## Contents

1 / PRESIDENT’S FOREWORD  
Melanie Marks  
page 4

2 / GLOBAL PRIVACY SUMMIT SNIPPETS  
Melanie Marks & Veronica Scott  
page 5

3 / Q&A WITH MARTA GANKO, CIPP/E, CIPM  
page 9

4 / AIR NEW ZEALAND AND THE GDPR  
Shivani Linghan  
page 11

5 / 5 QUESTIONS ABOUT DPOs  
Tim de Souza  
page 13

6 / NEW ZEALAND PRIVACY ACT REFORM  
Katherine Gibson  
page 15

7 / PRIVACY IN THE AGE OF SMART CITIES  
Nicole Stephensen  
page 21

8 / OPAL CARD PRIVACY CASE ILLUSTRATES DANGERS OF OVER-COLLECTION BY SMART DEVICES  
Anna Johnston  
page 23

9 / PRIVATE EYES: PARENTS, SCHOOLS AND THE TROUBLE WITH PHOTOS  
Colin Anson-Smith  
page 24

10 / AUSTRALIA’S FIRST DATA BREACH NOTIFIED UNDER THE NEW REGIME  
Lyn Nicholson  
page 26

11 / LEGISLATIVE UPDATE AUSTRALIA  
page 28

12 / UPCOMING EVENTS  
page 29
Our contact details

Privacy Unbound is the journal of the International Association of Privacy Professionals, Australia-New Zealand (iappANZ), PO Box 576, Crows Nest, NSW 1585, Australia (https://www.iappanz.org/)

If you have content that you would like to submit for publication, please contact the 2018 Editors:

Lyn Nicholson (Lyn.Nicholson@holdingredlich.com) and Katherine Gibson (katherine@gibonslaw.co.nz) the co-chairs, covering both AU and NZ together with Veronica Scott, Nicole Stephensen and David Templeton.

If you have an idea for the journal please share it with us. We are keen to broaden content and scope to all things privacy related and all aspects of the privacy profession.

Please note that none of the content published in the Journal should be taken as legal or any other professional advice.
Welcome once again to the region’s best publication for privacy professionals in Australia and New Zealand. Having just returned from the IAPP global privacy Summit in Washington DC, where privacy professionals from around the globe congregated to hear the latest in thought leadership, policy development and implementation, I am proud to return home with the view that we are at the forefront of privacy leadership and management.

During our visit to DC, the iappANZ cohort met with IAPP President and CEO, Trevor Hughes and members of his leadership team, Tory Bell and Amy Sherwood, to discuss developments at IAPP global HQ and how our organisations might work more closely and bring Kiwis and Aussies more from the global offering. One of the immediate developments for our region is a local certification (CIPP-ANZ), release of which is anticipated later this year. You will be hearing lots more about this over the coming months.

This month’s edition of Privacy Unbound features a few snippets from the global Summit by Veronica Scott and me, including synopses on managing vendor risk, privacy and artificial intelligence, perspectives on the online reputation debate and ethical issues with scraping the web. Next month we will feature more insights to the Summit and in the meantime recommend that all members look at the IAPP website for more information.

GDPR clearly has the attention of privacy professionals around the world and in this edition of Privacy Unbound we focus on a few different perspectives including:

- Marta Ganko, current Executive Manager, Privacy at Westpac Group and formerly National Privacy Lead in Risk Advisory at Deloitte shares her insights into the biggest issues under GDPR (and also discusses her experience in obtaining CIPM and CIPP/E certifications);
- Shivani Lingham from Air New Zealand shares their experiences in building the GDPR requirements into the airline’s wider privacy programme, combining regulatory obligations with its privacy commitment to customers. On this, I’d like to congratulate Air New Zealand on recently being recognised in SkaiBlu’s e-commerce consultancy report which benchmarked airlines’ digital capabilities. Air New Zealand was rated 5th overall out of 90 airlines and was called out as 1st in digital data privacy leadership. A terrific achievement for Air New Zealand’s global privacy team.
- Tim de Sousa outlines the requirements for a Data Protection Officer under GDPR and what sort of approach local companies should take.

Big regulatory changes are also on foot in the land of the long white cloud. Katherine Gibson, Co-Chair of the Privacy Unbound editorial committee asks some of the nation’s finest their views on the much-anticipated Privacy Bill. Hear from Daimhin Warner, Fiona Colman and Katrine Evans on:

- Which aspects of the Bill they support;
- What significant areas of reform are missing;
- Surprises in the Bill;
- Mandatory breach reporting provisions;
- How businesses need to change to comply; and
- What should Privacy Officers be doing right now.

How do we have a positive and proactive influence as privacy professionals? Nicole Stephenson writes about her experience talking at “Cities 4.0—Privacy in the age of Smart Cities”.

We also report on the first mandatory breach notification in Australia, the Svitzer breach.

We’ve also republished Anna Johnston’s recent blog on the collection of location data by Transport NSW in its Opal Cards system.

In another republished blog by Colin Anson-Smith, we look at parents, schools and the trouble with photos. What role do schools play in setting policies for the taking of photographs by other parents?

Finally, you can read updates on the progress of amendments to the Privacy Act in Australia.

What an incredible summary of developments, changes and challenges from our community. I’d like to say a big thank you to the Journal committee and all of our wonderful contributors. Happy reading!
The annual iapp Global Privacy Summit was held this year in Washington DC on March 27 and 28. iappANZ was delighted to have a number of its board members attend and provide some high level take-aways from the sessions that they attended.

We had a total of 4 representatives and in this edition of Privacy Unbound, we will provide a couple of snippets from iappANZ President, Melanie Marks and Vice President, Veronica Scott. The theme of the Summit was the “profession at a cross roads”. This theme took account of the variety of issues facing privacy including the fact that “data is the new oil” and that privacy is deeply human including, as a human right and that trust is fragile and easily broken.

The Summit provided a range of keynote speakers, presentations, and breakout sessions and much of the material is available at the IAPP website, for those that are interested. We are delighted to provide summaries from the sessions, below:

- “Vendor Risk 2.0 – Are You Sure You Know Where Your Data Is” and
- “Artificial Intelligence: Benefits and Harms of Always-Listening and Always-On”

“Vendor Risk 2.0 – Are You Sure You Know Where Your Data Is”

This was a panel based discussion featuring Michelle Beistle of AOL and Charlotte Young of The Nature Conservancy. On vendor risk, the panellists advocated for:

- A risk based, consistent and reasonable approach i.e. there is no magic bullet;
- Tackling highest risk data sets first then working with data owners and key stakeholders to understand systems, safeguards and risks;
- Developing a questionnaire for vendors (including a threshold test which would then open out to a full privacy and security assessment);
- Ensuring that contractual terms deal with the whole data lifecycle leading to expiration of the contract;
- Staff awareness of the process and positioning supplier risk management processes as a commercial requirement rather than a “compliance” one for maximum buy in;
- Not exempting law firms and consultancies from supplier vetting processes;
- Installing an assurance layer through audit; and
- Picking your battles – e.g. it may be sufficient to ask the vendor to maintain their ISO certification or for them to present an audit report by an auditor of their choosing.

As for responding to a supplier assessment as a vendor:

- Responses should always be transparent and not profess to know answers that the organisation does not know;
- Responses should be current and not cite outdated legislation like “Safe Harbour”. Vendors should ensure that privacy policies and other promises are up to date;
- Sales jargon and bluffing will always be seen as that;
- Stand out from the competition with a simple and honest one-page summary of who the entity
is, what they do, what data they collect and what they do with it; and

- Make sure that any links work.

“Artificial Intelligence: Benefits and Harms of Always-Looking and Always-On”

This was a panel discussion featuring Andrew Dale of dataxu, Vivek Narayanadas of Shopify and Pedro Pavon of Oracle.

Some of the key comments from panellists were:

- Notice and choice bargain does not work with artificial intelligence (AI)/machine learning. Even if compliance obligations are met, from a philosophical standpoint, the mechanism falls short;
- In view of this, a social roadmap is needed; i.e. an ethical framework for what is ok and what is not. Ethical frameworks should be set collaboratively with input from the various functions of the company and shared with customers;
- GDPR Art 22 (automated decision making) raises the question of how do you tell someone what you’re doing with their data when you don’t know because this has not yet been determined and will be determined by the algorithm? What is reasonably foreseeable?
- Machine learning requires privacy by design i.e. decision makers need to identify the potential harms that inputs could deliver.

The panellists were then asked - as smart devices in the home proliferate, will they have a chilling effect on how people behave i.e. will people be “less free”? The main risks identified included:

- Everything you say can be picked up, recorded and used against you and therefore devices take away your personal space.
- The power of combined data sets to identify and discriminate.
- The physical risks of a connected home – for example, what if your stove can be intercepted and activated without your control?

