provided to Centrelink, that data becomes subject to Centrelink’s secrecy laws, rather than the rules found under the taxation legislation. And it is Centrelink’s interpretation of its own ‘secrecy’ provisions which has led us here today.

This case is a stupid and petty own-goal for the government. If Centrelink or the Minister’s office were trying to disprove the accusations of “unprofessionalism and callousness in the way it has tried to crack down on welfare overpayments”, they have spectacularly failed. Maybe they wanted to challenge Ms Fox’s description of feeling ‘terrorised’ by her dealings with the bureaucracy, but instead they simply proved her point.
If the purpose of the disclosure was to maintain confidence in the welfare system, they instead caused confidence to plummet. If the idea was to paint Ms Fox as a ‘welfare cheat’, they instead earned her the sympathy of every other working parent who has ever tried to navigate their way through Centrelink to claim FTB or the child-care rebate.

I believe this will rebound not just on Centrelink, but throughout the federal public sector. The long-term impact will be to set back the government’s bigger picture digital transformation agenda, including e-health, digital identity and electronic voting projects, because public trust in how federal government institutions treat citizens’ personal information will simply continue to sink, unless trust is restored.

The repercussions have already included Labor re-thinking its support for veterans’ affairs legislation before Parliament, that would insert a similar provision to s.208, to allow for the disclosure of a veteran’s records, including medical records, at the discretion of the Secretary. The Veterans Affairs Minister has since had to order a new, independent Privacy Impact Assessment be conducted before the Bill proceeds to debate in the Senate.

Meanwhile, evidence before a Senate Inquiry has heard that the Tax Office has raised concerns about the impact on the integrity of the ATO, when tax data is used by Centrelink. Just imagine the fight in Parliament next time privacy-invasive laws are proposed.

The UK Information Commissioner’s office has noted that citizen and customer trust is essential for the efficacy of public policy and services: “trust and public engagement is a prerequisite for government systems to work”. The Harvard Business Review has described customer trust as “the key that will unlock” access to data, so critical in the type of forward-thinking information economy our Prime Minister likes to promote. So when government says “trust us with your personal information”, they have to mean it. Because we are all Andie Fox.

Anna Johnston, Director, Salinger Privacy
Editor’s introduction:

The next article has been written by Stephen Wilson about Blockchain. Blockchain, particularly since the rise of Bitcoin, has the potential to move into mainstream businesses such as financial services and capital markets. Given this, Privacy and Security Officers need to consider the tensions that this new technology creates:

- contrary to the data deletion or destruction privacy principle, blockchain data is never actually removed, it is always added to;
- whilst blockchain supports the transparency principle in order to validate a payment through a serious of protocols, these transactions cannot be considered as private or confidential; and
- there is a current move towards building blockchain with a larger focus on privacy and confidentiality, however, there are trade-offs that come with that. Mainly the loss of transparency, which was the major feature of the first blockchain, Bitcoin.

The blockchain space will be pathed with many privacy and security tensions and concerns, but it will be a fascinating road to be on.

Blockchain is an algorithm and distributed data structure designed to manage electronic cash without any central administrator. The original blockchain was invented in 2008 by the pseudonymous Satoshi Nakamoto to support Bitcoin, the first large-scale peer-to-peer crypto-currency, completely free of government and institutions.

Blockchain is a Distributed Ledger Technology (DLT). Most DLTs have emerged in Bitcoin’s wake. Some seek to improve blockchain’s efficiency, speed or throughput, others address different use cases, such as more complex financial services, identity management, and “Smart Contracts”.

The central problem in electronic cash is Double Spend. If electronic money is just data, nothing physically stops a currency holder trying to spend it twice. It was long thought that a digital reserve was needed to oversee and catch double-sends, but Nakamoto rejected all financial regulation, and designed an electronic cash without any umpire.

The Bitcoin (BTC) blockchain crowd-sources the oversight. Each and every attempted spend is broadcast to a community, which in effect votes on the order in which transactions occur. Once a majority agrees all transactions seen in the recent past are unique, they are cryptographically sealed into a block. A chain thereby grows, each new block linked to the previously accepted history, preserving every spend ever made.

A Bitcoin balance is managed with an electronic wallet which protects the account holder’s private key. Blockchain uses conventional public key cryptography to digitally sign each transaction with the sender’s private key and direct it to a recipient’s public key. The only way to move Bitcoin is via the private key: lose or destroy your wallet, and your balance will remain frozen in the ledger, never to be spent again.

