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 Liderwood
Kyle Lees
Marta Ganko
Katherine Gibson
Emma Kulinitisch

Please note that none of the content published in the Journal should not be taken as legal or any other professional advice.
Welcome to our latest edition of Privacy Unbound. With the evenings drawing in and more time inside, it’s the perfect opportunity to stop and indulge in the great range of articles we have for you from Australia and New Zealand.

Kathryn Dalziel reviews a recent High Court case in New Zealand that demonstrates that the Harmful Digital Communications Act 2014 is working and how the High Court has interpreted the meaning of serious emotional harm, with comparisons to the damage that the Privacy Act recognises can be caused by privacy breaches. Kyle Lees, our ‘local hipster’ and 2016 Journal writing prize winner, is back with his edgy and thought-provoking piece on what metadata really means.

With Privacy Awareness Week (PAW) in New Zealand and Australia just around the corner, The Office of the Privacy Commissioner in New Zealand and the OAIC give us a heads up as to what is on their agendas for PAW. We are also very excited to be hosting iCare’s David Lacey who will embark on a tour of five cities during PAW to discuss the personal side of data breaches. Book your tickets now if you have not already done so.

Katrine Evans’ article on the expanding definition of personal information is also timely as we reflect on the unprecedented developments in the information landscape and the ever-expanding amounts of data being collected. This is a challenge that the Australian Productivity Commission’s final report on data use and availability, due for imminent release, considers. We hope to bring you more about the report in our next edition.

Finally, we have a new Legislation Corner in the Journal for both New Zealand and Australia. It has been a busy time in New Zealand with the introduction of a range of legislation that addresses information sharing and privacy issues. Ilana Singer looks at the new South Australian Surveillance Devices Act 2016 that seeks to address regulatory gaps that exist in the patchwork of surveillance legislation in Australia and our own Board director Emma Hossack’s assessment of the Australian Bill that was rushed through to make re-identification of de-identified personal information an offence.

Remember that eligible articles will be entered for our 2017 writing prize and that we also have a job ad section in the Journal for any members or sponsors who wish to advertise jobs to our privacy professionals. You can contact Jess Abbey, our Operations Manager, for more information.

Finally, our new Advisory Committees for the Summit, Journal, iappANZ certification and Events have rolled up their sleeves and got down to business. We have an action-packed year still to come with more events following PAW and leading up to the Summit. In particular, we are very excited to be delivering in New Zealand a workshop run by Shona Rowan aimed at helping privacy professionals to deliver their message and raise privacy awareness across their organisations. It is proving very popular and tickets are still available.

As always, please feel free to contact myself, our President Kate or any of our board of directors if you have any questions or wish to get more involved in iappANZ. Enjoy the Journal.

Veronica Scott
Vice President
The Harmful Digital Communications Act 2015 is proving to be a workable piece of legislation in New Zealand which can provide victims of harmful digital communications with a quick and effective means of redress and hopefully will meet its stated object to deter, prevent and mitigate harm caused to individuals by digital communications.

A recent example of its application is New Zealand Police v B [2017] NZHC 526 in which the High Court upheld an appeal from the District Court by finding that the complainant’s former husband had caused her serious harm through posting on Facebook explicit pictures of parts of her body unclothed or covered just with a bra. When considering serious harm, the High Court referred to, amongst other things, significant humiliation, significant loss of dignity or significant injury to the feelings of the complainant under the Privacy Act.

The defendant was charged under s 22 of the Act which creates an offence for causing harm by posting a digital communication. The offence is committed when:

1. The defendant posts a digital communication with the intention it cause harm to a victim;
2. Posting that communication would cause harm to an ordinary reasonable person in the position of the victim; and
3. Posting that communication causes the victim harm.

Harm is defined in s4 of the Act as serious emotional distress.

The District Court accepted the first two elements above were proved but not the 3rd element. This was despite hearing the complainant’s friend describing the complainant as very shocked and very depressed: she was almost crying; and despite hearing the complainant say it caused a lot of emotion for her – she was upset for a long time, she was stressed, and the situation caused her frustration and anger. The complainant also said she was anxious and she felt medically unfit to go to work.

The High Court found there was no issue with the District Court Judge’s interpretation of the Act which demonstrates the workability of the Act. However, Justice Downs was concerned that the complainant’s unchallenged evidence of serious emotional harm had not been considered in the context of the entire case including the pictures themselves and that the defendant had threatened to post photographs of the complainant online if she did not stay away from other men and “cancel” a protection order which she held against him. The complainant said that threat made her feel scared and anxious.