However, one of the complexities for policy makers are that attitudes vary. For example, one of the panellists imagined a world where his smart car could act as a therapist, having gathered enough information to be able to counsel him.

On the question of whether consumers have a right to know if they’re engaging with a bot rather than a person, panellists agreed that it is contextual - for example, in a sales context they would often be unlikely to care but this would differ with online dating apps, life insurance products and other products with significant legal consequences for the individual. One panellist advocated for a “right to meaningful human interaction” – i.e. not just knowing the difference between a bot and a human but being given the choice to speak with a human.

Zoom through the IAPP 2018 Summit in DC

This is a brief round up of my first experience of the global IAPP Summit that takes place in Washington DC every year near Easter. It was a massive event, from Monday 26 through to Wednesday 28 March and very well run by an amazing team of IAPP staff, with over 3500 people moving over 4 floors plus an exhibition hall. The hall hosted a range of 21 vendors including iappANZ platinum sponsor Microsoft, Nymity, TrustArc and OneTrust. There were more than 30 sessions (with many sessions running consecutively), plus 5 key notes. The sessions covered topics including blockchain, data scraping, GDPR compliance, data breach notification and response, Privacy Shield, AI, Smart Cities, Big Data, online reputation. For more details of the sessions and recordings check out this link https://iapp.org/conference/global-privacy-summit-2018/

The Summit took place against the backdrop of another turbulent week in US politics including the Stormy Daniels interview and the student 'no guns in schools' march on the Capitol, as well as the Facebook/Cambridge Analytica revelations and Mark Zuckerberg’s interview acknowledging that Facebook and breached its users’ trust.

iappANZ Board directors attending the Summit were invited to pre and post Summit events to meet the IAPP team including CEO Trevor Hughes, its CIO, Operations and training team and Country Leaders in the UK, Ireland and Europe, some of whom we hope to see at our iappANZ Summit in November.

The keynote speakers Monica Lewinsky, Simon Schama and Jon Ronson gave a fresh take on privacy from a personal,
research and historical perspective respectively and there was a call to arms from the very impressive European speakers, MEPs Birgit Sippel and Vivian Reding.

As an Australian based privacy professional, my Summit experience confirmed that there is a real sense that this is the time of the privacy professional and we need to be setting the agenda. GDPR is the game changer, but no one has all the answers. In fact more questions were asked than were answered. Trust, user rights and control, digital reputation and data ethics, were common themes across the sessions.

Some highlights from some of the sessions I attended (which were very hard to choose from!):

**Perspectives on the online reputation debate**

This session tackled questions about whether our online reputation deserves protection and if so by what criteria, picking up the themes of Monica Lewinsky's very personal keynote. The Privacy Commissioner of Canada spoke about its recent consultation and research into the issue to develop its own position and the ability to control ones online reputation through new remedies such as de-indexing or take down requests, in light of the development of the right to be forgotten found in Article 21 of the GDPR.

So much of the public space in which we operate to express ourselves is now defined by so few players who can determine what is visualised online and act as information gatekeepers. Our online status depends on our online engagement, which is determined by them and the devices we use. Personal data online can be manipulated. But whose responsibility is it to protect freedom of speech or our privacy?

The starting point is that an individual can be harmed simply by their information being available online, because it is used for so many key decisions about them, even if it is out of date or inaccurate. This raises the challenge of new risks of harm and ongoing negative consequences for individuals. Social media did not exist when defamation laws were adopted and therefore its remedies are not necessarily appropriate. The aim is therefore to develop mechanisms to give individuals some measure of control and ensure a balance between privacy and freedom of expression. Canada’s focus is on the principle of accuracy and ensuring the most accessible version of one's history that is available in search results is accurate, up-to-date and complete and in the public interest, rather than changing the past. Its solution is not to delete everything and the primary focus should be on privacy education to prevent harm rather than remediation, to enable individuals to learn about and manage the risks and knowingly agree to them and to be good online citizens.

However, after the fact solutions are also required where individuals make mistakes. This requires a balancing act between freedom of expression and the right to a good reputation, which should also be protected and is important to self-realisation and individuals' desires to express themselves. This leads to the following questions –

- Who should decide how to arbitrate a balance between these various rights? Should it be the domain of private sector enterprises?
- What parties should be represented in any decision-making? Should it include the original sources of the information?
- While it may be ideal to have independent and fully funded agencies making these decisions in contested cases, after search engines have made their initial decision, is it appropriate for search engines to make the initial decisions? Does this promote or hinder access to justice and can it provide a practical and efficient means of resolving issues?

Apparently search engines are doing a reasonably good job in the EU according to the Canadian Privacy Commissioner. Less than half of the take down requests have been granted and when reviewed by Data Protection Authorities, for the most part, the take down decisions have been upheld. While not perfect, he sees this as a better avenue than defamation and a pragmatic way to give some meaningful control to individuals. It will involve considerations such as where an individual has contributed to the information, or if it is deceptive or inaccurate. The Canadian proposal is therefore what it says is a modest development of the data quality obligation, in the form of a right to have an individual's data rectified, or erased.

**Scraping the web - the ethics of collecting public data**

Data scraping and how to control it is becoming an increasingly hotly debated topic, particularly given the impact of the ability to combine and use large amounts of publicly available data for different purposes. With the push for open data and the development of smart cities, the debate about both the legal and ethical issues relating to scraping publicly available data is an important one to have. Its also another example of law and practice not keeping up with technology. This session sought to analyse the legal and technical issues and public interest arguments and come up with some practical answers.

There are competing interests in public data. If data scraping is technically illegal, can it be ethically justified? Your view about what is acceptable data collection will also depend on who you are (researcher, journalist, law enforcement, recruiter, start up, Cambridge Analytica, etc) and what the purpose of your data collection activities are – private or public interest?
The session looked at three recent US cases in the context of the scope of the US Computer Fraud and Abuse Act (CFAA) (which prohibits unauthorised access to computers). These were LinkedIn’s case against startup hiQ, actions by Craigslist and an appeal by David Nosal, a former employee of Korn Ferry International. The CFAA is currently the subject of a number of constitutional challenges by some researchers and journalists on the grounds that it has a chilling effect and offends the First Amendment because it makes scraping the internet a crime. The work of David Fahrenthold was cited as an example of this. He writes for The Washington Post and has been actively investigating the Trump administration and piecing together evidence from public sources to ‘follow the money’. But the other side of the coin is activities such as government surveillance that involves the scraping of data of targeted communities of colour and vulnerable groups using social media and demonstrating how different people are treated differently online through a practice known as web lining.

While companies should be developing their own policies on what use of data is acceptable, the challenge is how do you audit these uses? The Cambridge Analytica case is a prime example where it violated Facebook’s policy, but once the data has left the building it is hard to know what happens to it.

So what’s the answer? Is data scraping effectively a data security breach? While the legal answer may be no, what is the policy and ethical position which the law doesn’t cover? How can websites address these issues for themselves? Protecting privacy is not just about compliance and is protected as much by law as it is by friction. Developing a set of rules and policies to match user expectation and protect them will reduce friction. So instead of simply saying no scraping is permitted and calling your lawyer, consider a combination of the following tools that were proposed:

- be transparent and explicit about what data you are collecting and why;
- use front line user controls;
- nuanced policies with explicit and transparent statements about limitations on data use.

Because not all types of ‘scrapers’ should be treated in the same way.

Melanie Marks is iappANZ President. Melanie is also founder and privacy lead at elevenM, an Advisory Board member of Information Governance ANZ and an Expert Advisor to LexisNexis on privacy and data protection.

Veronica Scott is iappANZ Vice-President. She is also senior member of MinterEllison’s Media and Communications team and leader of the firm’s National Privacy Group. Her work covers all aspects of content gathering, creation and publication and big data across traditional and new media, including print, broadcasting and digital.
This month Privacy Unbound (PU) interviews Marta Ganko, the current Executive Manager, Privacy at Westpac Group and formerly National Privacy Lead in Risk Advisory at Deloitte. Marta is certified with the IAPP.org certifications CIPM and CIPP/E which is the European accreditation. As a privacy practitioner in Australia, PU is interested, in light of the GDPR, to learn about Marta’s experience of advising on current European laws and the upcoming GDPR while based outside of the EU and her CIPP/E certification.

**PU: When did you decide to apply for certification and what motivated you?**

MG: At the time the GDPR was first making its way through the European Parliament, I was the Privacy lead at Deloitte and knew that with a local client base which operates globally, including offering services to individuals in the EU, I would need to upskill and enhance my offering to clients. Once the GDPR was signed and we knew the effective date, I needed to enhance my credentials. As there are very few options available I decided to undertake the CIPP/E.

**PU: Once you started, how long did it take and what was it like?**

MG: When I did the course it was in a different format than it is now. Now there is a textbook. However, at the time I did it, it involved taking an online course which included a number of modules with quizzes at the end. As well it involved reading a significant bundle of resources that related to the final exam content, and effectively learning and applying that for yourself.

