## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>PRESIDENT’S FOREWORD</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>COMPREHENSIVE CREDIT REPORTING: ONCE ILLEGAL, SOON TO BE COMPULSORY</td>
<td>Patrick Dwyer</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>MANDATORY DATA BREACH NOTIFICATION OUR TOP TIPS, THREE MONTHS OUT</td>
<td>Melanie Marks</td>
<td>6</td>
</tr>
<tr>
<td>4</td>
<td>PREVENTING &amp; RESPONDING TO DATA BREACHES</td>
<td>Anna Johnson</td>
<td>8</td>
</tr>
<tr>
<td>5</td>
<td>DOES THE EQUIFAX INC BREACH HAVE IMPLICATIONS FOR AUSTRALIAN COMPANIES?</td>
<td>Lyn Nicholson</td>
<td>11</td>
</tr>
<tr>
<td>6</td>
<td>ARTIFICIAL INTELLIGENCE IN HEALTHCARE</td>
<td>Daimhin Warner</td>
<td>14</td>
</tr>
<tr>
<td>7</td>
<td>HEAD TO HEAD: THE GDPR AND THE AUSTRALIAN PRIVACY PRINCIPLES</td>
<td>Tim de Sousa &amp; Veronica Scott</td>
<td>16</td>
</tr>
<tr>
<td>8</td>
<td>PROFILE – JACQUELINE PEACE</td>
<td></td>
<td>24</td>
</tr>
</tbody>
</table>

---

**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 (http://www.iappanz.org/)

If you have content that you would like to submit for publication, please contact the 2017 Editors:

Veronica Scott (veronica.scott@minterellison.com), Carolyn Lidgerwood (carolyn.lidgerwood@riotinto.com) Katherine Gibson (katherine@gibsonlaw.co.nz)

Stay tuned for new Journal advisory committee contacts in 2018. This is the last issue with Veronica and Carolyn at the helm – who thank all contributors to Privacy Unbound over the past few years.

Please note that none of the content published in the Journal should be taken as legal or any other professional advice.
Welcome to the final edition of *Privacy Unbound* for the year.

As many of us working in the field would attest to, it is a lucky time to be a privacy professional. The industry is experiencing unprecedented growth now because of regulatory and commercial pressures onshore and overseas including:

- The Australian public sector is going through enormous uplift with a new Privacy Code introducing the need for every organisation to have a Privacy Officer, a Privacy Champion at executive level and a fully resourced program;
- The introduction of mandatory breach reporting in Australia from February 2018, necessitating policy and process improvements in the way Australian entities secure information and deal with incidents;
- A new Privacy Bill being drafted in New Zealand along with the recent advice from the Privacy Commissioner that there is an urgent need for privacy reform; and
- Internationally, the GDPR, which will from May 2018 require many organisations handling the data of European residents to have a Data Protection Officer and implement a fully resourced privacy program.

Perhaps unsurprisingly, there is a major shortage of privacy people globally (for example, the IAPP estimates that 70,000 DPOs will be needed from next year). The IAPP has seen extraordinary growth of its membership base to 30,000 in the last year, driven substantially by growth in Europe to prepare for the GDPR. (These stats and more are covered in the [IAPP-EY Annual Privacy Governance Report 2017](https://www.iapp.org/)).

One of our key objectives in 2018 is to support this international trend by growing our organisation and the profession in Australia and New Zealand over the coming year. We look forward to partnering with our members, sponsors and supporters to achieve this goal through events, certification and other resource offerings. With the early election of the Board this year, we are off to a flying start with these deliverables.

Events planning for next year is well underway. Stay tuned for the imminent release of our calendar of events for January to June 2018 – including leading speakers, diverse panels and social opportunities across all major cities in Australia and New Zealand.

Advisory committees have been established under the leadership of the following Chairs:

- Events (Australia) – Chris Rogers and Bronwyn Furse
- Events (New Zealand) – Daimhin Warner, Jacqui Peace and Emma Pond
- Certification – Carolyn Lidgerwood and Daimhin Warner
- Membership – Marina Yastreboff
- Journal and publications – Lyn Nicholson and Katherine Gibson
- Summit 2018 – Tim de Sousa and Kate Monckton

Joining an advisory committee is a great way to connect into the iappANZ network and contribute to our community and can be a stepping stone to successful Board election. If you would like to join an advisory committee for 2018, please contact our General Manager, Julie at julie@iappanz.org.

As announced at the Summit, we will be introducing a certification for privacy professionals in Australia and New Zealand next year (CIPP-ANZ). Our Certification advisory committee is working with the IAPP on the exam and we are now preparing to develop course content to support members in preparing for the exam. If you’d like to register interest in being part of the first cohort to attain CIPP-ANZ certification later in 2018, contact our General Manager, Julie at julie@iappanz.org.

Finally, on behalf of our editors, thank you to all writers who have been published in *Privacy Unbound* this year. We will announce the winner of our annual writing prize before the end of the year.

I’d like to wish you a happy and safe festive season and look forward to connecting with you in the new year.

*Melanie Marks*
In 1988, Australia’s main credit reporting body, the Credit Reference Association of Australia (CRAA), announced its intention to extend the credit information collected by the CRAA to include more comprehensive information about individuals’ total credit commitments. At the time it was called “positive reporting”.

Privacy concerns were raised. The Federal Minister for Consumer Affairs, Senator Nick Bolkus, asked the CRAA to put its plans on hold. And then in 1990 the Minister introduced the Privacy Amendment Bill to ban positive reporting in relation to consumer credit.

In his Second Reading Speech on the Bill, Senator Bolkus said that positive reporting represented an “unwarranted intrusion” into individuals’ lives and that the Government “did not consider that there is any proven substantial benefit from the positive reporting proposals. In view of the strong privacy concerns held by the community this massive expansion of the extent of information held about individuals should not be allowed to develop.”

The Bill was enacted as the Privacy Amendment Act, and introduced a new Part IIIA into the Privacy Act.

There was no prior consultation with industry about the legislation. It was a policy making debacle, and Part IIIA had to be amended a number of times before it became commercially workable.

Although Part IIIA banned positive reporting for consumer credit, the credit industry continued to argue the case for more comprehensive credit reporting information.

When the Wallis Financial System Inquiry considered the matter in its 1997 report, it was unable to conclude whether the benefits of positive credit reporting outweighed the costs, but recommended that a working party be established to review the credit provisions of the Privacy Act.

The turning point was the Australian Law Reform Commission’s 2008 report on the Privacy Act, For Your Information: Australian Privacy Law and Practice (ALRC Report 108). The ALRC accepted that making more information available to credit providers would tend to increase efficiency in the market for credit, assist in making credit more available to those able to repay, and reduce rates of default.

The ALRC recommendations for comprehensive credit reporting (CCR) were adopted in the 2014 amendments to the Privacy Act. The amendments allowed credit reporting bodies to collect and disclose “consumer credit liability information” and “repayment history information”. Consumer credit liability information (CCLI) includes the name of the credit provider, whether it is a licensee, the type of consumer credit, the start and end dates of the credit, the repayment terms and the credit limit. Repayment history information (RHI) includes whether an individual has met a monthly payment obligation, the due date, and the date when payment is made.

“It is ironic that almost 30 years after the Federal Government stepped in to ban comprehensive credit reporting (CCR), it is now proceeding with legislation that will make it compulsory …. The history of CCR in Australia is a case study in the challenges and limitations of top-down approaches to privacy regulation”.

By: Patrick Dwyer
However the amended Privacy Act only permits a credit provider to disclose RHI to a credit reporting body if it holds an Australian credit licence, and only allows a credit reporting body to disclose RHI to a credit licensee. What’s more, RHI may be disclosed by a credit provider to a credit reporting body only if the consumer credit to which the RHI relates has been consumer credit for which CCLI has been previously disclosed to the credit reporting body.