The blockchain’s network of thousands of nodes is needed to reach consensus on the order of ledger entries, free of bias, and resistant to attack. The order of entries is the only thing agreed upon by the blockchain protocol, for that is enough to rule out double spends.

The integrity of the blockchain requires a great many participants (and consequentially the notorious power consumption). One of the cleverest parts of the BTC blockchain is its incentive for participating in the expensive consensus-building process. Every time a new block is accepted, the system randomly rewards one participant with a bounty (currently 12.5 BTC). This is how new Bitcoins are minted or “mined”.

Blockchain has security qualities geared towards incorruptible cryptocurrency. The ledger is immutable so long as a majority of nodes remain independent, for a fraudster would require infeasible computing power to forge a block and recalculate the chain to be consistent. With so many nodes calculating each new block, redundant copies of the settled chain are always globally available.

Contrary to popular belief, blockchain is not a general purpose database or “trust machine”. It only reaches consensus about one specific technicality – the order of entries in the ledger – and it requires a massive distributed network to do so only because its designer-operators choose to reject central administration. For regular business systems, blockchain’s consensus is of questionable benefit.

Stephen Wilson is Managing Director and Principal Consultant at the Lockstep Group and can be contacted at swilson@lockstep.com.au
The IAPP Global Privacy Summit was held in Washington DC on 19 and 20 April 2017. With almost 3500 attendees at the Summit, this year’s event didn’t disappoint on delivering informative data privacy thought leadership from both industry privacy leaders as well as representatives of the data protection regulators. The Summit also provided privacy professionals from all around the world the opportunity to come together to network, exchange ideas and learn from shared experiences. While it would be impossible for me to cover everything which occurred at the Summit within a single Privacy Unbound article, here are a few of my observations and key takeaways from the sessions I attended:

1. GDPR READINESS IS AN IMPORTANT ISSUE

With over 30% of attendees at the Summit coming from Europe, and a schedule jam-packed with sessions and workshops about the new General Data Protection Regulation[1] (GDPR), it’s clear that global readiness for and awareness of the GDPR is a big issue for global organisations. The GDPR covers organisations which are located within the EU, as well as those located outside of the EU that provide goods or services to EU residents or monitor their behaviour[2]. The GDPR will bring about a number of new key compliance obligations for organisations, including: (i) stricter conditions for data controllers relying on data subjects’ consent as the legal basis for processing; (ii) the right to data portability; (iii) rights of objection around the profiling of data subjects; (iv) requirements for implementation of data protection by design and by default; (v) the appointment of Data Protection Officers; and (vi) data breach reporting requirements. It’s not all bad news for organisations though. While GDPR compliance carries with it risks, costs and burdens, it’s also expected to create valuable opportunities for organisations where data privacy is appropriately linked to their business and data strategy. One key takeaway from the GDPR sessions I attended was that the role of the data privacy officer within an organisation will also grow to become more strategic, senior and multi-skilled as a result of the implementation of the GDPR.

2. IT’S TIME TO RE-THINK HOW YOU CARRY-OUT PRIVACY IMPACT ASSESSMENTS

While on the topic of the GDPR, it’s important to note that Article 35 introduces the requirement for Data Protection Impact Assessments (“DPIAs”), which need to be undertaken whenever data processing by a data controller is “likely to result in a high risk to the rights and freedoms of natural persons”[3]. At two Summit sessions I attended on this topic, the panellists provided valuable insights as to how privacy practitioners can effectively and efficiently carry out DPIAs, including by taking steps to map the numerous systems/applications and processing activities within their organisation (including in particular those within their HR, training and marketing functions); consult with the necessary business stakeholders and populate the necessary information within this map using data discovery techniques or by data privacy questionnaires, and continuing to keep the data mapping up-to-date going forward. The general view of the panellists was that the stricter obligations of the GDPR will require organisations to have a more formalised DPIA process. From a practical perspective, it will no longer be possible for organisations to undertake their DPIAs manually using Excel schedules and/or Word templates (as many do today). An automated method of conducting DPIAs will be required and necessary going forward. On the upside, the automation of the DPIA process is expected to lead to greater efficiencies and in turn, better privacy compliance within an organisation. A handy takeaway from these sessions is that the IAPP offers its members two free applications which can be used to conduct DPIAs within their organisations, these can be accessed from the IAPP’s website.