As a non-practising lawyer and a privacy specialist outside of the EU, one of the most difficult parts of the exam for me was the understanding of the European Union legal system and understanding how the resources I had read operated within that framework.

I understand from discussion groups I am in that those who attend the residential courses that are now available as an option seem to find this helpful in passing the exam.

**PU: So if you are not practising as a lawyer what is your background?**

MG: Originally, I undertook a Bachelor of Science in Computer Science and Information Systems, spent many years as a business analyst, understanding in depth how organisations collect, use and share data in the context of large technology projects. I did a Masters in Communications Law a few years ago as I have always been interested in looking at the intersection of technology and law, and the different regulated and unregulated frameworks that apply. For example, I have a strong interest in social media, what it does and how it is regulated, or unregulated.

When getting the certification the real issue on how the EU legal system worked is probably difficult for anyone with a non-European legal background. I find that my deep understanding of how data is used by businesses supported by technology means I can apply a practical lens when suggesting solutions and the legal system may not really matter if the focus is to do the right thing by an individual. However, having said that I passed my exam.

**PU: Did you get a lot of work after your certification as a consequence of it?**

MG: While there seems to have been a lot of activity and industry media attention around GDPR recently, my perception is that, the interest of organisations in the application of the GDPR to them when they operate in Australia began with a very low base and has been increasing steadily over the last 6 to 12 months. Of course
now that I am no longer consulting, I don’t know what will happen in the next little while but there are clear signs that privacy and data protections regimes around the world are only getting stronger.

It is good to have the recognition of the certification. I am sure that as GDPR is implemented the interest in all organisations in employing Privacy professionals with some form of certification will rise.

**PU: Have you seen increased interest in certification amongst colleagues?**

**MG:** There is a new standard of a Privacy professional that is emerging. My view is certainly more Privacy professionals are now are looking at ways to differentiate themselves from others who call themselves Privacy professionals and certification is clearly one way to do this.

The great thing about these new laws is that in Australia we are all starting at an even level playing field – so it is an opportunity for all Privacy practitioners to upskill and learn from each others’ experiences.

**PU: In your experience in advising Australian organisations on GDPR, what is the biggest issue?**

**MG:** It is often quite difficult to find individuals with applied experience in Australia as opposed to theoretical experience and it is often necessary to engage advisors on the ground in each relevant jurisdiction. Certainly for clients, they don’t want to engage a local firm here for GDPR advice if there will need to be double handling and that firm needs to refer back to an EU affiliate.

**PU: As companies seek to become GDPR ready, what do you see as the biggest risk?**

**MG:** As you know, there are the various tests as to how the GDPR applies extraterritorially, including in Australia, such as: do you process personal data as part of an operation in the EU; do you provide goods and services in the EU. The third test, which is whether you monitor the activity of individuals in the EU, is one that is largely misunderstood and one that needs to be analysed to determine if companies who would otherwise dismiss the risk of GDPR application to them need to consider it.

While there is a question as to whether the authorities will aggressively seek to enforce GDPR in Australia, the issue for globally operating companies is to ensure that they have ascertained their risk exposure and addressed it with a sustainable solution, rather than react to events which may occur.

**PU: So Marta, you’ve recently changed roles and moved inside of corporate, rather than advising corporates. What do you think has been the biggest change?**

**MG:** It has been absolutely fascinating and I am enjoying every minute, although there seems to not be enough minutes in the day. While I have always had a consumer centric view on privacy, I have really found that my focus is on thinking about solutions from a customer’s perspective and doing the right thing by a customer. This is often achieved through practical solutions which demonstrate governance of end to end business processes.

**PU: But what about all of the technology that people are spruiking to help organisations to meet their GDPR obligations?**

**MG:** I am not across all of the technology but have certainly looked at a few options and while there are many benefits, one of the drawbacks is often that the technologies are not easily integrated into existing systems, and so with limited time and resources, I believe it is better spent implanting a practical solution within an existing business process and considering the longer term strategic solution separately.
At Air New Zealand we know the way we handle the personal information of our customers is crucial to earning and maintaining customer trust. Our privacy commitment to our customers is to "think privacy & do the right thing".

We put customers at the core of everything we do and engaging in good privacy behaviours helps us to remember that. Our privacy commitment applies no matter where in the world customers use our products and services.

A key focus for our privacy function at Air New Zealand over the last couple years has been working toward readiness with the incoming EU General Data Protection Regulation (the GDPR). The regulation is intended to establish a single set of data protection rules across European Member States. Its purpose is to give individuals better control over their personal data held by organisations. All companies who are captured by the GDPR are expected to be fully compliant by 25 May 2018.

Air New Zealand has a regional office based out of London, we also fly EU customers and market our services to them. Although our headquarters are outside of the EU, due to the extraterritorial scope of the GDPR, Air New Zealand is captured by the regulation.

At Air New Zealand we have been working toward readiness for compliance for a couple of years and have built the GDPR requirements into our wider privacy programme as “best practice”.

To support the privacy programme and increase awareness of the GDPR our internal Global Privacy Office (GPO) established a Privacy Working Group (PWG). The Privacy Working Group consists of key stakeholders including Legal, Digital, Customer Communications, Contact Centre, Airports and Regional functions. Several sub-working groups were also established in Digital, Legal, Information Security and Employment Relations to address specific GDPR deliverables. These working groups are aware of the need to own and address GDPR requirements that require technical and operational action in their business functions.

Where the GPO have defined the requirements for the new rights for individuals, such as the right to data portability, the right to erasure and the right to object under the GDPR, we have worked with key stakeholders and provided support to form supporting processes to ensure readiness. Our aim is that on the 25 May 2018 when the GDPR comes into effect, Air New Zealand staff will be equipped with the awareness, information and skills to identify and successfully manage requests from customers. The term GDPR isn’t one we have brandished about across the organisation, we are more focussed on ensuring staff “think privacy & do the right thing”.

Customers won’t necessarily specifically refer to the GDPR when asking for their data to be removed. We need staff to listen and respond appropriately by directing customers to our privacy centre when personal data is mentioned.

The GDPR obligations cannot be managed by one function alone, readiness relies on cross-functional collaboration from all business partners and stakeholders to be successful. Within Air New Zealand the Global Privacy Office is responsible for managing the GDPR readiness plan and the business partners and stakeholders are responsible for delivering the requirements in their respective areas.

Over the last year we have conducted various workshops and training and awareness sessions throughout the organisation to increase understanding of the importance of the regulation and to gain the support of our stakeholders in working toward readiness.

To Air New Zealand GDPR readiness means being prepared to act on GDPR related requests. We have identified the core requirements of the GDPR (listed below) and worked with impacted functions on compliance with each.

- **Mandatory data protection officers.** A data protection officer has been identified. The data protection officer is accountable for the delivery of the GDPR requirements and accountable to Air New Zealand Executive.
- **Records of processing activities.** We have defined and will continue to maintain system inventory requirements and update regularly.
• **Disclosure to law enforcement restricted.** We will continue to respond to and manage all law enforcement agency requests.

• **Privacy by Design / Default.** We will maintain Privacy by Design and Privacy Impact Assessment frameworks and templates.

• **Accountability framework.** We will maintain and update Air New Zealand’s internal & external Privacy Policies.

• **Transparency.** We will maintain and update our external Privacy Statement to meet transparency requirements and further explain how we handle personal information.

• **New Rights for individuals.** We will provide guidance and supporting the business in building processes to allow individuals to exercise these rights.

• **Increased security obligations.** We are ensuring that the current internal security policies reflect GDPR requirements.

• **Privacy impact assessments for high risk initiatives.** We will continue to undertake privacy impact assessments for high risk initiatives. Ensure PIA framework is reviewed and amended to comply with the GDPR.

• **Mandatory breach notification.** We are updating our breach response process to meet GDPR requirements for 72 hour compliance and informing individuals.

• **Clarification of legal grounds for processing (including consent).** We are maintaining documentation that supports the decisions taken for lawful basis for processing core customer related activities.

• **International transfers.** We continue to provide guidance and oversight to the business on compliance with international transfer requirements. Our Data Protection Schedule remains compliant with GDPR requirements.

At Air New Zealand we have taken a pragmatic approach to defining and achieving compliance. We have built the GDPR requirements into our wider privacy programme, combining regulatory obligations with our privacy commitment to our customers. We have assessed the likely impact of GDPR requirements and worked with key business partners to agree and implement an approach. It’s been an organisation wide initiative managed by the Global Privacy Office. Whilst we are poised to act on GDPR related requests to enable compliance, we will keep an eye on the developments post GDPR and amend our approach as necessary.