The Privacy Act amendments did not make CCR mandatory, and the credit industry sought to avoid a “free rider” situation where some credit providers might use CCLI and RHI disclosed by other credit providers without also contributing such information to the credit reporting body. The Australian Retail Credit Association developed its Principles of Reciprocity and Data Exchange (PRDE) and obtained authorisation from the Australian Competition and Consumer Commission for the PRDE.

Introduced in December 2015, the PRDE created tier levels of credit information and essentially required signatories to the PRDE to contribute information to the same level as their use. It was intended to incentivise credit providers to participate in CCR, but the take-up of CCR has been very slow to date.

Various reasons have been given for the limited voluntary adoption of CCR, including technology challenges and uncertainties about the application of some of the CCR concepts, particularly in relation to hardship arrangements. More broadly, for major credit providers, the net benefits might not be seen as greater than the initial costs to participate.

In the report of its inquiry into Data Availability and Use released in May 2017, the Productivity Commission recommended that the Australian Government adopt a minimum target for voluntary participation in CCR of 40% of all active credit accounts provided by licensed credit providers and that if this target was not achieved by 30 June 2017, the Government should circulate draft legislation to impose mandatory participation in CCR by licensed credit providers in 2018.

The Government accepted this recommendation and announced in the May 2017 Budget that it would make CCR compulsory if credit providers did not meet a threshold of 40% data reporting by the end of 2017.

The Budget statement did not seem to have any encouragement for the industry, and so on 2 November 2017 the Treasurer Scott Morrison announced that the Federal Government would legislate for a mandatory CCR regime to come into effect by 1 July 2018. According to the Minister, CCR will result in greater lending competition and also better access to finance for Australian households and small businesses.

The Federal Government proposes a phased introduction of CCR. The four major banks will be required to have 50% of their credit data ready for reporting by 1 July 2018, increasing to 100% by 1 July 2019. Because the big four banks account for approximately 80% of consumer lending, the Government believes that this will create a critical mass of participating credit providers, while giving smaller credit providers additional time to develop their systems for CCR. The other details of the mandatory CCR regime are yet to be worked out.

It is ironic that almost 30 years after the Federal Government stepped in to ban CCR, it is now proceeding with legislation that will make it compulsory. Perhaps if it had left the industry alone to develop its own CCR regime organically over time, we would have had the benefits of CCR many years earlier. The history of CCR in Australia is a case study in the challenges and limitations of top-down approaches to privacy regulation.
Mandatory Data Breach Notification – Our Top Tips, Three Months Out

By: Melanie Marks

There are approximately three months to go until your Australian organisation or agency will have to “fess up” if it experiences a serious data breach. While this article is directed at Australian entities, it also provides some guidelines and tips for managing data breaches generally, including across the Tasman.

As a privacy leader in your organisation, you should be deeply entrenched in looking at your processes and procedures for managing data breaches and assessing and ensuring your organisation’s capability to respond to them.

Preparedness will help you and your team to minimise stress and assist you to meet the short timeframes imposed by the new laws. You do not want to find yourself researching your obligations for the first time when faced with a notifiable data breach. The OAIC has stated that organisations “will need to be prepared to conduct quick assessments of suspected data breaches to determine if they are likely to result in serious harm”.

But for those who have not yet started - and we aren’t asking you to “fess up” to that one - it is not too late. Here are our top tips to get underway and be ready for the commencement of the obligation on 22 February 2018:

1. Read the OAIC’s resources and watch the OAIC NDB webinar (available for download here). The OAIC has stated that the finalisation of all its resources is imminent so keep watching that space.

2. Develop your data breach response plan. Having a data breach response plan is part of establishing robust and effective privacy procedures and will assist you to meet your obligations under APP 1.2 and APP 11. The data breach response plan is a practical, step by step guide on what to do, tailored for your organisation.

3. Understand the roles they will play and the actions they will need to take in the event of a privacy breach (whether notifiable or not). Then, prepare a RACI chart and ensure everyone has a copy of it. A list of phone numbers along with the RACI will help you to pull your response team together quickly.

4. Practice, practice, practice. Schedule your first simulated privacy incident in December/January. You may think this is not a good time to undertake a simulation because your staff are busy or on leave, but these factors make it a perfect time to simulate some of the challenges you may face when real incidents occur. In the longer term, look to complete 3-4 simulations per year.

5. Implement learnings from your simulations into your data breach response plan and RACI. Practicing is the best way to iron out organisational and process inefficiencies.

Key aspects of the law:

- **Threshold:** A notifiable data breach will occur where there is unauthorised access to, or unauthorised disclosure of, the information and “a reasonable person” would believe that such data breach is “likely to be result in serious harm” to any of the relevant individuals. A breach will also be notifiable if the information is lost in circumstances where it is likely to lead to unauthorised access or disclosure with serious harm to the relevant individuals a likely result.

- **Timing:** APP entities will be required to notify an eligible data breach as soon as practicable after becoming aware of it or if there are reasonable grounds to believe that there has been an eligible data breach. If they suspect a breach has occurred, APP entities must take reasonable steps to
complete, within 30 days, a “reasonable and expeditious assessment” of whether an eligible data breach has occurred.

- **Who must be notified?** APP entities will be required to notify the Australian Information Commissioner and each of the relevant individuals affected by the breach. Where it is not practicable to communicate with each of the affected individuals, the entity must publish a statement on its website or take reasonable steps to publicise it.

- **Penalties for non-compliance:** Failure to comply with the key provisions of the law is an interference of privacy under the Privacy Act. Serious or repeated interferences with the privacy of an individual attract a maximum penalty of 2,000 penalty units for individuals ($420,000) and 10,000 penalty units for bodies corporate ($2.1 million).

- **Remedial action to overcome reporting obligation:** Notification is not required if the entity takes action in relation to the loss of information or the unauthorised access or disclosure before serious harm to affected individuals has resulted and a reasonable person would conclude that serious harm to those individuals is no longer likely to occur.

- **Importance of securing information:** Effective security measures can mitigate the obligation to notify when information is lost. The law sets out a list of relevant factors in determining whether access or disclosure is likely to result in serious harm, including what security technology has been used to protect the information and the likelihood of interference.

- **The reporting obligation is not retrospective:** It will apply to breaches occurring after the date of commencement.
"We take your privacy seriously"

Not since the advent of electronic banking finally rendered obsolete the laughable phrase “your cheque is in the mail” has there been a phrase which is more likely to induce me to – depending on my mood – engage in exaggerated eye-rolling, mutter rude things under my breath, or simply shout “liar liar pants on fire”!

News that hackers stole information about 50 million Uber passengers (and 7 million drivers) from around the globe has put data breaches – and their repercussions – squarely on the front page.

What is particularly galling about the Uber example was not just the failure of information security, but the immoral corporate behaviour that followed. Instead of telling their customers or drivers (or indeed privacy regulators), Uber hid the news for a year, and paid off the hackers $100,000 to keep quiet. If you thought the job of the privacy and security team is to keep things quiet in order to protect the firm’s reputation, you would be wrong. Uber has now sacked its chief security officer and one of his deputies, for failing to properly disclose news of the data breach. Privacy regulators around the world are now asking questions.

How does this stuff happen? I don’t mean ‘how did the hackers get the data?’ I mean: Why are incredibly wealthy and powerful companies getting away with treating our personal information so shabbily that we are exposed to risk in the first place?

As security researcher and blogger Troy Hunt argues, there has been minimal accountability for data breaches because there has not been enough of a financial disincentive for companies to truly care about privacy and security. Until now.