Interestingly, in considering the meaning of serious emotional harm, Justice Downs highlighted material from the Law Commission’s paper on Harmful Digital Communications: The adequacy of the current sanctions and remedies (August 2012, Wellington) in which it was said that “[T]he Privacy Act requirement that an interference with privacy must cause damage including “significant humiliation, significant loss of dignity or significant injury to the feelings of the complainant” appears not to have been problematic.”

Justice Downs also made the following points about “serious emotional harm”:
Justice Downs also made the following points about "serious emotional harm":

The definition is exhaustive;
   a) The Act eschews minor emotional distress;
   b) The decision is part fact, part value-judgment;
   c) The Court needs to consider the nature of the emotional distress; its intensity; duration; manifestation; and context, including whether a reasonable person in the complainant’s position would have suffered serious emotional distress; and
   d) "serious emotional distress" is a broad compendious expression that means what it says.

The High Court’s decision in New Zealand Police v B demonstrates the Harmful Digital Communications Act does work in practice and that its concept of "serious emotional harm" is not a new or difficult area of law in reality. This has been a good result.

Kathryn Dalziel is a Partner at Taylor Shaw and can be contacted at kathryn@taylorshaw.co.nz

www.taylorshaw.co.nz
METADATA: A WORLD WITHIN A WORLD

KYLE LEES

What is metadata and why does it matter?

Any local hipster who has studied ancient Greek over the internet knows that Metadata means “data about data”. Although the “meta” prefix μετά translates from the original Greek as “after” or “beyond”, it is used to mean “about” in epistemology – essentially the theory or philosophy of knowledge. Metadata then is the data providing information about one or more aspects of the data itself; it is used to summarise basic information about data which can make tracking and working with specific data easier. Examples abound. Metadata can comprise a range of foundations from; the means of creation of the data; the purpose of the data; the time and date of creation; the creator or author of the data; location on a computer network where the data was created; standards used; file size; etcetera.

So why do minuita details about other details matter? Perhaps the answer harks back to immemorial questions of self and identity. The visceral trace of Kristeva, the formless follicles of Battailles, or even, lie unresolved in the disinterested gaze of Descartes. More fundamentally, and perhaps less philosophically, metadata reveals. It reveals inference, corollary, implication and can be used to ascertain detail – interpreted rightly or wrongly – about a wide range of relationships, interactions, locations, transactions – and perhaps most importantly and troublingly for the law – people.

What can Metadata tell us?

As ever, the best way to find out about something is to go and find out about it. As sure as this sentence smacks of irony, On 24 August 2015, the ABC published a year’s worth of reporter, Will Ockenden’s metadata in full and asked their audiences to analyse it.

As an exercise in understanding the power of metadata to draw inference, it was a powerful one. From this information – which Tony Abbott once described in December 2014 as “essentially the billing data”— the audience was able to accurately pick up on patterns in the journalists’ behaviour which served to reveal a plethora of precise details around: where he lives, where his parents live, where he works – and even how he gets to work on a particular day, whether that be by car, ferry or bus to Manly in Sydney’s North. Whilst communications content reveals the detail of a conversation or chat, metadata can be used to weave together patterns of communication and correlate these with the thread of actual events. It becomes the pieces of a mosaic with which to tessellate the whole.

Mr Ockenden described the experience as eerie and unsettling.

“Of course I was not surprised when the public’s analysis was at times scarcely accurate...

“They’ve trawled through everything very, very thoroughly. A year of my life has been given a very good going over. They picked up on the major trips, the work times, my habits and more.”

- Will

Image: ABC
Metadata as a tool of crime prevention or a method of surveillance?

As George Brandis, Attorney-General, has stated previously, metadata is the ‘basic building block’ of counter-terrorism, counter-espionage, and counter crime investigations. In the wake of the endorsement and implementation of data-retention legislation in Australia, the ABC’s investigative example of the practical application of the use of metadata to also reveal intimate details about people’s lives brings into relief an antediluvian question: Is it better to cast draconian laws which affect the whole of society to capture a few, or, is it better to advocate a rights based approach to ensure the protection of privacy and moreover enshrine freedom of expression and speech for all members of society?

In a country with a limited political freedom of speech and an absence of legislated safeguards around human rights (including privacy), it’s a question this writer can’t answer. Perhaps Orwell offers the best advice on the matter: “If you want to keep a secret, you must hide it from yourself”.

Kyle Lees writes in a personal capacity and as an iappANZ Member.