Through multiple training and awareness sessions, Air New Zealanders are excited by the opportunities presented by the GDPR. We know if we are seen to be raising our privacy game our customers will continue to trust us with their data as we continue to ‘think privacy & do the right thing’.

Shivani Lingham is currently Privacy Officer at Air New Zealand. She advises on privacy and data protection matters internally and focuses on a customer centric view of personal information and data privacy. Shivani has a legal background and is a qualified CIHF - IAPP, a registered Barrister and Solicitor (NZ Law Society) and a member of the IAPP.
1. What is a ‘DPO’, anyway? What are they even supposed to do?

In a nutshell, the Data Protection Officer (DPO) is a senior advisor with oversight of how your organisation handles personal data.

Specifically, DPOs should be able to:

- inform and advise your organisation and staff about their privacy compliance obligations (with respect to the GDPR and other data protection laws)
- monitor privacy compliance, which includes managing internal data protection activities, advising on data protection impact assessments, training staff and conducting internal audits
- act as a first point of contact for regulators and individuals whose data you are handling (such as users, customers, staff... etc.) (Art. 39(1)).

2. But we’re not based in Europe, so do we even need one?

Well, even if you aren’t required to have one, you should have one.

If you’re processing, managing or storing personal data about EU residents, you’ll need to comply with the requirements of the GDPR – this is one of those requirements, whether you’re based in the EU or not.

Specifically, the GDPR requires that you appoint a DPO in certain circumstances (Art. 37(1)).

These include if you carry out ‘large scale’ systematic monitoring of individuals (such as online behavioural tracking).

You’ll also need to appoint a DPO if you carry out ‘large scale processing of personal data’, including:

- ‘special categories of data’ as set out in article 9 – that is, personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric identifiers, health information, or information about person’s sex life or sexual orientation.
- data relating to criminal convictions and offences (per Art. 10).

The Article 29 Working Party has stated that ‘large scale’ processing could include, for example, a hospital processing its patient data, a bank processing transactions, the analysis of online behavioural advertising data, or a telco processing the data required to provide phone or internet services.

Even if you don’t fit into one of these categories, you can still appoint a DPO in the spirit of best practice, and to ensure that your company is leading from the top when it comes to privacy.

In this respect, New Zealand is already ahead of the game. Entities covered by the New Zealand Privacy Act are already required to have a privacy officer, and they largely fulfil the same functions as a DPO. However, they’ll still need to meet the other DPO requirements; see below.

While Australia hasn’t made having a privacy officer an express requirement for the private sector, the Office of the Australian Information Commissioner recommends that companies appoint a senior privacy officer as part of an effective privacy management framework.

Government agencies aren’t off the hook

Being Public Service will not save you. Public authorities that collect the information of EU residents are also required to have a DPO (Art. 37(1)).

It’s worth noting that Australian Government agencies will need to appoint privacy officers and senior privacy ‘champions’ under the Australian Government Agencies Privacy Code, which comes into force on 1 July 2018. Agency Privacy Champions may also be able to serve as the DPO.

As New Zealand Government agencies already have privacy officers, the only question they must answer is whether their

---

privacy officer meets the other DPO requirements; see below:

3. OK, fine. We get it. We need a DPO. Who should we appoint?

The DPO needs to be someone that reports to the ‘highest management level’ of your organisation; that is, Board-level or Senior Executive (Art. 38(3)). They’ll need to be suitably qualified, including having expert knowledge of the relevant data protection laws and practices (Art. 37(5)). The DPO also needs to be independent; they can’t be directed to carry out their work as DPO in a certain way, or be penalised or fired for doing it (Art 38(3)). You’ll also need to ensure they’re appropriately resourced to do the work (Art. 38(2)).

If you’re a large organisation with multiple corporate subsidiaries, you can appoint a single DPO as long as they are easily accessible by each company (Art. 37(3)). You can appoint one of your current staff as DPO (Art 37(6)), as long as their other work doesn’t conflict with their DPO responsibilities (Art. 38(6)). This means that you can’t have a DPO that works on anything that the DPO might be required to advise or intervene on. That is, they can’t also have operational responsibility for data handling. This means you can’t, for example, appoint your Chief Security Officer as your DPO.

4. But that means we can’t appoint any of our current staff. We can’t take on any new hires right now. Can we outsource this?

Yes, you can appoint an external DPO (Art 37(6)), but whoever you contract will still need to meet all of the above requirements.

Some smaller companies might not have enough work to justify a full-time DPO; an outsourced part-time DPO might be a good option for these organisations.

It might also be hard to find qualified DPOs, at least in the short term; IAPP has estimated that there will be a need for 28,000 DPOs in the EU. A lot of companies in Australia and New Zealand are already having trouble finding qualified privacy staff, so some companies might have to share.

5. This all seems like a lot of trouble. Can we just wing it?

I mean, sure. If you really want to. But under the GDPR, failure to meet the DPO obligations may attract an administrative fine of up to €10 million, or up to 2% of your annual global turnover (Article 83(4)). Previous regulatory action in the EU on privacy issues has also gained substantial media attention. Is it really worth the risk? Especially given that, in the long run, having robust privacy practices will help you keep your users and your customers safe - having an effective DPO may well save you money.

Tim De Sousa is an iappANZ board director and a privacy and information governance legal and policy specialist, with a focus on emerging technologies. Tim now holds a senior advisory role with elevenM, working with some of Australia’s leading brands to build privacy capability and manage risk.

5 https://iapp.org/news/a/study-at-least-28000-dpos-needed-to-meet-gdpr-requirements/
NEW ZEALAND INTRODUCES ITS PRIVACY BILL
By: Katherine Gibson

It is here, at last... the Privacy Bill has finally arrived, having been introduced into parliament by the Minister of Justice in March. New Zealand’s Privacy Act turns 25 this year and law reform is well overdue, so this much anticipated legislation was widely welcomed by privacy professionals.

The Bill includes many of the changes recommended by the Law Commission in 2011 and in Reports by the Office of the Privacy Commissioner, including mandatory breach notification, increased enforcement powers for the Privacy Commissioner, new criminal offences and greater protection for overseas information transfers. While the technology-neutral principle-based model is retained, there are some unexpected proposed procedural changes to the access request regime which may complicate a current process that is working.

However many will consider the Bill does not go far enough to ensure we are keeping up with international trends and other jurisdictions – such as Australia and the EU. Reforms on issues such as re-identification, anonymity, data portability, public registers and introducing a meaningful civil penalties framework for serious breaches, are all missing.

The Bill is available at https://www.parliament.nz/en/pb/bills-and-laws/bills-proposed-laws/document/BILL_77618/privacy-bill and will now have its first reading in parliament and will then be referred to a Select Committee where submissions can be made. Katherine Gibson asked three well-known New Zealand privacy practitioners their views on the Bill and what businesses and Privacy Officers should be doing right now in readiness for the proposed changes.

Daimhin Warner is Auckland Director of Simply Privacy, a consultancy providing privacy advice, strategy and training to business and government. Daimhin is a Board Director of the International Association of Privacy Professionals ANZ (iappANZ) and Co-Chair of iapp’s ANZ Certification Advisory Board.

Daimhin Warner, Director, Simply Privacy

What aspects of the Bill do you support?

The Bill does not fundamentally alter the current privacy framework. Rather, it sharpens the edges. This is good and not so good. In general, the Bill improves privacy protection in New Zealand, but it does so more gently than many may have hoped. That said, the Bill is a positive step forward in a number of ways:

1. **A lift in agency accountability**: By introducing a mandatory privacy breach notification framework, and bolstering the obligations on agencies that use third party (particularly overseas third party) providers to process data, the Bill sends a clear message to agencies that they will need to be more publicly accountable for the way they handle personal information.

2. **More teeth**: The Bill gives the Privacy Commissioner a set of additional powers to enforce compliance, including the ability issue compliance notices to agencies and to make binding decisions on access requests. These powers have been long overdue and, as the Office of the Privacy Commissioner has proved itself over the years to be a reasonable regulator, agencies should have confidence that these powers will be appropriately exercised. The Bill also introduces new criminal offences, including an offence to knowingly destroy personal information that is subject to an access request.
3. **Retained flexibility:** Importantly, the Bill retains the privacy principles model that has worked well until now, guiding agencies to manage personal information fairly and responsibility but allowing them the latitude to get on with business. This approach should be preferred over more complex and prescriptive legislative frameworks seen overseas, which are significantly more difficult to operationalise for agencies. The Bill updates the principles to ensure that they are fit for purpose, including new obligations when disclosing personal information overseas.

**What significant areas of reform are missing and why should we be concerned about that?**

For many years, New Zealand has been highly regarded internationally as a jurisdiction with strong and effective privacy regulation. The Privacy Act managed to be flexible and pragmatic, by focusing on principles that allowed agencies to get on and do legitimate business, but also wide in scope and coverage by applying to all agencies regardless of size or turnover, covering personal information about employees, customers, and anyone else an agency might deal with, and providing people in New Zealand or overseas with strong access and complaint rights. As a result, New Zealand was one of the few countries to be recognised by the EC as "EU adequate". This underwhelming accolade in fact shone us, and our agencies, in a remarkably strong light the world over.