The consequences of a data breach will get much, much more serious in 2018. Here in Australia, our notifiable data breaches scheme kicks off in February, with maximum civil penalties of A$2.1M for a failure to properly follow the notification requirements. Then in May the GDPR commences, with its seriously hefty fines of up to €20M, or 4% of a company’s annual global turnover, whichever is the greater. Even though it is European data protection law, its reach can extend to Australian organisations.

Things are ramping up in the US too. A failure to notify the appropriate regulator and affected individuals within the specific timeframe landed an Illinois surgery in hot water earlier this year. For delayed reporting on the loss of hard copy records about 836 patients, the US Department of Health and Human Services levied its first fine - of US$475,000 - for non-compliance with data breach notification requirements.

Of course, fines from privacy regulators are not the only cost incurred for a company dealing with the fallout from a data breach. Following an incident earlier this year in which the personal information of more than 145 million people in the US and the UK was potentially exposed, the credit bureau Equifax lost $87.5m in the first quarter after the breach. That cost included legal and consulting fees, as well as costs related to the services offered to people whose data was compromised. Its quarterly profits also dropped by 27%. (And, importantly, in the wake of the Equifax breach, lawmakers in the US are finally talking seriously about the need for broad-based data protection legislation. Hurrah!)

“…. there has been minimal accountability for data breaches because there has not been enough of a financial disincentive for companies to truly care about privacy and security. Until now”.  

Meanwhile Target’s 2013 data breach, in which hackers were able to steal information about 40 million credit and debit cards used by customers in its stores, had cost it a staggering US$202M by May 2017 - with a consumer class action still outstanding.

So what might cause the kind of data breaches which, come 2018, will need to be notified?
Leaving aside examples of malicious hacking and deliberate misconduct by disgruntled employees, let’s review a few other scenarios, which are disturbingly common:

- Putting databases or backups on a publicly-facing website. This was the cause of the Red Cross data breach affecting more than 1M people in Australia, the Capgemini leak of Michael Page recruitment data, as well as the leak of more than 43,000 pathology reports in India, and the personal information about more than 198 million American voters from the Republican National Committee.

- Leaving unsecured AWS ‘buckets’ of data in the cloud. This has happened most recently to the ABC, as well as Accenture, Viacom and a recruitment company holding data on military veterans and others holding security clearances. Plus to a contractor holding staff records from AMP, the Department of Finance, the Australian Electoral Commission and others.

- Allowing sensitive data to be stored on unencrypted mobile devices. A paediatric hospital in Texas, contrary to prior security advice, failed to deploy encryption or other measures on all of its mobile computing devices. So no surprise when a staff member left behind at an international airport an unencrypted non-password protected BlackBerry, containing the electronic health records of 3,800 patients. Still not learning the importance of information security, a few years later the same hospital suffered the theft of an unencrypted laptop from an unsecured work area; the laptop contained the electronic health records of 2,462 individuals. The hospital was fined US$3.2M for the two instances providing evidence of their failure to comply with data security rules.

(And if those examples of insecure electronic health records from the US scare you, don’t imagine that things are magically any better here. The Chief Information Security Officer of the Australian Digital Health Agency, the agency charged with implementing the My Health Record, said of GP clinics here: “they’re going to be sitting on a Windows XP machine that has vulnerabilities up the kazoo”.)

So, dear privacy and infosec professionals, I hope you are already mentally creating your list of ‘things I need to check that our organisation doesn’t do’.

But that’s not all of it. Preventing data breaches is not just about the tech. It’s about people. *All* of your people. It’s about the things that you do do.

Because just like US President Trump leaving the key in a classified lock-bag in the presence of non-security-cleared people, we all have our bad days. (Hands up anyone who has ever accidentally emailed something to the wrong person.) Research from both the UK and the US suggest that human frailties – ignorance, laziness, carelessness – are the root cause of more than half of all data breaches.

So here’s some more, sadly common, examples:

- Failing to properly redact government documents before their public release. This year’s examples alone include the accidental publication of the private mobile phone numbers of hundreds of federal politicians, former prime ministers and senior political staffers; the publication by Comcare of the personal details of an injured worker; and the publication of information contained in hundreds of confidential submissions from families of children who have self-harmed and been the victims of bullying.

- Mishandling the mailout or other transmission of records. There have been examples from Victoria of posting confidential children’s court records to a violent family member; or in NSW where 2,693 photo ID cards, including driver licences and gun licences, were sent to the wrong people.

- Poor disposal of paper records. Examples include the medical letters about more than 1,400 public and private patients found in a public bin in Sydney after being dumped by a contracted transcription service provider; or the private hospital medical records found lying in the street in Victoria.

- Leaving a laptop in a parked car. This happened to a company providing mobile monitoring of patients with cardiovascular disease. When the employee’s laptop, containing health information about 1,391 patients, was stolen from their parked car, the company was fined US$2.5M.

So what’s a privacy officer to do?

The privacy team should be working hand-in-hand with the information security team, to prevent data breaches. The privacy messages to staff need to include: don’t collect more personal information than we need; only keep it for as long as we genuinely need it; and don’t use it for secondary purposes without permission. The less personal information you hold, the less risk you need to manage for.

(And yes, sometimes that means saying to the CEO or venture capitalists: No, we should not be collecting intrusive location data about our customers – or, you know, littering the streets with dockless share bikes - just because we might find a way to monetise our customers’ personal information later on.)
You also need to embed a culture of good data security, at every level in the organisation. Obviously you need good policies and procedures, and visible enforcement of those policies and procedures. But it’s more than that: staff need training. And reminders. And more training. And more reminders. And then you can make sure that your tech is delivering on your security promises. (For one example of data loss prevention tech, see the White Paper on data classification we wrote for our client janusNET.)

Oh, and don’t forget your contractors: third party involvement can be the weakest link in the security chain. A study of data breaches by the Ponemon Institute and IBM found that third-party involvement was the top ranking factor that led to an increase in the cost of a data breach. A recent example: customer data leaked from a supplier to Domino’s Pizza. And another: the leaking of data about 8,500 current and former staff of the Department of Social Services, blamed on a third party contractor.

Of course, while hoping for the best you still need to plan for the worst. We all know that prevention is better than the cure … but it’s smart to have a first-aid kit, just in case.

That same study by the Ponemon Institute found that the best steps you can take to lessen the consequences of a data breach are the steps you take before the breach even occurs: staff training, and having a data breach response plan in place.

So - are you ready for 2018?

You should be doing your upmost to prevent data breaches anyway – but once the new Australian and European regimes of mandatory notification kick in, the consequences of failing to do so will become much more significant.

To help you get ready, we will shortly be launching some new privacy compliance tools, including a template Data Breach Response Plan you can download and easily customise for your organisation, as well as a template Privacy Risk Assessment Framework. Look out for those on our website soon.

In the meantime, if you need privacy awareness staff training to help spread the message throughout your organisation, we have standard and customised eLearning options available. Our training content has already been updated to incorporate the new data breach notification requirements. And of course, we’ve also got our more specialised eLearning modules for privacy professionals, about identifying and mitigating privacy risks. (Plus some more modules for privacy pros, coming soon). Look out for those on our website soon.

Time to get your skates on. 2018 will be here before you know it.

ATTENTION PRIVACY PRACTITIONERS: You can help us design the best privacy guidance and toolkit solutions to meet your needs – tell us what you are looking for! Our customer needs survey is at www.salingerprivacy.com.au/competencekits and is open until Friday 15 December 2017.
As Australian businesses prepare for the amendments to the Privacy Act 1988 (Cth) that will introduce mandatory data breach notification, the recent Equifax breach in the US provides some important lessons. Those lessons cover all aspects of privacy and data compliance, from governance and internal structures to breach response and planning.