3. GETTING YOUR COMPANY’S PRIVACY STATEMENTS CORRECT IS NO SIMPLE TASK

An informative practical workshop at the Summit on Privacy Statement Creation provided attendees with some helpful tips and best practices for drafting effective privacy statements. While preparing a privacy statement may be considered a basic task for a privacy officer, the workshop demonstrated that there can be many traps involved for the “inexperienced player” in this field. Some of the key takeaways from the workshop were that privacy statements are a disclosure of your organisation’s privacy practices, they are not a legal contract and accordingly should not be incorporated into any legal “terms of use” or other “general terms and conditions” issued by your organisation. Also, when preparing a privacy statement for your organisation, it’s important to consider the different audiences who will be reading them, and the different perspectives they will have on them. The various audiences include: (i) your customers, vendors and employees, whose personal information you are processing; (ii) data protection regulators; and (iii) journalists who may be reporting about a data breach.
The workshop panel highlighted that privacy statements need to have a proper balance of both formal and informal content, to meet the differing expectations of these parties. While they may be drafted by lawyers to make sure they contain the appropriate legal and regulatory required content, it's important to make sure they are also reviewed by your organisation's communications, marketing and/or business operations teams so that they are accessible and understandable to the audience.

4. LET'S NOT FORGET ABOUT ASIAPAC!

A number of Peer-to-Peer Roundtables held over the course of the Summit provided attendees a great opportunity to select a specific topic of interest to them and connect with fellow privacy professionals over a smaller and more interactive group discussion. For my part, I attended a topical group discussion which was chaired by Alec Christie, a Partner in the Digital Law team of EY Australia, covering data transfers and hot privacy issues in Asia Pacific. Some current developments in the AsiaPac region which were discussed by the group included: (i) general readiness for Australia's new mandatory data breach notification law, which will come into effect in early 2018; and (ii) the compliance requirements imposed upon organisations under China's new Cyber Security Law, which were due to come into effect on 1 June 2017, but have now been deferred until late 2018.

5. CONGRATULATIONS TO BRENDON LYNCH

Proving that our region produces exceptional globally recognised privacy leaders, New Zealander Brendon Lynch, the CPO of Microsoft and long-time active supporter and member of IAPP, was awarded the IAPP Vanguard Award at the Summit. The Vanguard Award is awarded to pioneers and innovators in the field of privacy and recognizes privacy professionals "who show exceptional leadership, knowledge and creativity in the field of privacy and data protection, whether through spearheading projects or programs that positively impact the profession or through achievements over the course of an entire tenure or career."

CONCLUSION

The 2017 Summit certainly delivered on its objectives to provide attendees with innovative perspectives and to offer a whole new take on working in privacy and data protection. I would encourage all members of iappANZ to make the journey to the IAPP Global Privacy Summit in the US at least once during their professional career, to experience data privacy thought leadership delivered in a truly global forum. For those who prefer however something a little closer to home, IAPP's Asia Privacy Forum 2017 will be held in Singapore on 24 and 25 July 2017. Its programme contains an interesting schedule of topics which will be delivered by privacy experts from both Asia and beyond (which you can read more about HERE. The preparations for our own iappANZ Privacy Summit to be held in Sydney later this year are also well underway. It promises to advance data privacy knowledge and education through informative content delivered by experts in the profession. I'll look forward to seeing you there!

Christopher Rogers is Senior Global Legal Counsel, Office of the General Counsel (GCO), EY and an iappANZ Director

[2] GDPR Article 3(2)
[3] GDPR, Article 35(1) A
NEW ZEALAND

The Domestic Violence – Victim’s Protection Bill 2016 is a Member’s Bill (Green MP Jan Logie), amending the Domestic Violence Act 1995, Employment Relations Act 2000, Health and Safety at Work Act 2015, Holidays Act 2003, and Human Rights Act 1993 aiming to enhance legal protections for victims of domestic violence. The Bill introduces a new definition “domestic violence document”. It is unclear the level of detail that is required for the reports comprising the “document” and this may raise significant privacy issues for the victim, and others (for example the alleged perpetrator). Submissions are closed and the Select Committee is due to report on 8 September 2017. The Government also has a bill on domestic violence before the House – the Family and Whanau Violence Legislation Bill (mentioned in the last edition).

The Anti-Money and Countering Finance of Terrorism Amendment Bill 2017 amends the Anti-Money and Countering Finance of Terrorism Act 2009. The Bill extends the core obligations of the Act to real estate agents, lawyers, accountants, conveyancers, the New Zealand Racing Board and some high-value dealers. This Bill introduces new and expanded powers for agencies to share personal information. Submissions are closed and the Select Committee is due to report by 24 July 2017.