However, as we now know, privacy regulation overseas is rapidly catching up and, with recent changes such as those witnessed in the EU (with the forthcoming GDPR) and Australia, will soon overtake us entirely. This privacy reform process is our opportunity to keep pace with international trends. However, many consider that the Bill has stopped short of bringing in the level of change we need to do so. This means that our privacy law is at risk of losing its adequacy status and our globalised and innovative businesses are at risk of losing out to competitors based in countries with stronger privacy regulation in place.

There were a few things the Bill should have included, that would have strengthened its overall impact. The Bill does not, for example, require agencies to complete privacy impact assessments (something that the GDPR does). The Bill also fails to provide New Zealanders with any right to anonymity (something expressly provided in other jurisdictions, such as Australia). As we witness the growth of smart cities, AI and the internet of things, the right to operate with some level of pseudonymity or anonymity becomes all the more important. It is a shame this was not made expressly clear.

Most importantly, however, the Bill has fallen short on creating real consequences for serious breaches of the law – consequences that have formed the backbone of international privacy regulations (most prominent of which, the GDPR, introduces penalties of up to 4% of an agency’s annual global turnover, to a maximum of 20 million Euros). The Privacy Commissioner openly called for lawmakers to consider providing for a penalties framework in the new Act, suggesting a modest $1 million civil penalty for serious breach. The fact that this has not been considered for inclusion in the Bill will weaken our overall privacy framework relative to other jurisdictions.

The Privacy Commissioner framed this issue very well in a recent blog: "...without real and meaningful consequences for non-compliance, rogue agencies will continue to thumb their nose at the regulation, meaning responsible organisations will disproportionately bear the cost of compliance, while cowboys will ignore their obligations".

**Were there any surprises in the Bill?**

The short answer is, no. This Bill was a long time coming. The Law Commission made a set of very robust recommendations that set expectations early, and the government responded relatively soon after to indicate that some things - including mandatory breach notification, enforcement powers for the Privacy Commissioner, and greater accountability for overseas information transfers - would be very likely to follow. The Bill delivers these things but makes no other radical changes to the regulatory regime.

That said, the Bill has somewhat complicated the procedural provisions in respect of subject access requests (under information privacy principle 6) and this was neither expected nor necessary. The new Part 4 expressly separates the way an agency should respond to requests for confirmation of whether personal information is held and requests for access to that information. In practice, this distinction is not particularly useful. An individual rarely seeks only to know whether an agency holds personal information about them. They almost always want a copy of it. This complicated approach is likely to muddy the waters for many agencies.

**The notifiable privacy breach requirements - how workable are the provisions and would you recommend any changes?**

The notifiable privacy breach framework initially contemplated involved a two tier notification approach. It required the notification of material privacy breaches to the Privacy Commissioner, and of serious privacy breaches (that is, those that may cause harm) to the Commissioner and the affected individuals. Material privacy breaches included breaches that impacted a large number of records or individuals, but may not involve the disclosure of sensitive or detailed information. The current Bill does not follow this two tier approach. Thus, an agency will be
required only to notify privacy breaches that may cause harm. Notification will be to the Commissioner and to affected individuals.

The upshot of this is that the notifiable privacy breach framework is simpler and more workable. By raising the threshold to only those breaches that have caused harm, the Bill reduces a lot of noise that would be created under the two tier framework. Under the current formulation, the Privacy Commissioner will not be inundated with notifications, and agencies will be required to show openness and accountability where it matters most. After all, a key driver of notification is to arm affected individuals with the knowledge they need to protect themselves. If no harm is likely, then the case for notification is greatly weakened. This also aligns more closely with the approach taken overseas (for example in the EU).

Many agencies - including those in the finance and insurance industries - already handle a broad range of reporting and notification regimes. Almost all agencies have already been required to improve the way they manage and notify health and safety breaches. Putting notification itself into practice will not be the difficult part of the process. The key risk for most agencies will be identifying privacy breaches and building a culture where staff will feel safe to alert their managers or properly escalate them. Without an employee base that is empowered to understand what a privacy breach looks like and how they escalate it, an agency will have a very poor picture of their risk exposure and little chance of properly complying with the law.

Agencies may also find the assessment of harm, and therefore the question of threshold, difficult in practice. Agencies today have a hard enough time understanding harm in the context of privacy complaints before the Commissioner. The notifiable privacy breach framework will require agencies to make fast assessments of harm when faced with the facts of an immediate or recent privacy breach. This is likely to result in over-caution and therefore over-reporting. In time, and with clear guidance and assistance from the Commissioner’s Office, this assessment will become easier but any new procedures put in place by agencies will need to accommodate this difficult part of the process and ensure that the right people are involved in the assessment.

How will businesses need to change to comply with the Bill?

As noted above, the Bill does not fundamentally alter the currently privacy framework. Rather, it sharpens the edges. So, current levels of apathy or inertia in respect of privacy cannot continue. At a high level, businesses will need to better resource privacy compliance to ensure that they do not fall foul of many privacy obligations or requirements that have always existed in some form or another. So, perhaps the best advice to businesses is that they will simply need to start caring more about privacy.

What aspects of the Bill do you support?

I support the introduction of mandatory notification of privacy breaches, the new provisions for compliance orders, and clarifying the protections for information sent offshore.
**What significant areas of reform are missing and why should we be concerned about that?**

I would have liked to have seen a new principle prohibiting re-identification of de-identified data (as was recommended by the Law Commission). I understand that that principle might still be in development, and I would like it to eventuate to ensure greater protection of anonymised data.

**Were there any surprises in the Bill?**

I was surprised that provisions for responding to access and correction requests were separated. For example, there are separate provisions for confirming that an agency holds information, for responding to requests to access that information, and then responding to requests to correct information. This seems to be unnecessarily complicated because, to me, the current legislation is pretty clear about what to do with such requests.

**The notifiable privacy breach requirements – how workable are the provisions and would you recommend any changes?**

I’m a little unclear about how it would work in practice. For example, agencies decide themselves, using the legislative criteria, whether a breach is notifiable or not. But the Privacy Commissioner can fine an agency for failing to notify them, and it is not a defence if the agency did not consider the breach to be notifiable when it was reasonable to have done so. I anticipate some confusion as the legislation beds in around understanding the criteria for notifying, and the Commissioner’s office could initially be overwhelmed by reports of all levels of privacy breaches.

**How will businesses need to change to comply with the Bill?**

They need to have a Privacy Officer and privacy policy in place to ensure at least a basic compliance with the legislation. Compliance orders and mandatory breach notification could take some agencies by surprise if they don’t have frameworks ready for educating staff and following good privacy practice.

**What should Privacy Officers be doing right now?**

Making sure that they establish a robust and safe breach reporting culture. Staff need to be reporting anything that might be a privacy breach to the Privacy Officer (or a dedicated central point). Just knowing that they have to tell someone about a privacy incident, even if it’s not technically a breach or might not be notifiable, is the first step. If staff are ignoring or covering up breaches then this could create a risk for the organisation.

---

Katrine Evans, Senior Associate, Hayman Lawyers, Wellington

**What aspects of the Bill do you support?**

It’s fabulous to have a Bill in the House finally! There are some crucial updates in there, and it’s great to see some of the key Law Commission recommendations finally making it to the legislative stage. It’s also good to see that the Bill’s retained the technology-neutral, principle-based approach to the Act – not that I expected it to do otherwise since the Law Commission was so firm about it, but you never know till you see a Bill in print…

Mandatory breach notification and extra protections for export of personal information are pretty high on my cheerleading list. However, it’s probably the new powers for the Commissioner that I’ve been waiting for most. This is because the Act isn’t just a series of individual hot topics like breach notification or information sharing. It’s a system of protection that needs to work as a whole – effectively, in a timely way, and in a way that creates firm but proportionate incentives for organisations to do the right thing.

The new access determination and compliance notice powers should both hit that sweet spot. Access determinations should cut some of the time and complexity out of the existing enforcement system, which will benefit both complainants and agencies. And compliance notices will give new teeth to the Commissioner’s ability to investigate on his own motion, as well as when he’s responding to complaints.

It’s arguable that we need to go further and introduce strong financial penalties for repeat or serious non-compliance, but the Bill represents real progress.

Mind you, we desperately need timely access to appeals as well so that parties have access to appeals or can enforce the Commissioner’s determinations. There are massive delays in the Human Rights Review Tribunal - it takes between two to three years to get to hearing. This isn’t acceptable now, and the problem will be compounded when the new provisions of the Bill kick in. It’s vital that the Tribunal should be adequately resourced to clear its backlog and get ready for the new types of cases coming through.