On 9 November 2017 Equifax filed their third quarter results with the US Securities and Exchange Commission, reporting that the data breach (which affected approximately 145.5 million American citizens and included records of their banking details and social security numbers) cost Equifax in the order of $87.5 million dollars before the end of September. Given that the Equifax breach contained such a significant number of records (about 50% of the American population) and due to the nature of the entity (being a credit-reporting agency), it is unlikely that an event of that scale would occur in Australia. Despite this, even if a breach were one-tenth of the size and the costs one-tenth, it would still cost an entity over $8 million dollars, which far exceeds the cost of any regulatory fines or undertakings.

So what happened at Equifax?

The timeline for the incident, as reconstructed from public sources is summarised below.

Facts & Timeline

March 2017

(a) Equifax is notified by the Department of Homeland Security that they need to patch their open-source web application framework, ‘Apache Struts’. This was not applied.

(b) Three days after this notification, Equifax’s security scan failed to detect any vulnerabilities in Apache Struts.

(c) One of Equifax’s payroll subsidiaries suffers a security incident, whereby the tax and salary data of at least five companies is stolen.

13 May – 29 July 2017

(d) Hackers gained continuing, unauthorised access to personal information (including Social Security numbers, birth dates and addresses) until July, when it was detected by Equifax.

(e) At this point, the breach is estimated to have exposed personal information on up to 143 million individuals in America.

(f) The incident also potentially exposed the credit card numbers of 209,000 Americans and some driver’s licence numbers.

29 July 2017

(g) Equifax discover the breach.

1-2 August 2017

(h) Three top executives in Equifax (including the CFO) sell $1.8 million of shares in the company.

14 August 2017

(i) Equifax CEO, Richard Smith, allegedly becomes aware that consumer personal information was breached.

22 August 2017

(j) Richard Smith notifies the director of Equifax’s board.

24-25 August 2017

(k) The Equifax board of directors is briefed on the data breach.

7 September 2017

(l) Equifax informed the public about the breach.

(m) Equifax offer free identity theft protection and credit file monitoring packages to all individuals affected. Considering that their current ‘Premier’ package is $19.95 a month, this is a prospective $2.85 billion worth of free services every month.

15 September 2017

(n) Equifax admits that up to 400,000 U.K. residents may also be affected by the breach.

(o) Equifax’s Chief Information and Chief Security Officers resign.
19 September 2017
(p) Equifax announce that approximately 100,000 Canadians may have had their information breached.

26 September 2017
(q) Richard Smith retires.

2 October 2017
(r) Equifax announce that Mandiant, an independent cyber security firm hired by Equifax, has finished its forensic investigation into the breach.

(s) Investigations revealed that an additional 2.5 million individuals were affected, bringing the total to 145.5 million individuals.

(t) Equifax confirm that the breach has only affected 8,000 Canadians.

3 October 2017
(u) Congressional hearing into the data breach starts.

4 November 2017
(v) Equifax internal investigation concludes that there was no insider trading when the executives sold their shares.

What was the threshold issue?

The first issue for companies to consider is Equifax’s response to the notification in March 2017 to patch Apache Struts. While it is never merely an IT issue, the fact that the patch was not applied and was not detected raises an issue of internal accountability and reporting, both inside Equifax’s IT department and within their executive team. The response to this notification from the Department of Homeland Security was ultimately insufficient. The fact that someone within Equifax emailed someone else to say “patch Apache” and there was no follow up other than routine scans, suggests that the internal process could have been improved. One simple lesson to learn from this would be the use of a ticketing system, which would have ensured that the organisation was not reliant on one individual (as the former CEO Richard Smith reportedly stated at the Senate Congressional Hearing), but would instead ensure that a number of individuals had the opportunity to certify that the relevant version of the software was identified, patched and tested.

While this is a technical issue, the structure for reporting and monitoring of such issues is important. The second system architecture lesson to be learned from the incident is one of ensuring that vulnerabilities of web-facing systems are limited to those systems. One might ask how a breach of the web-facing system on which Apache Struts was based, which was the external dispute resolution public-facing web layer, allowed hackers to reach into the heart of Equifax and its important personal information.

Following the Equifax breach, Apache Struts, who obviously received some adverse publicity as a result, made a public statement which included five recommendations including the following:

4. Establish security layers. It is good software engineering practice to have individually secured layers behind a public-facing presentation layer such as the Apache Struts framework. A breach into the presentation layer should never empower access to significant or even all back-end information resources.

As a matter of governance, a system should be structured in such a way that a breach of a web-facing part of a system does not allow a hacker to then access core secured data.

Why did finding the breach take so long?

The timeline for discovery is important. The time at which Equifax became aware of the vulnerability was in March 2017. Hackers gained access between 13 May and 29 July, and it was only on 29 July when Equifax discovered the breach. One might argue that if Equifax had better scanning and reporting systems in place, the breach would have been discovered earlier and their exposure would thus have been limited. However, in any event, the important issue is what happened after the discovery on 29 July 2017.

Under Australia’s new mandatory breach notification rules, once an entity becomes aware that there are reasonable grounds to suspect that there may have been an eligible data breach of the entity, it must take all reasonable steps to carry out an assessment as to whether or not there is an eligible data breach. The assessment must be finalised within 30 days, during which an entity must complete the assessment and then, under section 26WK, prepare a statement to give to both the Office of the Australian Information Commissioner (OAIC) and the affected individuals.

The OAIC has issued a guidance resource on assessing a suspected data breach which requires that when an entity becomes aware of reasonable grounds to suspect that there may have been a breach (which may be a security incident, notification of loss of unencrypted media or a “tip off”) then they must undertake the assessment within the 30 days. In order to undertake an assessment that is compliant with the Privacy Act, it must be reasonable and expeditious, and the OAIC considers that entities need to include a three-stage process:

- Step 1: Initiate – evaluate and decide whether an assessment is necessary, and identify the person or group who will be responsible for completing it;
- Step 2: Investigate – gather information around a suspected breach, including what information is likely to impacts; and
Step 3: Evaluate – make a decision based on the investigation about whether it is an eligible data breach. If it is an eligible data breach, then the entity must promptly notify affected individuals and the OAIC about the breach.

In the example of Equifax, it took more than 30 calendar days (between 29 July and 7 September) to inform the public and for part of that time period, the breach was supposedly not known within the parts of the company where you would expect it to be known. For example, when it was revealed that three top executives, including the CFO, sold shares they held in the company on the 1st and 2nd August, it caused outrage that they were involved in insider trading. However, the CEO indicated that it took from 29 July until 15 August for him to become aware of the breach and it then took him a further week before he notified the Equifax board. This process would clearly be inadequate in an Australian context. Accordingly, companies need to prepare their data breach response plans, including their processes for investigating and documenting their investigations into breaches. A significant issue for organisations would be determining who makes the call on whether a breach amounts to an eligible data breach requiring notification. We expect that many entities will seek advice from their law firms on this point, as it is not an issue for which anyone internally would wish to take responsibility.

Notifying affected individuals – Key takeaways

There are a number of lessons to be learned from the Equifax breach about what to do when you inform individuals. There were a number of criticisms about the way that Equifax did this, including that the microsite they set up to allow individuals to determine whether they had been affected by the breach, had insufficient security and individuals were being asked to input the last six digits of their Social Security Number, something that many refused to do given the lack of security. There was also a lack of clarity around the actual site and one ethical hacker, in order to demonstrate the problem, set up a fake site which was then tweeted or retweeted by the Equifax Twitter feed at least eight times. Equifax further enraged the public, and is now the subject of regulatory issues, because it also offered free identity theft protection for a short period but, in order to sign up for this free period, individuals had to enter their credit card details so that at the end of the free period they would automatically take the paid service.