References:
2. Kristeva, Batailles, Descartes, Op cit. e: nor
4. https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/2
5. George Orwell, 1984, Penguin, USA (1977)
Privacy Week is around the corner and it’s always a hub of activity in New Zealand and Australia. This year, New Zealand’s Office of the Privacy Commissioner (OPC) is promoting the Privacy Week theme ‘Trust and transparency’. It is one of two themes adopted by the Asia Pacific Privacy Authorities (APPA) – the other theme APPA members are using is ‘Share with care’.

Building trust

‘Trust and transparency’ fitted for us because we have emphasised transparency as a foundation of trust between agencies and their clients.

Encouraging transparency has been a significant feature of our recent work, including our Transparency Project, (https://privacy.org.nz/news-and-publication/statements-media-releases/transparency-project-reveals-thousands-of-government-info-requests/), and more generally in the practical guidance we give agencies.

By letting customers know what personal information is disclosed, collected, how it is used and stored, and willingly giving people access to their own information, a business demonstrates a level of transparency that supports client trust. We’ll be using Privacy Week to promote these privacy rights and what agencies need to know about them.

Employment e-learning

Employment privacy is an area that affects everyone. We are looking forward to launching a new free e-learning module dedicated to employment. The employment module will add to our growing range of e-learning modules, including general modules on the Privacy Act, health privacy and credit reporting. We’re also hoping (fingers-crossed!) to have finished the development of our first e-learning ‘mini-module’ for Privacy 101, taking a practical focus.

Partnering for events

We’re keenly aware that partnering with stakeholders spreads the privacy message more effectively and we’ve been working with a number of other organisations in the lead up to Privacy Week 2017. We are very pleased to host the Data Futures Partnership, and Chair Dame Diane Robertson, who will release their findings in relation to long-term projects on re-identification, and empirical research on social licence. We’re working with InternetNZ to jointly host an event showcasing recent research on pre-teens’ use of social media and their concepts of privacy; and InternetNZ’s own private messaging campaign. Other PrivacyLive forums during Privacy Week include the Broadcasting Standards Authority presenting on recent privacy decisions and, to help launch the employment module, well-known employment lawyer, Susan Hornsby-Geluk, speaking on emerging employment and privacy issues. All these events will be streamed live on Periscope, and will be available later on our YouTube page.

Where we can, we are supporting Privacy Week events being held by other organisations. We will be working with Air New Zealand, Auckland Council and the credit reporting industry, and of course iappANZ itself - all of which are hosting Privacy Week events.
Resources

We’re taking the opportunity to launch a number of resources during Privacy Week. These include a poster series on privacy tips and one illustrating the life cycle of personal information. There will be a new privacy brochure, a privacy quiz for workplaces and a video message from the Privacy Commissioner. There can never be enough when it comes to Privacy Week but in the meantime, keep an eye on the Privacy Week page on our website for regular updates, or sign up to receive our fortnightly Privacy News.

/privacy-week/

https://privacy.org.nz/subscribe/
UPDATE FROM THE OAIC - 2017 PRIVACY AWARENESS WEEK IS ON IN MAY!

Australia’s largest privacy event, Privacy Awareness Week (PAW), returns this year between 15 and 19 May to prompt discussion about the importance of protecting personal information, and how to achieve this in the digital age. The OAIC will be holding various events, which you can find out more about on the recently launched PAW 2017 website. The highlight of the week will be the release of the 2017 Australian Community Attitudes to Privacy Survey (ACAPS) report — which provides an in-depth understanding of the Australian community’s privacy expectations.

Privacy issues will be explored through this year’s theme, ‘trust and transparency’. This theme speaks to the value of open, and clearly communicated privacy practices in fostering community trust in organisations and data-based projects. It also reflects a fundamental shift in how privacy is understood today. The idea of privacy-as-secrecy is increasingly incompatible with our experience and values. Various products and services now rely on personal information, and generally Australians are happy to provide their information when it is clear how it will be used, and the benefits of providing it. Privacy is therefore about transparency, and evidencing that privacy rights are being respected and protected.

The impact of this shift on Australians’ attitudes towards personal information handling will be revealed through the 2017 ACAPS report. The report is the latest in Australia’s longest-running privacy survey, which has been conducted periodically since 2001, and last occurred in 2013. The survey has provided a way of tracking the Australian community’s perspectives on privacy as digital technologies proliferated, and support for public data initiatives has grown. The Commissioner will unveil the ACAPS report at a launch event in Sydney during PAW, and discuss what lessons about community expectations can be drawn from the results for businesses and agencies. The OAIC is currently taking expressions of interest to attend the launch event and hear the regulator’s perspective on Australia’s privacy landscape and future trends.