The Ministry of Business, Innovation and Employment has issued a Discussion Paper Consultation On Whether to Introduce A Director Identification Number. The insolvency Working Group in 2016 recommended introducing a unique identification number for directors of companies. MBIE seeks submissions on the issues a director identification number would address and the benefits and costs of a director identification number, including the privacy issues arising. Submission close 23 June 2017.

Other Bills currently before the House (further details provided in last edition) include the Customs and Excise Bill, the Children, Young Persons and Their Families (Oranga Tamariki) Bill, the Enhancing Identity Verification and Border Processes Legislation Bill, the Family and Whanau Violence Legislation Bill.

The Law Commission and the Ministry of Justice are conducting a review of the Search and Surveillance Act 2012.

AUSTRALIA

As part of the Victorian Government IT strategy 2016-2020, the Freedom of Information (FOI) Amendment (Office of the Victorian Information Commissioner) Bill 2016 (Vic) has been passed by both houses of parliament in Victoria. The bill will amend the Freedom of Information Act 1982 and Privacy and Data Protection Act 2016 to:

- abolish the FOI Commissioner and Privacy and Data Protection Commissioner;
- establish the Office of the Victorian Information Commissioner; and
- appoint an Information Commissioner and confer on them functions under both Acts; and
- appoint a Deputy Public Access Commissioner and Privacy and Data Protection Commissioner.

The new Information Commissioner which will therefore have under a single administrative structure, overall responsibility for FOI, privacy and data protection in Victoria and other powers of oversight. This follows changes earlier this year made by the Health Complaints Act 2016 which replaced the Health Services Commissioner with the Health Complaints Commissioner responsible for health services, including complaints in relation to the management of health records. These changes will significantly impact on the governance of privacy and data protection.
News about employment opportunities is provided as a service to iappANZ members. If you would like a notice about employment opportunities at your organisation published in Privacy Unbound, please contact opsmanager@iappanz.org

No current listings.
IAPP CERTIFICATION

Our global body, the International Association of Privacy Professionals (iapp) says this about privacy certifications:

‘In the rapidly evolving field of privacy and data protection, certification demonstrates a comprehensive knowledge of privacy principles and practices and is a must for professionals entering and practicing in the field of privacy. Achieving an IAPP credential validates your expertise and distinguishes you from others in the field.’

What certifications are currently available in Australia/New Zealand?

Currently, the iapp offers Certified Information Privacy Professional (CIPP) certifications for the following regions:

- Canada (CIPP/C)
- Europe (CIPP/E)
- U.S. Government (CIPP/G)
- U.S. private-sector (CIPP/US)
- Asia (CIPP/A)

In addition, there are globally-focussed certifications which may be of more relevance to iappANZ members:

- Certified Information Privacy Manager (CIPM)
- Certified Information Privacy Technologist (CIPT)

The iapp manages certification registrations and provides online training and other learning materials, and you can set an appointment to sit your exam online at a testing centre in Australia or New Zealand.

More information about the certifications and the iapp fees is available on the iapp website - https://iapp.org/certify/programs/

What about a certification for Australia and New Zealand?

A new CIPP/ANZ certification is currently in development. The iapp is currently working with an advisory board (drawn from iappANZ members) to develop the content for the certification. Stay tuned for further updates!
The iappANZ Writing Prize is open to an article that is published in Privacy Unbound during the 2017 calendar year (up to and including the pre-Summit edition of Privacy Unbound). You can enter by writing and submitting an article that tells us something interesting, new and relevant about privacy. The preferred length for articles is 500-1500 words.

All articles must be submitted by email, preferably in Word, to opsmanager@iappanz.org. We will need the author’s email address and contact number. You can submit as many articles as you like.

The winner will be announced at our Annual Privacy Summit and their name and details (with an author profile) will be published in Privacy Unbound.

Additional details:

§ Our Journal Advisory Committee, plus up to two iappANZ board representatives will decide on the winner whose article they judge to be the most interesting, original and relevant to our members.

§ Some people won’t be eligible for the prize (sorry!). They are: iappANZ board members, Journal Advisory Committee members, our contractors and employees and their family members.

§ There will be one prize with a value of A$250.

§ After the winner is announced we will notify them and arrange for the prize to be delivered to them if they are unlucky enough not to be at our Summit. We may need to verify the winner’s identity so we don’t give the prize to the wrong person.

§ If the prize is not claimed for any reason (and we hope this won’t happen) the author of the runner-up article will receive the prize.

To make sure things go smoothly and fairly (and we are sure they will) we just have to say that our decision in relation to any aspect of the award of the prize, including the content and publication of submitted articles, is final and binding and not up for discussion.