Taking a holistic approach

While many of these issues are not legal and require a team to assess and respond to an incident, there are many governance matters that can be planned for in advance and many legal protections that can be put in place. Certainly, data breach simulation exercises with internal and external teams are one way to do this because when a crisis is going on it will be too late to plan for the crisis, and in this instance, time spent in advance is well worth any internal and external cost to the organisation.
Trust, transparency and accountability were the key focus of discussion during an enlightening session on Artificial Intelligence, co-hosted by iappANZ, Microsoft and the AI Forum NZ in Auckland on 17 November 2017. There was also a measure of reality checking thrown into the mix. It seems Siri is not likely to take over our lives – Hal-style – anytime soon. It is apparent that proponents of AI are also proponents of care and restraint. There’s time, says the industry, to design AI that is properly regulated and it appears that the industry is intent on doing this right.

This session was refreshing in that it was not delivered by privacy professionals. Instead, we heard about AI from a variety of viewpoints – the technology provider, the data scientist and the health professional. This meant discussions focused on opportunities, not risks. The risks were noted, of course, but as conditions to work through, not handbrakes on innovation. It was a good reminder for us as privacy professionals to put ourselves in the shoes of our clients and remember that we should, where possible, be aiming for a positive sum, not zero sum, outcome.

The Technology Provider – Dave Heiner is VP, Corporate, External and Legal Affairs for Microsoft. Dave is right in the thick of AI development, leading research into policy issues at the intersection of data and society. Dave works to leverage AI and other technologies to help bring about equal access to justice and promote human rights.

Well aware of the doomsayers out there (Elon Musk, Stephen Hawking), Dave took the view that we were a long way off the sort of technology that could pose any real risk to humanity as we know it. Rather, AI presents opportunities to assist humans, improve decision making and remove error. AI (or, more accurately, Computational Intelligence) must be designed to augment not replace humans.

By making patterns out of data, AI can provide the intelligence we need to make better health decisions. AI can do clever things with data but Dave acknowledged that it lacks important human qualities such as empathy, fairness and judgement. A good AI system would combine the strengths of the technology with the strengths of its human users.

AI presents a number of key compliance challenges which are not confined to the health industry. These systems must be designed in a way that ensures safety and reliability (of data and decisions) and that promotes fairness in decision making (and does not perpetuate existing biases or discrimination). If these challenges are adequately addressed, the healthcare industry and its consumers are more likely to trust AI systems. Dave considered the following would help:

- Increase diversity within the AI industry, to reduce the likelihood of human biases being written into AI systems.
- Find techniques to detect whether AI systems and the datasets they rely on are facilitating fair outcomes.
- Develop guidelines to ensure Fairness, Accountability, and Transparency in Machine Learning (“FATML”).
- Ensure strong privacy controls are built into AI systems that guide the way in which AI systems infer things about individuals that they may have chosen not to share. This might help to avoid a repeat of the Target story.

The Data Scientist – Kevin Ross is Director of Research at Orion Health and leads the Precision Driven Health Partnership. Kevin is all about data analytics, having founded
Frith reminded participants of recent regulator criticism of the NHS – Google DeepMind collaboration, noting that trust and transparency were lacking in that case, which involved the sharing of health information of about 1.6 million people. Accountability, transparency and choice must be key elements where AI uses personal information, agreed the panel.

The panel generally agreed on a few other things too:

- AI is raising the stakes, both in terms of benefits and risks. Ultimately, the way AI is developed and used, just as the way personal information is collected and used, will reflect societal values. These values can differ across jurisdictions, with some cultures valuing individual privacy over wider societal benefits.
- Consent is an important consideration, particularly where sensitive health information is used for secondary purposes, but it presents real practical challenges. The industry might be better to focus on transparency of collection and purpose, and effective messages on the benefits, to build general public comfort in the use of health data for wider community health purposes.
- AI is only as good as the data we give it. Equally, AI is only as ethical as the boundaries we set for it. It is not inherently dangerous (yet) but it lacks the common sense – or emotion – a human can introduce into decision making. For health, this limits the extent to which AI can, or should, ever replace a human.
- In the healthcare space, AI is tied up with the move to eHealth and a national health record. Without access to big-health-data, AI will not function at its optimum. This also means that health agencies must move away from paper records and embrace technologies that facilitate the creation and retention of consistent and accessible notes, diagnoses and treatment plans.

The Privacy Professional – Frith Tweedie is leader of the Digital Law practice at EY Law NZ, advising on legal issues associated with new and emerging technologies. With over 15 years’ experience advising on digital, technology, privacy and IP matters in both NZ and the UK, Frith was well placed to drive a panel conversation on the privacy impacts of AI.

Analytics Forum (a best-practice network of professionals dedicated to improving NZ’s analytics capability).

Acknowledging that this will require a careful calculation of risk versus reward, Kevin believed that AI presented a valuable opportunity to support all the players in the healthcare industry to make better use of health information. Clinicians (and their patients) could benefit from assisted decision making, health coordinators could benefit from smarter planning tools and researchers could use AI to better reveal patterns and predict health issues.

Kevin shared Dave’s concern that biases can be unwittingly written into AI systems but took the alternative view that AI systems could reveal already existing biases and help healthcare professionals and researchers to eliminate them. Kevin also offered some thoughts on ensuring that AI evolves in a privacy-protective way:

- Get ahead of the issues by developing a clear set of principles on data ownership and control. The Data Futures Forum has done good work in this space that could be used to shape public conversations on these issues.
- Ensure clear rules are in place controlling the way AI outcomes are used, such as communicating predicted health risks to patients.

The Health Professional – Dylan Mordaunt is a physician with the Waitemata District Health Board. As a Paediatrician and Clinical Geneticist, Dylan has a strong interest in genomics, precision health, health IT and data science, with a particular focus on improving public health outcomes.

Dylan could see the potential AI offered in improving equity in healthcare. By utilising big-health-data in a responsible way, Dylan believed that AI could address current inequalities for the greater good, leading to improved public health outcomes. Dylan noted that, currently, patients create a highly disconnected data trail across various health agencies. The fragmentation of this data limits its usefulness in identifying trends in healthcare and improving wider access to public health services. AI could address this, provided that the public were sufficiently engaged to understand the benefits.

The Privacy Professional – Daimhin Warner is an iappANZ board director and is the Auckland Director of Simply Privacy, a consultancy providing privacy advice, strategy and training to business and government. simplyprivacy.co.nz
The EU’s new and wide-ranging General Data Protection Regulation (GDPR) represents an unprecedented shakeup of the European data protection regulatory environment. The GDPR promises to set a new regulatory benchmark and drive reform in jurisdictions around the world. The GDPR will come into force on 25 May 2018, replacing the current EU Data Protection Directive 95/46/EC. It will have immediate direct effect in all EU Member States.

Australian companies with exposure to the European market should take note – the GDPR can and will apply to companies based outside of Europe. Australian-based companies should take this opportunity to confirm whether the GDPR will apply to them come May, or whether they need to prepare for GDPR compliance to access the European market in the future.

The costs of non-compliance may be extreme – the GDPR introduces a new set of sharp teeth for European regulators, including fines of up to €20 million or 4% of global revenue, whichever is the greater. However, the added burden of compliance promises to pose a challenge for many businesses working with limited resources.

Part 1 of this article will help you understand whether the GDPR will apply to your business.

Part 2 will help you focus your efforts in preparing for the GDPR by identifying links and differences between the 13 Australian Privacy Principles and the GDPR’s 99 Articles.

Part 1 The long arm of the law

The GDPR’s extra-territorial application

Critically for Australian companies, Article 3 of the GDPR extends the GDPR to any company that controls or processes the personal information of individuals in the EU (whatever their nationality or place of residence) if the processing is related to offering goods or services or monitoring their behaviour, whether or not the company is located in the EU or the processing occurs in the EU.