The OAIC will also be releasing a new Privacy Impact Assessment (PIA) eLearning tool at PAW, which is designed to help organisations get privacy right from the start. The tool supports the implementation of a privacy-by-design strategy across an organisation, by outlining how to complete an assessment of a project to identify and address privacy risks before work begins. PAW provides an opportunity for all sectors of the Australian community to address perceived privacy risks, challenges, and solutions. As both government agencies and private sector businesses continue to explore the potentials of personal information in improving products and services, this opportunity is increasingly significant. For organisations, PAW is an opportunity to better understand how Australian’s expect their personal information to be managed. Meeting these expectations will be vital to the success of gaining consumer and community trust in data-based projects, products, and services.

For individuals, PAW is a reminder of the value of their personal information, and an opportunity to learn more about how their personal information is managed by the organisations they share it with. A subtheme of PAW this year is ‘handle with care’, to emphasise the importance of personal information, and being informed about where it is shared, and how it is used. We encourage organisations to show their support for good privacy practices by signing up as a PAW partner for 2017 via the website.
THE EXPANDING DEFINITION OF PERSONAL INFORMATION

KATRINE EVANS
Senior Associate, Hayman Lawyers

When it comes to defining personal information, I sometimes feel I’m singing Monty Python’s ‘Galaxy Song’ about how the universe keeps on expanding. Every way you turn, recent developments in our ability to create, combine and process information push the boundaries of what we previously understood personal information to be.

Fortunately for sanity, it’s usually pretty obvious whether something fits the bill. However, it has always been a topic with many (though maybe not 50) interesting shades of grey. It has also been the subject of some of my fiercest and most cheerful debates with colleagues over the years.

This article considers some recent trends and developments. It focuses on New Zealand law, but also draws on overseas examples. It acknowledges that we need to make sure the concept of personal information stays coherent, but also suggests that there is no need to panic. Often, we can adjust to the expanding universe more easily than we think.

Developments in the information landscape

While defining “personal information” has never been 100% straightforward, several relatively recent changes in the information landscape have created further complications. Those changes are forcing us to rethink what we thought we knew and making us consider how to craft our laws so they are coherent and don’t become unwieldy.

2. The explosion in information generation, where everything we touch, work with and have in our homes is creating and communicating information;

3. Our dramatically expanded ability to wrestle meaning – or at least assumptions – out of fragmented information, that in earlier years would have said nothing about individuals, if it was accessible at all.

It’s this increased ability to separate people out from the crowd and use information in ways that materially affect them that justifies including a widening variety of information in our privacy protection framework. Anything that affects our ability to carve out personal or bodily space, affects our ability to control information, or leads others to focus their attention on us can be a privacy matter.

However, it’s also important to recognise that the law still needs limits on what “personal information” is – that is, what it is prepared to regulate. As Paul Ohm says in “Broken Promises of Privacy”, expanding the definition too far makes it meaningless and unworkable.

This is a particular concern in jurisdictions where there are strict rules for how to handle personal information and stiff penalties for failing to comply. The tougher our privacy laws get, the clearer we’d usually like to be on what personal information means.
What the statute says

Statutory definitions of personal information vary between jurisdictions. Some are relatively closed, list-based definitions. Many are much more flexible and contextual. New Zealand’s Privacy Act 1993 is the latter.

There are four deceptively simple components to our definition. Personal information is:

- information
- about
- an identifiable
- individual

Information

"Information" is not separately defined, but our leading case says it is anything that "instructs, tells or makes aware".

The importance of the term is therefore not that it limits what "information" covers – it is that there is no limitation. "Information" goes beyond documents or particular formats. It includes information in a person’s memory and in conversations as well as tangible documents or electronic records. It is not restricted to sensitive information – the blandest, most public items are still "information".

The other elements of the definition create the limits. All three are needed before something is personal information. For instance, the contents of a file with someone’s name on are not necessarily all personal information. The information might be linkable to an individual and be retrievable by reference to them, but it might not all be "about" that individual.

Individual

First, and easiest, the information needs to relate to a living human being.

This is because only people have privacy rights. Corporations have a legal personality and have confidentiality or reputational interests, but privacy is a uniquely human right. So a man who uses his company’s bank account for his personal finances can’t complain about a breach of privacy when the bank sends a copy of the account transactions to his ex wife. Privacy law isn’t going to help because, legally, all the account information is about the company.

Also, restricting that right to living people acknowledges that while it is important to respect the dead – including to support those who survive them – they no longer have feelings, autonomy, or a need to transact in the world that can be damaged by how their information is handled.

Identifiable

People do not need to be identified by or within the information itself. They only need to be identifiable. There is no need for a name or a unique identifier to be attached. For instance it’s enough if:

- people who know you would recognise you
- the information can be retrieved by reference to you
- the information can identify you when combined with other information that the agency has or that is reasonably accessible from other sources.