**What significant areas of reform are missing and why should we be concerned about that?**
It’s really surprising that there’s no mention of the Law Commission’s recommendation that agencies must let people be anonymous or use a pseudonym unless the nature of the transaction requires them to be identified. That recommendation reflects an important aspect of data minimisation, - it would fit perfectly into principle 1. It also reflects sound ethical principles and would be an important up-front protection, particularly in the IoT environment. It’s unclear why the recommendation has not made it into the Bill as it was not controversial. Hopefully the Select Committee can fix it up.

Up the other end of the information lifecycle, there’s nothing in the Bill about re-identification. While prohibitions on re-identification aren’t necessarily effective on their own, they can be a useful part of the information protection system – if nothing else, they enable regulators to take direct action if they catch up with malicious actors.

There’s been no attempt in the Bill to update the public register privacy principles either, which is a real pain. The existing principles haven’t ever been as effective as they needed to be, and the Law Commission did a whole report on public registers (Stage 2 of the review of privacy law). Even a simple reform that the Privacy Commissioner proposed last year would have made a real difference. I’m spending a lot of my time at the moment working on information sharing in the family violence space. If a victim gets a protection order or a harassment order, they can already ask for their details to be suppressed from public registers. But they have to apply separately to each register. That’s seriously difficult for people in traumatic situations, and half the time they don’t know what registers they might be on. Let’s give them a central place to apply for protection, which then gets pushed out to all the Registrars. It would require all the different public agencies that run registers to work together, of course, and someone needs to be responsible for building the system and operating it. Integrated government isn’t always our strong suit, but this is a place where it would pay dividends.

Were there any surprises in the Bill?

I’m bemused by the way in which the Bill treats access and correction requests. There are different provisions depending on whether the person asks whether the agency holds information, or whether they ask for access to information. And there are also separate provisions depending on whether they ask for correction, or for a statement of correction to be attached. I can’t see the value. There’s nothing broken about the provisions now, and the new set-up doesn’t seem to change entitlements or obligations in practice. The Bill just makes it miles harder to read.

The notifiable privacy breach requirements – how workable are the provisions and would you recommend any changes?

There’s probably a little work to do on the breach notification requirements, but they’re shaping up along the right lines. The definitions of ‘privacy breach’ and ‘notifiable privacy breach’ appear reasonably straightforward – the tie-in to the definition of “interference with privacy” is helpful, for instance, as it defines clearly what types of harm you’re talking about.

It’s good that the original decision to have a two tier notification system has gone (one tier of breaches notified only to the Commissioner, and one tier notified to both the Commissioner and affected individual). A single tier will be clearer to understand and operate, and having the main focus on breaches that can cause harm is logical and workable.

Unfortunately, what’s dropped off the radar as a result is the need to notify the Commissioner of large scale breaches, even if the nature of the information means that individuals might not suffer harm – or it’s hard to show what the downstream effects might be. For example, a breach could involve thousands of email addresses and names, but no credit card details or location history or other information that we might consider sensitive or harmful. The Privacy Commissioner at least still needs to be told about that breach.

I’ve never been a fan of having a penalty based on an offence for failure to notify. You need a decent financial penalty for sure, otherwise people don’t take the obligation seriously. But a civil penalty would be far more appropriate. It would apply equally to public and private sector agencies, and it would avoid the heavy-handedness of a criminal sanction (which could lead to over-notification, because of a fear of conviction). It’s also easier to administer: you could deal with it in the Human Rights Review Tribunal which has a civil jurisdiction. There’s a lot more complexity involved in taking a prosecution to obtain a conviction, both evidentially and procedurally. Again, if we don’t make it easy to deal with non-compliance, then the system doesn’t function as it should.

How will businesses need to change to comply with the Bill?

There are probably two key things that businesses need to do as soon as possible to start to move their processes into compliance (if they don’t already). Both are valuable now, regardless of how long the Bill takes to pass – but both will take time and need to be started as soon as possible, so that the agency is prepared for commencement of the legislation.

First, businesses need to know where their breaches are
happening. Set up a central honesty box system so your staff tell you when things go wrong, and think about how else to diagnose your breach problems. You can develop processes and policies and plans as much as you like, but if you don’t know when things go wrong, they’re not going to be worth the paper they’re written on.

Secondly, figure out what information you’re sending offshore, where it’s going and what protections apply to it. Is there a contract in place, and if so what are its terms? Is there a PIA and if not should you do one? If you do a stocktake of the information you’re sending offshore and how it’s governed, you’ll be in a good position to see whether you comply with the law now, as well as seeing whether you’ll meet the new thresholds in principle 11(3)-(6).

**What should Privacy Officers be doing right now?**

Privacy Officers need to analyse as soon as possible how the Bill’s changes are going to affect their own agency, and make sure that any critical changes make their way onto the privacy programme as fast as possible. Some things are going to take time to implement – for example if you don’t know where your breaches are occurring now, then you’re not going to be able to turn that situation around overnight. That means getting senior managers (and, if necessary, the C-suite) over the required changes as soon as possible, particularly any that may need significant change management, people-time or financial investment to implement.
Cities 4.0 – Privacy in the age of Smart Cities

Privacy in the age of Smart Cities. Catchy, right? Well, when I was invited to join my colleague Grace Guinto (of PWC) on a Cities 4.0 panel discussing that very thing, I was a bit stumped. How would I talk about all that worries me about Smart Cities in a room full of people who are excited about building and refining our urban centres so that they are efficient, connected, safe and sustainable?

The premise of the Smart City is that it leverages technology within cities for social good, sustainability, resilience and equity, primarily evident in the foundational sectors of smart cities - from mobility and transportation to health, infrastructure, energy and finance.

In the privacy profession, I have learned that much can be accomplished when privacy becomes a topic of opportunity (rather than a road block). Catching flies with honey, so to speak. In preparing for our panel discussion, which took the form of a casual fireside chat, Grace and I worked out a few questions that (if our audience didn’t move discussion in other directions) may generate a level of post-event privacy assessment in the various groups represented in the room; municipal government, strategy, urban planning, vendor engagement, cyber-security, research and governance.

The best laid plans

The questions we had in mind were as follows:

1. How can privacy officers assist in the roll out of Smart Cities initiatives?

Smart Cities initiatives are all about using the data of our urban environments and our citizens, which necessarily include Personal Information, to make life better – more connected, more accessible, faster, cleaner, safer and sustainable into the future. Privacy concerns associated with these initiatives can be both real/measurable (that is, there is an actual risk) and perceived (that is, there is a worry or a fear within the community). Privacy officers can assist in both identifying these concerns and coordinating targeted information privacy programs in cities in order to address them.

A good privacy program includes – at a minimum:

- having in place a dedicated "chief privacy officer" (or someone similarly named and empowered);
- conducting privacy impact assessments (PIA) when new systems or technologies are proposed;
- rigorous vendor management;
- privacy training for employees; the ability for citizens to access and (if necessary) correct the personal information held about them;
- and a mechanism for citizens to make privacy complaints.

2. If you were to list them, what are your top initiatives that we may see in our Smart Cities that would benefit from a level of privacy caution?

There are a number of initiatives that raise privacy flags, particularly in terms of how citizens may perceive an erosion of their privacy rights. These include:

- Facial recognition points in public locations;
- Free wi-fi in urban centres;
- RFID tags on items in libraries and other public facilities;
- Body-worn cameras for municipal officers (e.g. inspectors and complaint handlers);
- Mobile phone apps that connect users to city services they would otherwise access fairly anonymously (e.g. route planners, transportation services); and
- Drones.

There is an interactive tool published by the Future of Privacy Forum that highlights top privacy concerns associated with Smart Cities. It can be accessed here. It’s pretty neat and does a good job of making privacy concerns digestible. If you are involved in any of the initiatives listed above this is a resource that can assist in crafting a policy to respond to concerns.

“The technology is already here, already being trialled, already part of many urban landscapes”
One thing that isn’t immediately obvious in the Smart Cities context is whether there has been any attention to Privacy by Design principles – that is, designing privacy into all these groovy functionalities and platforms from the outset as opposed to trying to patch privacy holes when they arise in the future. In fact, having discussed this very point with a colleague who leads a strategic engagement team for a top telco, the technology is already here, already being trialled, already part of many urban landscapes. However, unlike the exhaustive PIA processes we have seen for initiatives under the National Identity Security Strategy banner, you’d be hard pressed to find PIA documentation published by cities for their adoption of free urban wi-fi or transportation route planning apps.

However, in the US there are examples such as Seattle, Washington that has made the bulk of its data publicly available to the benefit of other cities here.

3. Do you think that Smart Cities initiatives can adequately address privacy concerns?

YES, assuming that privacy is considered an important touch point from the outset. Tackling privacy early, via Privacy by Design and targeted privacy consultations (particularly with the community), is key!