For the purposes of the GDPR, a data ‘controller’ determines the purposes and means of the personal information, and the ‘processor’ processes the information on their behalf. ‘Processing’ is not a term found in Australian privacy law. The term is broadly defined and essentially means any act or practice that is done to, or in connection with, personal information.

Therefore, Australian companies that service or supply European clients, or otherwise offer goods or services to or monitor the behaviour of individuals in the EU that takes place in the EU, need to assess their client and individual customer bases, operations, systems and processes to answer three key questions:

1. **Do you have an ‘establishment’ in the EU?** (Article 3.1)
2. **Do you offer good or services to individuals who are in the EU (whether or not you charge for them)?** (Article 3.2(a))
3. **Do you monitor any behaviour of individuals in the EU?** (Article 3.2(b))

**Establishment**

Article 4 provides that the main establishment of a data controller is the “place of its central administration” in the EU. That is, where the “decisions on the purposes and means of the processing” occur. For example, if you have an EU office or headquarters.

For processors, the main establishment will be either the place of central administration in the EU or, if the processor does not have one, then where the main processing activity in the EU takes place. For example, if you have your head office in Australia, but maintain an EU data centre.

**Offering goods and services**

The GDPR recitals explain that a range of factors will be relevant to deciding whether a company is ‘offering goods or services’ to individuals in the EU. These include:

- the use of language and currency or a top-level domain name of an EU Member State
- delivery of physical goods to a Member State
- making references to individuals in a Member State to promote the goods and services, or
- targeting advertising at individuals in a Member State.

Mere accessibility of an Australian company’s website or app to individuals in the EU will not, by itself, reach the threshold.

Some of these factors obviously indicate that goods and services are being offered. But it may ultimately be the
cumulative effect of various activities that bring a company’s data processing within the reach of the GDPR.

Part 2 A Tale of Two Jurisdictions

Gap analysis - Comparing the GDPR and Australian Privacy Principles

If the GDPR is likely to apply to your data processing, understanding the gaps in your current privacy framework will be critical. A gap analysis can help you identify the key areas to focus on.

The GDPR shares some thematic similarities with Australia’s national privacy regulatory regime, set out in the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs).

The GDPR and the Privacy Act share a similar purpose - to foster transparent information handling practices and business accountability in relation to the handling of personal information. The two regimes take different approaches – the GDPR’s 99 articles are highly prescriptive, whereas the Privacy Act relies on a principles-based approach supplemented by extensive guidance. However, the founding principles of the GDPR (the lawful, transparent and fair processing of personal data) laid out in Chapter III (Articles 5-11) and many of the GDPR’s express obligations align with the steps that the OAIC expects Australian companies to take to comply with the APPs (as set out in OAIC guidance). In short, best practice compliance with the APPs will help Australian companies support compliance with the GDPR.

There are some key differences - both in terms of legal concepts and additional data subject rights and corresponding obligations found in the GDPR. These are set out in the comparison table below.

Summary of the APPs vs the GDPR

The Australian Privacy Act applies to ‘APP entities’ – that is Australian and Norfolk Island government agencies (agencies) and private sector businesses (organisations) as well as credit providers and credit reporting bodies. Individuals and many ‘small business operators’ – businesses with an annual turnover of less than AUD $3 million – are exempt from the operation of the Act.

Unlike the GDPR, the Privacy Act does not distinguish between ‘data controllers’ and ‘data processors’ – any APP entity that holds personal information must comply with the APPs.

APP 1 — Open and transparent management of personal information

This first APP requires APP entities to manage personal information in an “open and transparent way”, including taking reasonable steps to ensure that they comply with the APPs.

Monitoring

To determine whether a processing activity can be considered to be ‘monitoring’ the behaviour of individuals in the EU for the purposes of Article 3.2(b), you should consider whether your company is:

- associating individuals in the EU with online identifiers provided by their devices, applications, tools and protocols, such as IP addresses and cookie identifiers
- tracking their behaviour on the Internet, and
- using data processing techniques that profile individuals, particularly in order to make decisions concerning them for analysing or predicting their personal preferences, behaviours and attitudes.

Enforcement

European data protection authorities will have increased supervisory powers under the GDPR. However, the question of how those authorities will approach extraterritorial enforcement against companies established and operating outside the EU is far from settled.

GDPR Article 50 imposes obligations on the EU Commission and authorities to take appropriate steps to cooperate with international stakeholders. In recent years, there has been increasing cooperation between authorities. Under the GDPR, it is likely that EU authorities will liaise with the Australian privacy regulator – the Office of the Australian Information Commissioner (OAIC) – when responding to data processing by an Australian company. This may in turn trigger regulatory action by the OAIC or a cooperative effort to effect an appropriate response. Any evidence of a company’s presence in or nexus with an EU Member State may influence the potential for cross-border enforcement action.

How can you prepare?

If any of your answer to the three questions above is ‘yes’, then you will need to consider:

- what are the risks from gaps in your current compliance under Australian privacy law against the GDPR requirements, and
- what additional steps you need to take to ensure that you can comply with additional GDPR requirements, or
- whether you need to cease any activities in relation to individuals in the EU to which the GDPR will apply and/or restructure your EU operations.
APP 1 is similar in effect to GDPR Article 5 Principle 2, which requires controllers to be able to demonstrate compliance with the obligations set out in Principle 1. Principle 1(a) also requires data processing to be done in a “transparent manner”.

APP 1.3 and 1.4 also require APP entities to have a clearly expressed privacy policy that deals with specified matters. GDPR Article 7 discusses obtaining of consent from an individual in the context of a “written declaration”, and Articles 12-14 address similar matters to those specified in APP 1.3 and 1.4. GDPR Articles 13 – 14 also require additional information to be provided; this includes information about how long personal data will be stored, the enhanced personal rights under the GDPR (such as data portability, the right to withdraw consent, and the right to be forgotten), and any automated decision-making including profiling.

APP 2 — Anonymity and pseudonymity
APP 2 requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym, unless a listed exception applies.

There is no direct analogue to this provision in the GDPR. However, the GDPR may apply to pseudonymous information (see Recital 28).

APP 3 — Collection of solicited personal information
APP 3 outlines what personal information an APP entity can collect. In particular, this APP requires that organisations only collect personal information that is reasonably necessary or directly related to their functions or activities, by “lawful and fair means” and, where reasonable and practicable, directly from the individual. Higher standards are applied to the collection of ‘sensitive information’ (see comparison table below); specifically, sensitive information may only be collected with consent, or where a listed exception applies.

A comparison can be drawn here to GDPR Article 5, which requires data collected for “specified, explicit and legitimate purposes”, and be processed “lawfully [and] fairly” (Principle 1(a) and (b)). The question of whether a company has a lawful basis for processing personal information is critical.

APP 4 — Dealing with unsolicited personal information
APP 4 requires APP entities to destroy or de-identify unsolicited personal information that they could not have otherwise collected under APP 3.

There is no direct analogue in the GDPR, however it should be noted that the GDPR does not permit collection of personal data without a specified, explicit purpose.

APP 5 — Notification of the collection of personal information
APP 5 requires APP entities to notify individuals (or otherwise ensure that they are aware) of specified matters when they collect their personal information (for example, by providing individuals with a collection statement).

Again, GDPR Articles 12, 13 and 14 impose requirements for the provision of privacy information about how data is processed that are substantially similar to the matters specified in APP 5, as well as additional obligations (see APP 1, above). This includes a requirement that the information is clear and easy to understand. Australian companies should consider, for example, whether their privacy policies are written in plain English.