So if an IP address is used to identify that an individual was in a particular place at a certain time and engaging in certain activities, the context means it’s personal information about that individual.

About

Finally, the information needs to be about that identifiable individual. That is, it needs to be genuinely linked to, and say something relating to that person. This is the hardest element. When is information that is ostensibly about a thing capable of being information about a person?

It tends to depend on the way in which you phrase the question. Take the case of Apostolakis v Siewwrights. Mrs Apostolakis’ lawyer wrote to the mortgagee of her property to say that the building’s insurance either had lapsed or was about to lapse.

Was this information about the building (“this building is uninsured”) or about her (“Mrs Apostolakis has not insured her building”)? The Tribunal, and later the High Court, said that it was clearly the latter. The information was about her responsibilities in relation to the property.

So it is a case of assessing the context, the emphasis and the potential impact on a person. How strong is the link with the individual? Is any mention of their name purely incidental or are you being told something about them, their activities, circumstances, rights or responsibilities?

Other examples include:

- Geotechnical information about earthquake damaged land can be highly relevant to the status of an insurance claim, and therefore say something important about the insured party’s rights and responsibilities.
- Dogs do not have privacy rights, even when alive and kicking, but if a subject access request to the vet is actually about the owner’s obligation to pay the bill then some information might fall into the "personal information" category.
The upshot is that personal information is inherently contextual, which can be frustrating for those seeking a brighter line.

**Recent cases reflect the difficulties**

It’s probably not surprising, then, that recent opinions of judges and regulators have taken such different approaches to what personal information is, even in jurisdictions that you’d expect to be similar.

At one end of the scale is *Vidal Hall v Google*. The claimants argued that Google collected personal information about them through a cookie that captured information about how their devices had used Safari. Influenced strongly by European law the English Court of Appeal agreed that it was arguably personal information:

- The cookie ascribed a unique ID code to the device allowing tracking of websites visited, times visited, time spent etc;
- Devices are generally used exclusively by a single user. Identifying the device therefore tracks the habits and interests of real individual users;
- Google’s own business model is based on ability to individuate users and target advertising;
- It is inmaterial that that the agency might not intend to link up the information with other information it holds. The question is whether it can do so if it wishes.

Towards the other end of the scale are recent Australian developments. Ben Grubb’s request to Telstra for his telecommunications metadata resulted in see-sawing legal opinions. The Privacy Commissioner agreed information such as times, durations and locations of calls were about him as an identifiable person, particularly as it would routinely be made available to the police if they were investigating him. The Administrative Appeals Tribunal disagreed: it suggested if the agency hadn’t collected information with the purpose of knowing something about the individual, it wasn’t “personal” – it was information about the underlying telco system. The Federal Court stepped back from that, but too narrowly suggested that the individual has to be “the subject matter of the information or opinion.” It’s probably fortunate that the new legislation is clearer and the facts are relatively easily distinguishable.

The AAT’s approach reflects the difficulties that agencies themselves experience with personal information.

They view it through the lens of their own purpose. If they don’t mean to identify people or to use it to affect identifiable individuals, they may not spot that it’s personal information.

However, what you mean to do is irrelevant. Allowing that approach would provide a huge gap in privacy protection. Proving intentions is hard and allows agencies to evade responsibility too easily.

Sticking to a factual analysis is far better. This illustrates why privacy impact assessments are so important, as they can alert agencies to angles that they never thought of before. In New Zealand we tend to occupy the cheerfully objective and pragmatic middle ground. The Privacy Commissioner’s recent opinion about whether the Fire Service could publish addresses with callout information on its website is a good example. It concludes that an address can clearly be personal information. It’s easy to identify the homeowner: that information is readily available from a number of sources. The non-personal information that’s already on the website (date, time, duration and type of callout) then also becomes personal information by association. It tells a reader that the Fire Service came to my address to deal with a medical emergency, not because I had inadvertently flambéed my dinner.

**Dealing with the uncertainty**

The changing boundaries of personal information create a tendency to panic about floodgates and liability. However, I suggest that it often doesn’t matter that the category is wider than we might have thought.

Most importantly, it’s only a gateway to say the Privacy Act is relevant at all. If something is personal information, you quietly step to seeing how the privacy principles say you should be handling that information to deal fairly with people.

“Personal information” does not necessarily equate to a big bill either. Before that happens, the agency has to have:

- breached a privacy principle (that is, none of the pragmatic exceptions apply)
- in most cases caused some variety of significant harm
- failed to see the writing on the wall and have voluntarily done something about it.