A strong privacy focus is not necessarily inconsistent with Smart Cities goals. Rather, a good information privacy program will provide a level of quality control as regards the collection and handling of personal information at key junctures. Vendor management will likely become a critical issue as regards data security and data breach notification expectations, as well as maintaining public confidence that the personal information of citizens will not be misused.

An area of privacy risk that has been little discussed but remains critical, is managing citizen access/correction of their own personal information. Citizen rights in this regard may become blurred in the Smart Cities context, especially where there are multiple points of personal information collection, multiple entities involved (cities, local companies and service providers, technology vendors and cloud infrastructure suppliers) and an ever increasing approach to personal information – whether identifiable or not – as capital.

The outcome

Our discussion did meander, by the way. A lot. Still, it was productive and privacy was not the uncomfortable ogre in the room. In fact, the audience was engaged and offered great insight. If you are interested in hearing more and understanding the various issues raised, Alan Mihalic, a cyber security consultant who focuses on Security by Design in physical spaces (e.g., our buildings), filmed the entire session for the Smart Tribes network. It can be accessed here.

Some take-aways from the day:

First, those in the audience, who represented a diverse group of stakeholders, really responded to the notion of having a person responsible for privacy with whom they could consult on Smart Cities initiatives.

Second, consultation is not a problem for cities in the development process. The attention currently being paid to cyber-security is evidence of this. It is possible that to date privacy has either:

1. not been seen as a critical touch stone for cities in their development and adoption of Smart Cities initiatives; or
2. it is seen as a potential drag on progress. That is, with technologies ready to be deployed now, there is no time to waste!

It is apparent that approach is about to change.

Finally, old-school views about privacy (e.g. the right to be left alone, the right to engage in society with a degree of anonymity) do not necessarily align with perceptions of the modern generation’s approach to privacy. Prolific use of social media and the sharing of personal information to receive a service or a benefit (e.g. online shopping) suggests that many people are happy to supply their personal information in circumstances where they feel they are exercising

“Citizen rights... may become blurred in the Smart Cities context, especially where there [is an]... ever increasing approach to personal information – whether identifiable or not – as capital.”

While compiling this piece for the iappANZ, it was timely to read a LinkedIn article published by ANZSOG (Australia and New Zealand School of Government) featuring Professor Genevieve Bell. The article referred to her presentation at the recent **Breaking The Data Silos conference** in Canberra. A resonating message for me was Professor Bell’s assertion that “[c]onsumerism has a very different endpoint to citizenship and there is something about the intermingling of those endpoints those narratives that makes it easier to violate trust.”

Indeed. Smart Cities, listen up! The time for embedding privacy and considering in a new and different light the balancing of technology and the rights of citizens is upon us.

Nicole Stephensen is a Privacy Specialist with extensive local and international experience in operational and strategic privacy matters. She is Principal Consultant at Ground Up Consulting, a boutique firm she established in 2011. Nicole is a member of the IAPP, as well as iappANZ where she sat for three consecutive terms on the Board.
A recent article by Anna Johnston, about a privacy case in relation to location data collected as part of the NSW Opal Card system, highlights the dangers of over collection of personal information, particularly in relation to ‘smart’ devices.

An unrepresented individual, Mr Waters, brought a case against Transport for NSW (TfNSW), arguing successfully that its collection of the history of his movements on public transport was unlawful.

In NSW some passengers entitled to a concession fare, such as pensioners and seniors, are required to register their Opal Card. Registration of a card means that the card itself is linked to an identifiable individual. By contrast passengers paying full fare do not need to register their cards, and can travel anonymously.

Mr Waters did not object to the collection of information about his identity, or the processes by which he had to demonstrate his eligibility for a concession rate. But he did object to the by-product of registration – the creation of a record of his physical movements when using public transport, linked to his identity via the Card number. (The physical movements of all cards are tracked and the data can be easily interrogated; but only if the card is registered can TfNSW link that card’s use back to the identifiable individual assumed to be using that card.)

In other words, Mr Waters objected to the fact that some passengers could choose to use public transport anonymously – i.e. without their physical movements as identifiable individuals being tracked by an arm of the State Government – but others could not.

The NSW Civil and Administrative Tribunal agreed with Mr Waters, finding that the collection of the travel history data was not reasonably necessary “for the stated purpose of enforcement/eligibility for the entitlement to the concession card”.

The Tribunal found that TfNSW had therefore breached Information Protection Principle 1 in its design of the Opal Card system, and ordered TfNSW to stop collecting Mr Waters’ travel history data. It also noted that the same result would apply to other concession card holders, and thus suggested that TfNSW take legal, privacy and technical advice on how best to re-design the Opal Card system to make it compliant.

The full article can be found on the Salinger Privacy blog here.

Anna Johnston is a Director at Salinger Privacy. Salinger Privacy offers privacy consulting services, compliance training, and a range of publications including a free Privacy Officer’s Handbook, template policies and procedures, checklists and eBooks. Find out more or sign up for their monthly newsletter at www.salingerprivacy.com.au
Recently a friend of mine fell out of favour with some of the parents at her daughter’s school. There was a moment of standing toe-to-toe in the playground, supporters evenly divided, before she was able to elicit a promise from the parent in question to “remove my child’s photos” from a recent social media post.

Let’s set the scene: we’re on a school excursion to the museum. Parent “helpers” are invited along as part of the containment strategy for the bouncing, giggling, sticky-fingered packs of eager first graders. The museum guides are guiding. The teachers are teaching. And the parents… they are taking photos of the whole event on their smartphones.

In the evening, after the kids are tucked into bed, the parents scroll through their favourite photos from the museum trip… and post the best of them (i.e., the ones involving their kids looking studious and adorable) to social media for friends, family, and other school families in their circle to see.

The next morning at school drop-off, my friend hears a chuckled comment from a parent she barely knows about a photo of her daughter circulating on social media – she with her delighted gappy-toothed grin after accidentally soaking herself at the museum’s water fountain. Say what?! You know the rest…

In this case, there wasn’t a concern about child or family safety – like in instances where details gleaned from a photo can place a child or their family at risk of domestic violence. My friend was just concerned about privacy; particularly, that the happy-snapping parent hadn’t asked her first before placing her daughter’s photo online for the wider (and unknown to her) community to see.

The photos were taken on a school excursion, during school hours, capturing school kids doing school-related things. Schools are supposed to have policies and procedures relating to when, how and with-what-restrictions photos are taken and published of children in their care. Indeed, my friend had clearly stated to the school (on the requisite “media usage consent form”) that her daughter’s photos must never be published on the school’s website or social media feeds.

But here’s the thing: when it’s not the school taking the photos, and it’s not the school’s social media feeds we are talking about, the rules (and, indeed, individual sensitivities about when it is appropriate to be photographing kids) are muddied a bit. I would argue, however, that schools have a continued role to play in 1. ensuring the privacy of their students and 2. ensuring that parents have good information at their disposal to help them make responsible decisions when dealing with photos of kids.

When it’s “on their watch”, schools must be vigilant about upholding privacy obligations around the taking and publishing of images of children:

Photos that identify (or could lead to the identification of) children are ‘personal information’ under Australian privacy law – not just the Commonwealth Privacy Act 1988 (to which private schools are bound), but also State and Territory privacy laws (which regulate the personal information handling practices of public, state-funded schools). This means that there are rules attached to how images of children are handled and that schools risk breaching student privacy if they fail to follow those rules.

Applying rules

Many schools have access to clear policy and procedural advice, as long as they know where to find it. In Victoria, for example, the Department of Education supplies
Policy advice around image privacy for state schools, with bodies such as Independent Schools Victoria providing similar guidance to the independent school sector. There is also directly-from-the-horse’s-mouth guidance available from the various privacy regulators.

Where parents or other community members are recruited to help during school events, the school’s attention to privacy requirements mustn’t slip. Schools should actively communicate to the P&C Association, other volunteer groups, on-site after school care providers and parents exactly what the school’s expectations are in relation to the taking, keeping/storing, using and publication of photos.

In my friend’s case, perhaps a pre-excursion reminder bulletin (or even a quiet word) to all parent “helpers” about the school’s policy for taking photos would have prevented the uncomfortable playground exchange the next day. Equally important, the same reminder bulletin would have clearly demonstrated the school’s awareness of, and commitment to, its privacy obligations when conducting on- and off-campus student events.

In today’s technology-driven world, schools could also consider implementing automated systems where photos of students are gathered and managed in one secure place and subject to the specific consents (or restrictions) parents have placed on what happens to the images of their children. Before doing this, however, the school should check the privacy credentials of the technology or platform they choose.