APP 6 — Use or disclosure of personal information
This APP outlines the circumstances in which an APP entity may use or disclose personal information that it holds. Where an APP entity has collected personal information for a specific purpose, and wishes to use it for a secondary purpose, APP 6 provides that entities may not do so unless the individual has consented, it is within their reasonable expectations, or another listed exception applies. Exceptions include circumstances involving health and safety and law enforcement.

GDPR Article 6 similarly requires that personal data may only be processed where the data subject has consented to one or more of the specific purposes of the processing, or the processing is otherwise lawful as another listed scenario applies. For example, where the processing is necessary to perform a contract or comply with a legal obligation.

APP 7 — Direct marketing
APP 7 provides that an organisation that is an APP entity may only use or disclose personal information for direct marketing purposes if certain conditions are met. In particular, direct marketing messages must include a clear and simple way to opt out of receiving future messages, and must not be sent to individuals who have already opted out. Sensitive information about an individual may only be used for direct marketing with consent of the individual.

GDPR Article 21 provides individuals with, amongst other things, the right to object to the use of their personal data for direct marketing.

APP 8 — Cross-border disclosure of personal information
This principle requires an APP entity, before it discloses personal information to and overseas recipient, to take reasonable steps to ensure that the recipient does not breach the APPs in relation to that information. Personal information may only be disclosed where the recipient is
subject to a regulatory regime that is substantially similar to the APPs, where the individual has consented, or another listed exception applies. APP entities may be liable for the acts and practices of overseas recipients in certain circumstances (s16).

Chapter 5 of the GDPR provides that transfers of personal data outside of EU jurisdiction may only be made where the recipient jurisdiction has been assessed as ‘adequate’ in terms of data protection, where sufficient safeguards (such as a binding contract or corporate rules) have been put in place, or a listed exception applies. The European Commission has not, to date, assessed Australia as ‘adequate’, but the Commission is currently reviewing its adequacy assessments.

APP 9 — Adoption, use or disclosure of government related identifiers
APP 9 provides that an organisation that is an APP entity may not adopt a government related identifier of an individual as its own identifier, or use or disclose such an identifier, unless a listed exception applies. There is no direct analogue to this provision in the GDPR.

APP 10 — Quality of personal information
APP 10 requires APP entities to take reasonable steps to ensure the personal information it collects, uses or discloses is accurate, up to date and complete. Accuracy and currency of the information are mentioned in GDPR Article 5 (Principle 1(d)); “every reasonable step must be taken” to ensure that inaccurate personal data is “rectified without delay”.

APP 11 — Security of personal information
This APP requires APP entities to take reasonable steps to protect personal information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure. This provision is a frequent focus of investigations into APP entities conducted by the Australian Information Commissioner.

GDPR Article 5 similarly requires that data processing be undertaken in a manner “that ensures appropriate security of the data” (Principle 1(f)). Further, Article 32 requires the data controller and the processor to implement appropriate technical and organisational measures to ensure a level of security appropriate (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes). Those measures must also address the confidentiality, integrity and availability of the data.

APP 11.2 provides that APP entities must also take reasonable steps to destroy or de-identify personal information that they no longer require for a lawful business purpose.

GDPR Article 5 imposes a similar storage limitation – personal data may “kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed” (Principle 1(e)). However, the GDPR also explains that “personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)”.

APP 12 — Access to personal information
APP 12 requires APP entities to give an individual access to the personal information about them that the entity holds, on request by that individual. APP 12 imposes procedural requirements around access, and includes limited exceptions.

Article 15 of the GDPR imposes a similar right of access, with additional rights to know information about the collection and envisaged use of the data (such as recipients or potential recipients, likely storage period, and safeguards for overseas transfers).

APP 13 — Correction of personal information
APP 13 requires APP entities to take reasonable steps to correct personal information they hold about an individual, on request by the individual. This APP also imposes procedural requirements and includes limited exceptions.

GDPR Article 16 imposes a similar but stronger right; data subjects have the absolute “right to obtain…without undue delay the rectification of inaccurate personal data concerning [them]”.

GDPR rights that are not in the APPs
What none of the APPs provide is an express right to erasure, the right of restriction of processing, data portability and the right to object. The GDPR provides for these rights in Articles 17, 18 ,20 and 21.
### Legal Concept Comparable Table

<table>
<thead>
<tr>
<th>TOPIC</th>
<th>Privacy Act 1988 (Cth)</th>
<th>GDPR</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Personal Data</strong></td>
<td>The Privacy Act governs the handling of ‘personal information’, defined as “information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not.” (s6(1)).</td>
<td>Articles 17 and 20: Any information: (a) Relating to an identified or identifiable natural person; (b) An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.</td>
</tr>
<tr>
<td><strong>Data Subject</strong></td>
<td>‘Individual’ is defined as “a natural person” (s6(1)). Regulator guidance indicates that a deceased person is not a natural person (APP Guidelines para. B95).</td>
<td>Relating to an identified or identifiable natural person.</td>
</tr>
<tr>
<td><strong>Controller</strong></td>
<td>The Privacy Act does not distinguish between controllers and processors. Instead, the APPs apply to any APP entity that collects personal information. The definition of ‘APP entity’ includes: • most Australian Government agencies • all private sector and not-for-profit organisations with an annual turnover of more than AUS $3 million</td>
<td>The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or member state law, the controller or the specific criteria for its nomination may be provided for by Union or member state law.</td>
</tr>
<tr>
<td><strong>Processor</strong></td>
<td>• all private health service providers, and • some small businesses (ie, that trade in personal information for a benefit, are a contracted service provider to the Australian Government, or are a credit reporting body; ss 6(1), 6A).</td>
<td>A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. However, GDPR does also have a definition for “third party”: A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.</td>
</tr>
<tr>
<td><strong>Consent</strong></td>
<td>‘Consent’ is defined as “express consent or implied consent” (6(1)). Regulator guidance indicates that the four key elements of consent are:</td>
<td>Article 4: (11) ‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action,</td>
</tr>
<tr>
<td>Sensitive Data</td>
<td>'Sensitive information' is a subset of personal information and is defined as:</td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• information or an opinion (that is also personal information) about an individual’s:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>o racial or ethnic origin</td>
<td></td>
</tr>
<tr>
<td></td>
<td>o political opinions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>o membership of a political association</td>
<td></td>
</tr>
<tr>
<td></td>
<td>o religious beliefs or affiliations</td>
<td></td>
</tr>
<tr>
<td></td>
<td>o philosophical beliefs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>o membership of a professional or trade association</td>
<td></td>
</tr>
<tr>
<td></td>
<td>o membership of a trade union</td>
<td></td>
</tr>
<tr>
<td></td>
<td>o sexual orientation or practices, or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>o criminal record</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• health information about an individual</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• genetic information (that is not otherwise health information)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• biometric information that is to be used for the purpose of automated biometric verification or biometric identification, or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• biometric templates (s 6(1)).</td>
<td></td>
</tr>
</tbody>
</table>

APP 3 provides that sensitive information about an individual must not be collected unless the individual consents and the collection is reasonable necessary for an APP entity’s functions or activity, or a listed exception applies.