We can therefore be relatively relaxed about letting a lot through the gateway. The Act has its own inbuilt mechanisms to make sure that liability is limited to situations where there are genuine problems.
And if something has the capacity to materially affect someone, and cause them harm you should let it through that first gateway. It forces you to figure out how to mitigate the risks. The result will be that you have much more principled and trustworthy business practices.

Secondly, we can waste a lot of time and effort in fighting about what is personal information when what we need to do is handle all information properly. Many organisations have a single system for corporate and individual information, for instance – it usually doesn’t make any kind of sense to treat them differently.

Law reform also has a part to play, but the solutions need to be principled, pragmatic and sustainable. We need our privacy laws more than ever. In a growingly complex world, people desperately need the ability to make choices, to control excesses and to obtain assurances and be confident about who is trustworthy. We don’t want to undermine the credibility of our privacy laws by making them unworkable.

Law reform solutions that will assist include:

- restricting or prohibiting reidentification from anonymous datasets – so we can get the value from the information but stop the harm from happening;
- introducing formal requirements for agencies to demonstrate accountability – including requirements to engage in risk management processes and privacy by design.

We also need to invest in creating trustworthy environments, based on inclusion, control and transparency.

If we do this perhaps we can chill a bit about what personal information means – and just enjoy the collegial arguments that it inevitably creates.

Katrine Evans is a Senior Associate at Hayman Lawyers and can be contacted at k.evans@haymanlawyers.co.nz
The Intelligence and Security Act 2017 replaces the four Acts that currently apply to the Government Communications Security Bureau, the Security Intelligence Service, and their oversight bodies. A number of provisions came into force on 1 April 2017, with the remaining provisions effective 29 September 2017.

The Privacy (Information Sharing Agreement Between Ministry of Justice and Statistics New Zealand) Order 2017 under the Privacy Act comes into force on 26 April 2017. This allows the Ministry of Justice to share information with Statistics New Zealand about people who have faced criminal charges in the District or High Courts or who have had certain orders made against them (such as protection or restraining orders). This information can be linked with other administrative information to be made available for bona fide research purposes and also for the production of official statistics.

The Customs and Excise Bill seeks to update New Zealand’s border legislation. This bill includes proposals covering the collection of biometric information at the border, a new information sharing regime and searching of electronic devices. It is currently before the select committee who is due to report on 6 June 2017.

The Children, Young Persons and Their Families (Oranga Tamariki) Bill is also at the select committee stage with a report due on 13 June 2017. This omnibus bill amends five Acts to establish a new statutory framework aimed at meeting the needs of vulnerable children and young persons. The bill introduces new information sharing provisions that will override the Privacy Act.

The Enhancing Identity Verification and Border Processes Legislation Bill is the legislative response to issues identified after the escape of Philip John Smith/Traynor. The bill includes proposals on collecting biometric information from offenders on community work and from prisoners. The bill also introduces a new Part 10A of the Privacy Act, authorising specified agencies to access and use identity information to verify the identity of individuals within the justice system and at the border. The select committee has issued its report and the bill is due back in the House for its second reading.

The Family and Whanau Violence Legislation Bill replaces the Domestic Violence Act 1995 and amends a number of other Acts. Its main aim is to ensure legislation dealing with family violence is more complete and fit for purpose. The bill proposes new information sharing provisions. This bill has just passed its first reading and has been referred to a select committee. Public submissions close on 24 May 2017.

The Law Commission and the Ministry of Justice are conducting a review of the Search and Surveillance Act 2012. The Act, which mandates this review, governs how the police and other government agencies carry out searches of property and people and use surveillance devices for the purpose of investigating crime. Submissions are now closed and the report is due by the end of June 2017.
South Australia’s Surveillance Devices Act 2016 (the Act) has recently come into effect. It expands the scope of regulated surveillance devices, and attempts to balance privacy with the reasonable use of a surveillance device. It indicates that surveillance devices laws will remain a feature of State level regulation, despite the compliance burden for multi-state organisations. This article will reflect on the Act’s impact to organisations, and Australia’s privacy regulatory landscape.

Why was this Act introduced?

The Act repeals the out-dated Listening and Surveillance Devices Act 1972 (SA). It is not the first time the South Australian government has attempted to overhaul the now-superseded law. In 2014, a surveillance devices bill was defeated in Parliament because of its publishing restrictions for information or material collected in the public interest. The new Act draws from, and builds upon, comparative State surveillance devices laws, namely in Victoria and New South Wales.

What’s new in the Act?