In my friend’s case, and in conjunction with the pre-excursion reminder bulletin about privacy… if the school had a process whereby all parent “helpers” could supply/upload the photos they had taken at the museum directly to the school, then the school would have had the ability to manage those photos in accordance with the school’s media usage policy.

Schools should spend time educating parents and community members

No matter what the schools do at school, there is still a need to address the extent to which parents should post photos of their kids (and other people’s kids!) online. Schools have more resources at their disposal than just their own local policies and procedures; and, where appropriate, they should use them to help educate their community.

From time to time, concise and well-packaged information becomes available through Australian Government websites in relation to posting images of children and young people online – see, for example, the Office of the eSafety Commissioner or the Australian Institute of Family Studies. Similarly, Australia’s mainstream news media may publish a useful article about privacy that touches on the key messages parents ought to receive.

A well-placed regular link in the school’s newsletter may be just what’s needed to get parents talking about when it is (or isn’t) cool to post the photos of children online.

^ Blog article (29.08.2017) re-printed with permission.
On 15 March 2018 Svitzer Australia, a national towage services company notified the Office of the Australian Information Commissioner (OAIC) of a data breach under the new mandatory data breach notification laws.

The facts, as reported in news media, are that between May 2017 and March 2018, for a period of almost 11 months emails from three employee email accounts in the finance, payroll and operations departments were hacked, with approximately 50,000-60,000 emails being maliciously on-forwarded to external locations outside the business. Those emails were said to include personal information of about 500 of Svitzer Australia’s 1,000 Australian employees. Investigations are currently being undertaken.

The emails contained information on employees including tax file numbers, next of kin details, and superannuation account information, as reported by the ABC.

The company said it had stopped the auto-forwarding after becoming aware of the issue on 1 March 2018. The report to the OAIC occurred 14 days later.

“This is a reminder of the constant threat individuals and businesses alike face,” Svizter Australia managing director Steffen Risager said in a statement.

The company sent a notice to employees via their union, the Maritime Union of Australia on the following terms:

“Since becoming aware of this incident, Svitzer Australia has taken the following actions:

- We engaged advisers, including forensic experts, to assist with identifying the extent of the data theft, and to conduct a comprehensive investigation.

- We made an urgent application to the Federal Court of Australia to block further access to the account through the provider. This process was successful and served this morning.

- We notified the Office of the Australia Information Commissioner and are working with it in relation to this incident.

Svitzer Australia takes employee privacy very seriously. We are taking all necessary steps to ensure we support those affected. We want to make it clear that as part of the investigation, and consistent with company policy, no emails have been read by anyone in Svitzer Australia, including management. The investigation is being undertaken by specialist lawyers. Svitzer Australia email accounts are safe to use. Furthermore, the forensic investigation has determined that no other Svitzer applications or systems have been compromised. Since November 2017, all Svitzer systems and servers have been hardened and multi-level authentication access processes have been applied, effectively minimising the risk of similar unauthorised access going forward.”

Svitzer also confirmed through the union that it was taking the following action:

- A letter to employees will be sent out
- A letter to the maritime unions will be sent out
- Employees that have been directly affected by the leak will be contacted personally and informed what details of theirs has been leaked.
- No emails that are part of the 50000 bundle of leaked emails will be read by management and will only be sited by the forensic IT company to determine all personal information that has been leaked is identified so those affected can be informed
- The ATO has been briefed and employees who have had their TFN leaked will be asked to contact the ATO to discuss how their personal situation will be managed.
- Svitzer has set up a team in HR to deal with working through each employee’s requirements to ensure identity theft is managed post haste
- A web site has been set up for all employees to access updates and relevant information. http://www.svitzeronlinehelp.com

Svitzer also advised that they will continue to work with the union and implement all reasonable measures to protect employee’s private information.

But these were employee records – aren’t they exempt from the Privacy Act?

It is well established that the Privacy Act 1988 (Privacy Act) contains an exemption whereby the handling of personal information by a private sector employer

Privacy Unbound | 26
does not trigger the application of the *Privacy Act* if it directly relates to an employee’s current or former employment relationship. The exemption applies to information relating to the employment relationship as between the employer and employee. The framing of the exemption in section 7B(3) is that

An act done, or practice engaged in, by an organisation that is or was an employer of an individual, is exempt for the purposes of paragraph 7(1)(ee) if the act or practice is directly related to:

(a) a current or former employment relationship between the employer and the individual; and

(b) an employee record held by the organisation and relating to the individual.

Accordingly, it is not a blanket exemption and the question of whether employee records are exempt from the reach of notifiable data breaches is less clear. If information about the employment relationship is subject to unauthorised access then surely the Privacy Act applies?

An affected employee could well argue that while the employee records exemption might limit their rights to access and correction, the obligation under Australian Privacy Principle 11 to take all reasonable steps to keep information secure remains applicable to the information.

Although, there is uncertainty as to whether an unauthorised disclosure of information retained in employee records alone triggers the new disclosure obligation, the Svitzer case shows that in a practical sense an organisation can’t treat employee records differently.

**Have other breaches been notified?**

The breach is the first to be made public since the mandatory notification scheme came into force last month.

However, the OAIC said at the time of the Svitzer breach that it has received 31 notifications in the first three weeks of the scheme being in operation.

It will release information on the notices it receives each quarter. The first publication of breach notices is expected in early April.

An OAIC spokesperson said the office would assess the information provided by Svitzer and decide whether any further action was required.

As at the date of writing this article that publication by the OAIC has not yet occurred.

It will be of interest to see the level of detail provided. Many security specialists have stated that if organisations shared information about security breaches then it would assist in shutting down criminal activity as shared information could be used to plan to defend against known attack methods. Where methods are discovered organisation by organisation, there is no opportunity to plan for this, but merely to be reactionary.

**What can we learn from Svitzer?**

Apart from the risk of business disruption, loss of faith by employees, customers and service providers, and potential claims by those affected, businesses operating in Australia now face significant penalties if they don’t have in place sufficient systems to prevent, detect and report on data breaches.

Despite the employee records exemption, the nature of information held about employees is often of a nature that can give rise to significant harm if breached e.g. identity theft, financial loss and embarrassment due to sensitive information. The obligation to keep information secure remains key.

The UK class action case by aggrieved employees reported in the last edition of Privacy Unbound, Morrison’s, cannot be discounted as a possible outcome for Australian employers.

It also noted that the primary point of the new mandatory breach notification scheme was to ensure affected individuals were notified of a breach of their personal information. Svitzer’s published actions indicate it has taken all of the steps to contain the damage and mitigate any harm by assisting affected individuals.

While it is clear that third party malicious actors were involved in this breach, organisations need to be prepared for this eventuality.

The facts as reported support the statistics that breaches are often ongoing, or have occurred well before they are discovered. In this case Svitzer managed to investigate and be in a position to report within 14 days, well inside the 30 days in the new regime.

It is clear from the media reports that this breach has been costly in terms of both management time and third party expenses, and this again highlights the benefits, including the cost benefit, of having a breach plan in place and having a team ready.
As at 6 April 2018, the two bills amending the Privacy Act 1988 (Cth) have progressed as follows:

1. **Intelligence Services Amendment (Establishment of the Australian Signals Directorate) Bill 2018 [CTH]**

   The second and third reading were agreed to and subsequently passed by the House of Representatives on 28 February 2018. Public submissions to the Bill closed on 9 March 2018. In the Senate, the Bill was introduced and the second reading moved on 19 March 2018. The report from the Senate Standing Committee on Foreign Affairs, Defence and Trade was released on 21 March 2018. The Bill’s second and third reading were agreed to and passed by the Senate on 28 March 2018. The Bill is currently awaiting assent.

2. **National Consumer Credit Protection Amendment (Mandatory Comprehensive Credit Reporting) Bill 2018 [CTH] (Draft)**

   The Bill was introduced to the House of Representatives and the second reading moved on 28 March 2018. On the same day, the Bill was referred to the Senate Economics Legislation Committee for inquiry. The subsequent report from the Committee is to be released on 29 May 2018.
GDPR in Action: Practical perspectives on GDPR compliance – Auckland

Date: 11 April 2018
Time: 7am – 9am
Venue: The Maritime Room, Maritime Museum, corner Quay and Hobson Street, Auckland, New Zealand

A fire-side chat with NZ Privacy Commissioner John Edwards about the Privacy Bill and other recent events - Auckland

Date: 7 May 2018
Time: Lunch
Venue: Auckland

OPC Privacy Forum – Wellington

Date: 9 May 2018
Time: all day
Venue: Wellington

More details at privacy.org.nz

Privacy Awareness Week Events

We will be holding PAW events in Sydney, Melbourne and Brisbane on 15 May and Adelaide on 16 May.

More details will be available shortly on iappANZ.org

2018 iappANZ Summit

Date: 1-2 November 2018
Time: 8am – 5pm
Venue: ZINC @ Federation Square, Melbourne, Australia