<table>
<thead>
<tr>
<th>Article 9:</th>
<th>Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Listed exceptions apply.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Transfer of Personal Data to third countries or</th>
<th>APP 8 provides that, before disclosing personal information outside of Australia, a business must take reasonable steps to ensure that the recipient does not breach</th>
</tr>
</thead>
<tbody>
<tr>
<td>APP 8 provides that, before disclosing personal information outside of Australia, a business must take reasonable steps to ensure that the recipient does not breach</td>
<td></td>
</tr>
<tr>
<td>Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if the</td>
<td></td>
</tr>
<tr>
<td>International organisations</td>
<td>the APPs in relation to the information, unless a listed exception applies.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Right to restriction of processing</td>
<td>No equivalent.</td>
</tr>
<tr>
<td>Right to be forgotten</td>
<td>No equivalent.</td>
</tr>
<tr>
<td>Data Portability</td>
<td>No direct equivalent.</td>
</tr>
<tr>
<td>Data breach notification</td>
<td>Amendments to the Privacy Act to introduce a mandatory data breach notification requirement will come into force on 22 February 2017. APP entities that experience an ‘eligible data breaches’ (that generate a “likely risk of serious harm” to affected individuals) must give a statement in a prescribed format to the Information Commissioner as soon as practicable (s26WK), and to affected individuals (26WL). If it is unclear whether a breach is eligible, APP entities must conduct an assessment within 30 days of becoming aware of the breach (s26WH).</td>
</tr>
</tbody>
</table>
A breach of the APPs is an ‘interference with privacy (s13).

Serious or repeated interferences with privacy may be subject to a civil penalty of up to AUD $2.1 million for companies (s13G).

Under Article 83:

- Up to 10 000 000 EUR, or in the case of an undertaking, up to 2 percent of the total worldwide annual turnover of the preceding financial year, whichever is higher for infringements of obligations such as controllers and processors, the certification body, and the monitoring body.

- Up to 20 000 000 EUR, or in the case of an undertaking, up to 4 percent of the total worldwide annual turnover of the preceding financial year, whichever is higher for infringements of obligations such as principles of processing, conditions for consent, data subject’s rights, transfer beyond EU, etc.

Under Article 84, each member state can lay down the rules on other penalties applicable to infringements of GDPR in particular for infringements which are not subject to Article 83, and can take all measures necessary to ensure that they are implemented.

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.  

Veronica Scott is the iappANZ Vice President, and Special Counsel at Minter Ellison Lawyers (Melbourne). Veronica’s specialist areas of practice include data protection and privacy, media law, risk and crisis management and freedom of information.  
[https://www.minterellison.com/people/veronica_scott](https://www.minterellison.com/people/veronica_scott)
PROFILE – JACQUELINE PEACE
Chief Privacy Officer, Air New Zealand
iappANZ Board Director and Secretary

What is your current role and how did you come to be a privacy professional?
Currently Senior Manager Data Protection and the Chief Privacy Officer for Air New Zealand. I head up the Global Privacy Office. My introduction to the privacy profession was through systems implementation and programme management. I was running an identity management stream for a large programme at BP. Approximately 200k employees and contractors across 96 countries needed to be issued unique IDs. No one realised until three days before “go live” that issuing unique IDs in many countries had privacy implications that needed to be addressed. Some Data Protection Authorities had to approve the adoption of IDs before they could be issued. Suffice to say, the project go live date was delayed...

Can you comment on the proposed reforms to the NZ Privacy Act?
I can comment but it may not be printable. The reforms have been talked about for a number of years now and there isn’t much sign of them coming soon. Perhaps the delays are due to watching how the new EU General Data Protection Regulation will play out or how Australia’s mandatory data breach laws will affect business – regardless, it’s time we stepped up a notch. As a global airline, we are setting our privacy “bar” at that of the GDPR as this is relevant for a large number of our customers who reside or travel through EEA member states. Equally though, we’ll be able to pass on some of the increased privacy rights for individuals to customers outside of the EEA. That can only be a good thing. Our reforms will need to keep up if we want to maintain “adequacy” when sharing data between NZ and the EU.

What are the data security and privacy challenges for your business?
Keeping up with global legislation is one but we have rationalised our approach to adopt the highest standard and where there are outliers in terms of privacy requirements in other jurisdictions, we take a risk based assessment of what additional requirements we may need to meet in any jurisdiction. Keeping everyone informed in a manner that is easily understood is also a challenge and an opportunity. We need to consider the privacy and commercial implications important to a business like ours that is constantly trying to personalise relationships to provide the most relevant products and services. No one in the business really wants to know the fine details of legislative change, they just want to know what they need to do to comply.

Why did you join iappANZ?
It was a great place to meet “like-minded professionals”, i.e., other privacy geeks. Funnily enough, not everyone is that interested when I tell them what my job is, although it’s definitely changing.

Do you agree that there should be mandatory data breach reporting and if so why?
Yes, within reason. It’s just not practical or feasible to report all breaches. It’s important and necessary though to report any that have an impact on individuals in a detrimental, harmful or distressing manner or that pose a risk to the rights and freedoms of individuals. We need to tell the individuals impacted also, it’s not just about reporting to the regulator. Why wouldn’t we tell people what threats there may be to their personal data or what harm may come to them? It’s our responsibility to inform people so they can take necessary steps to safeguard their physical or digital well-being.

What are your favourite apps and why?
My Sonos app, because it is all about the music and nothing else. I choose what I want to hear. It’s not chosen for me.
What tips and suggestions would you give to fellow privacy practitioners?

Changing hearts and minds to adopt a privacy mindset and culture, takes time. Don’t force this through fear of the regulator, or fines and sanctions but help people to understand why we care about handling personal information. Identify real examples within your business that your colleagues can relate to about harm or distrust that your customers feel when the business doesn’t live by its promises. Don’t spend too much time teaching the business about the legal requirements or the principles, these are important and matter but you’ll convince people more about the importance of privacy if you provide pragmatic solutions they can adopt. Little tweaks can go a long way. Have an open door, let them know you are there to help not to block their progress and work with them to enhance their initiatives as early as possible. Build a relationship with your regulator, they are there to help and from my experience, welcome being approached. They would rather help us avoid privacy complaints than be at the other end of a complaint, trying to un-ravel it.

How do you see technology disrupting current privacy practices and the way we approach compliance?

Technology is constantly impacting privacy practices but this doesn’t have to be a negative outcome. It can also work in our favour. For example, new technologies offer new opportunities to raise privacy awareness. We have a new chatbot called Oscar as a channel for customers to ask questions and get information. We’re teaching Oscar to answer questions in a privacy compliant manner. We are moving to APIs and as a result we’re building new tighter controls over what data can or can’t be accessed, so the business needs to be clear on what data is being shared and be clear about the purpose of access before the APIs are activated.

Have you been on any recent work trips and if so where and what did you learn?

I’ve recently been to our EU regional office in London. I sat amongst the team for a week, making myself available to talk to people to learn more about what they do. This provided real hands on insights to their challenges and an opportunity to work with them face to face to identify what works and not impose solutions that wouldn’t support their business needs.

Favourite place in NZ and why?

There are too many but my favourite local haunt is Cornwall Park, it’s a gem. I can pick up a great coffee and stroll amongst the sheep, cows, rabbits, chickens and the many healthy kiwis running or cycling away their work worries.
We’re looking for speakers! Do you have something you’d like to share at the 2018 Summit?

Each year our annual Summit gets bigger and better and we’re already well on track to continue this trend in 2018. Amongst our ANZ membership we have many talented, inspiring and engaging people so we’re turning the spotlight on you and accepting expressions of interest to present at next year’s Summit at Zinc, Federation Square, Melbourne on 1 & 2 November 2018.

We want to hear from you if you’ve got something to talk about that you think privacy and related professionals should hear. Maybe you’ve implemented a new program or initiative in your workplace that has had amazing success. Or on the flip side, maybe there are some lessons you’ve learned from things that didn’t go so well that you’d like to share with us. Perhaps you’ve done some research or written a paper on an exciting or new area of privacy. Or maybe you have a ‘very particular set of skills’ that should be shared with iappANZ members.

Interested? If so, drop us an email <Julie@iappanz.org> with a quick summary (no more than 500 words) of what you’d like to talk about, a bit about you and why you think it would be great to share with the wider community before Wednesday January 31st 2018.