The Act not only regulates the installation, use and maintenance of listening devices, but also optical surveillance, tracking, and data surveillance devices. It regulates the communication or publication of information or material derived from the use of these surveillance devices, and sets up an extensive warrant regime for investigative agencies to install, use, maintain or retrieve a surveillance device.

The lowdown - how does the Act protect privacy?

Listening devices

The Act maintains the prohibition to use and maintain a listening device to overhear, record, monitor or listen to a private conversation to which the person is, or is not, a party. A ‘private conversation’ will not include circumstances in which all parties to the conversation ought reasonably to expect that a person who is not party to the conversation may hear it.

The Act now provides several exceptions, including where all principal parties to the conversation consent, expressly or implicitly, to the device being used (a theme which makes an appearance throughout the Act), if it is reasonably necessary for the protection of the lawful interests of the person using the device, or it is in the public interest.

Optical devices

The Act prohibits the installation, use, and maintenance of an optical device on or in premises, a vehicle or any other thing, to record or observe the carrying on of a private activity. The inclusion of ‘thing’ is broad enough to include surveillance without entering a premise or a vehicle, such as the ever-increasingly popular use of drones.

A ‘private activity’ excludes activities conducted in a public place, or an activity carried on or in premises or a vehicle if the activity can be readily observed from a public place (e.g. from the street), or an activity carried on in any other circumstances in which the person ought reasonably to expect that it may be observed by some other person (e.g. likely, a public speaker). Similar exceptions to the use of listening devices also apply.
Tracking and data surveillance devices

The Act prohibits the installation, use or maintenance of a tracking device to determine the geographical location of a person, without the express or implied consent of that person, or for a vehicle or thing, without the express or implied consent of the owner or a person in lawful possession or control of that vehicle or thing. Lastly, the Act prohibits the knowing installation, use or maintenance of a data surveillance device to access, track, monitor, or record the information stored in a computer, including its input into or output from, without the express or implied consent of the owner or the person with lawful control or management of the computer. The exceptions for the use of these devices are limited to where such use is permitted under another Act.

Use, communication and publishing

The Act specifies permissible instances to use, communicate, or publish information or material derived from a surveillance device, including, for instance, if each party to which the information or material relates has consented. Where a listening or optical device is used to protect the lawful interests of that person, such permissible instances also include, but are not limited to, where there is a situation where a person is being subjected to violence or there is an imminent threat of violence to a person, or to a media organisation. Where the surveillance device was used in the public interest, a court order will be required, unless it is disclosed to or by a media organisation.

Warrant regime for investigative agencies

The extensive warrant regime for investigative agencies will require a judge to consider, against other persuasive factors, the extent to which the privacy of any person would likely be interfered with by use of the kind of device to which the warrant relates.

How will the Act impact organisations?

The Act distinguishes between a body corporate (maximum penalty $75,000) and a natural person (maximum penalty $15,000, or 3 years imprisonment). Unlike the Privacy Act 1988 (Cth), all body corporates, regardless of their annual turnover, must comply with the Act. A breach of the Act could have substantial financial implications for small businesses, along with other substantial ramifications for all types of organisations, such as impacts to reputation and customer trust. Although actions taken under a State surveillance devices law can be counted by hand, businesses operating in South Australia should be cautious and ensure that they are compliant with the Act.

Organisations should consider taking the following steps:

- Document the breadth of their surveillance practices (e.g. CCTV in an office space or in a shop, phone recording capabilities, email and web browsing monitoring),
- Assess surveillance practices against their new compliance obligations,
- Identify strategies to resolve compliance gaps (e.g. providing notice and/or consent for the use and disclosure of information and material collected from a surveillance device), and
- Incorporate compliance obligations and identified strategies into their privacy policies and procedures.

How will the Act impact the Australian regulatory landscape?

The Act addresses regulatory gaps in other State surveillance legislation, including by:

- Using technology-neutral terms to recognise trending surveillance devices and capabilities, and
- Attempting to balance privacy and consent against concepts such as reasonability, necessity, lawful interests of a person, and the public interest.

South Australia has taken a leap forward to modernise its surveillance devices legislation. In the absence of a streamlined Commonwealth surveillance devices legislation (that regulates beyond law enforcement agencies), other States should consider following suit.

Ilana Singer is a Privacy and Data Protection Specialist at Deloitte and can be contacted at isinger@deloitte.com.au
LEGISLATION CORNER: AUSTRALIA: PART 2

Is Australia leaning towards a more market driven approach to privacy - or is this a one off example of expediency?

EMMA HOSSACK
Treasurer, iappANZ,
President, Medical Software Industry Association
CEO, Extensia

The Privacy Amendment (Re-identification Offence) Bill 2016 (the Bill) has not been passed at the time of writing (see at http://www.aph.gov.au/Parliamentary Business/Bills_Legislation/Bills_Search_Results/Result?bld=s1047).

The Bill originated from the Attorney General’s Department in October 2016 hot on the heels of a media report about the re-identification of de-identified health information which had been provided by the Department of Health to researchers at the University of Melbourne. The re-identification was not malicious. What’s the fuss about? The 15 submissions made to the Senate Legal & Constitutional Affairs Legislation Committee make good points not all of which were considered by the Committee which published their report recommending the Bill’s passage on 7 February 2017. The OAIC, NSW Privacy Commissioner and Australian Bankers Association in particular all make excellent points. In summary:

- All parties agree that open data is a valuable resource and support its use for research and innovation. So far, so good;
- The public service should have a new Australian Public Service-wide Privacy Code & an onus to record which data sets released by the APS contain de-identified information. This is beginning to look creepy. The public service gets my prescription history and tax information and can purport to de-identify it and release it without being trained about privacy? I have to provide the data to get a service or observe the law but the collectors may not know how to protect it;
- The Public Service should release the data in a more calibrated manner – i.e. if it’s really sensitive its availability should be limited (iappANZ members may recall Dr Khaled El Eman’s work on the likelihood of all data being able to be re-identified). Hold on – it’s likely my health information will become subject to a public data set if I forget to opt out of a My Health Record in the future. Seriously, is this something that should be released? Surely the public service has to treat it as more sensitive than my dog’s registration details?
- Responsible disclosure of vulnerabilities in databases is a valuable service carried out by many who are not acting in a nefarious manner. Will this legislation reduce responsible disclosure leaving privacy breaches open for longer than necessary?
- The Bill is “too blunt an instrument” to both protect privacy and advance research. Well said Dr Coombs!
- The retrospective nature of the Bill which has criminal and civil penalties militates against human rights legislation. Right – so research opportunities are now more important than human rights. Is this really for the greater public good?

The speed and way this Bill has been drafted brings to mind the comments by the UK Parliamentary Committee which commented on the then failed £16B national health record:

“We commend the enthusiasm of the team working on this project – but it has little else to recommend it.”
Privacy Awareness Week - Rights, Responsibilities and Roller-Coasters –
The Inevitability of a Data Breach

**Wellington**
Date: 9/05/2017  
Time: 7:30am - 10am  
**Venue:** EY - Majestic Centre, 21/100 Willis St, Wellington, 6011, New Zealand  
**Cost:** Members - Free of Charge  
Non-Members - AUD $49.00 per person

**Auckland**
Date: 10/05/2017  
Time: 7:30am - 10am  
**Venue:** TBC  
**Cost:** Members - Free of Charge  
Non-Members - AUD $49.00 per person

**Melbourne**
Date: 16/05/2017  
Time: 7:30am - 10am  
**Venue:** MinterEllison - Level 23, Rialto Towers 525 Collins Street, Melbourne VIC 3000  
**Cost:** Members - Free of Charge  
Non-Members - AUD $49.00 per person

**Sydney**
Date: 17/05/2017  
Time: 7:30am - 10am  
**Venue:** MinterEllison - Governor Macquarie Tower, 1 Farrer Place, Sydney NSW 2000  
**Cost:** Members - Free of Charge  
Non-Members - AUD $49.00 per person

**Brisbane**
Date: 18/05/2017  
Time: 7:30am - 10am  
**Venue:** Corrs Chambers Westgarth - 42/111 Eagle St, Brisbane City QLD 4000  
**Cost:** Members - Free of Charge  
Non-Members - AUD $49.00 per person
Workshop: Raising the Privacy Brand - Clarifying the Message and Increasing Awareness in 2017

**Auckland**

**Date:** 1/06/2017

**Time:** 1pm – 3pm *(Registration will open at 12:30pm with the workshop concluding at 2:30pm for afternoon tea and networking)*

**Venue:** KPMG Auckland  
18 Viaduct Harbour Ave, Auckland 1140, New Zealand

**Cost:** Members - AUD $99.00 per person  
Non-members - AUD $175.00 per person

**Wellington**

**Date:** 2/06/2017

**Time:** 9am – 11am *(Registration will open at 8:30am with the workshop concluding at 10:30am for morning tea and networking)*

**Venue:** KPMG  
10 Customhouse Quay, Wellington 6011, New Zealand

**Cost:** Members - AUD $99.00 per person  
Non-members - AUD $175.00 per person

*For more event information visit www.iapanz.org*
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.
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/
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.