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

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

Veronica Scott
veronica.scott@minterellison.com

Carolyn Lidgerwood
carolyn.lidgerwood@riotinto.com

Please note that none of the content published in the Journal should be taken as legal or any other professional advice.
Hello and welcome to the first edition of Privacy Unbound for 2017.

Well, we’ve really hit the ground running this year with several events already taking place, including Privacy After Hours evenings in Wellington, Sydney and Melbourne. Great to see so many of you.

We also recently co-hosted a panel session with Information Governance ANZ at iappANZ sponsor, Commonwealth Bank’s, office which was brilliantly moderated by iappANZ Board Director, Melanie Marks and received very positive feedback from attendees.

Coming very soon we have ‘Perspectives on Privacy and Security in eHealth Workshops’ held with our sponsor Microsoft in Australia and New Zealand – if you haven’t registered for a place, get in quick.

We have a lot of other events in the pipeline across Melbourne, Sydney, Brisbane, Wellington and Auckland up to and including Privacy Awareness Weeks in both New Zealand and Australia in May. More to follow very soon.

We recently had the our second meeting with the new Board and we are getting together again in person this week for a full day to discuss strategy and plans for the coming years. Our new Board comprises;

**Executive Committee**

Kate Monckton - President
Emma Hossack – Treasurer
Veronica Scott – Vice President
David Templeton – Secretary

**Board Directors**

Carolyn Lidgerwood
Christopher Rogers
Marta Ganko
Katherine Sainty
Melanie Marks
Jacqueline Peace
Richard Kilpatrick
Olga Ganapolsky

I’d like to welcome back some familiar faces and extend a very warm welcome to Christopher, Marta, Jacqui, Katherine and Richard who are serving their first term on the Board. I’m very exciting by the ideas and enthusiasm that is already coming out of this group of fantastic people.

Part of the Board meeting this week will be spent finalising our new advisory committee model. We’re always looking for members who are keen to get more involved and this is a great time to consider it as we set up the advisory committees. These committees will help lead the planning for iappANZ events, journal content and the Summit. If you would like more information, please get in touch with us.

As ever if you have any questions or suggestion, please contact me or any of our Board.

Kate
Hello,

It seems like so much has happened in the past couple of months both locally and globally that the summer holidays are all but a distant memory. Luckily Anna Johnston is here to remind us that it is a new year and shares her predictions and suggestions for new year’s resolutions for all of us.

Here in Australia, we watched as the Full Federal Court dismissed the Privacy Commissioner v. Telstra appeal, something which Peter Leonard covers in is inimitable style within this edition of Privacy Unbound. Veronica Scot and Helen Lauder also take a look at this case and the interpretation of personal information.

On a more international level, we asked some of our iappANZ Board Directors and members to provide us with some thoughts on current issues, including what the impending General Data Protection Regulation in the EU may mean for Australia and New Zealand. Julie Inman-Grant, the Australian e-Safety Commissioner (and former iappANZ Board Director) takes a look at where security and privacy meet especially in the context of cyber safety and young people. She also provides a great overview of the broad scope the Office has and what you can expect from them in 2017.

Annelies Moens provides an excellent book review – the first I’ve seen published in Privacy Unbound in some time – on Cathy O’Neil’s ‘Weapons of Math Destruction’.

One of our new Board Directors, Christopher Rogers shares his considerable experience and practical advice on choosing studying for and maintaining the right the IAPP certification for you.

As those of you who were at the Summit last year in Sydney will know, the IAPP is developing an Australia and New Zealand certification. We have a wonderful advisory board made up of members from both countries who are working very closely with the IAPP to ensure that the local certification really hits the mark. I’m very much looking forward to seeing the final product and I’ve heard from many of you that you are also.

As always, if you have any questions or suggestions about the organisation please contact me.

Veronica
Welcome to 2017, Dear Readers! I do hope you had a good break. Now, back to work!

What will 2017 bring for privacy professionals? I shall be so bold as to make some wild predictions:

- There will be new privacy challenges posed by drones and artificial intelligence. (Yes, the robots will be taking over. Deal with it, cats.)
- GDPR-readiness testing will ramp up, as will the level of panic.
- Trump’s presidency will pose ethical dilemmas for Silicon Valley.
- Here in Australia we will finally get mandatory data breach notification (though don’t hold your breath).

And yes, there will be more data breaches. Oh lord, there will be many, many more.

So what should be on your agenda?

Call it a work plan, call it a wish-list, call it what you like – but I would suggest that if Santa didn’t bring you everything here, you might need to make these your 8 New Year’s Resolutions:

1. Show you care about the privacy of your customers by changing the social media ‘sharing’ buttons on your website to ‘do not track’ versions like these from PrivaCore.
2. Avoid a #censusfail - remind HR to implement privacy awareness training.
3. Review what data is being collected and used. Check in with ICT to make sure you know about all their Big Data projects (buzzwords to look out for: Data Warehouse, data analytics, Business Intelligence, dashboard and reporting projects) - and then advise them on how to build-in privacy best practice. But meanwhile don’t forget about records management for all the little comms like text messages.
4. Review what data is being disclosed without authority. New laws like GDPR and the Victorian Protective Data Security Standards (as well as the Australian Government Information Security Manual and NSW equivalent guidelines) are going to ramp up the requirements to classify and label data in order to apply the right infosec controls. Ask ICT about implementing tools like these from JanusNet.
5. Review what data is being publicly released. Talk to your ICT & Comms people about de-identification and the risks of re-identification, and establish ethical review processes for research and other data analytics projects.

6. And while you’re talking to ICT, please remind them not to do dumb stuff like putting database 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.

7. Hope for the best, but also plan for the worst. Don’t wait for mandatory data breach notification laws - develop a data breach response plan now. And check out Red Cross as an example of good customer communications in the wake of their data breach.

8. And finally: look after yourself too! Stay on top of your professional development. If you haven’t already, join iappANZ. And look out for our specialised training for privacy professionals. We already offer face-to-face workshops on things like privacy risk management, but coming soon in 2017 will be our new online pay-per-view Privacy Professionals Training modules. Yippee!

Our own New Year’s Resolutions? Here at Salinger Privacy we really really do want to finish that guide to De-identification for Dummies Privacy People that we promised months ago and which is half-written, as well as the aforementioned new online training modules ... but while it is still summer the beach also beckons ...

All the best, dear readers, for a happy and productive new year!
Obtaining an IAPP Certification is a great way to get ahead in your career as a privacy professional, achieve recognition amongst your peers and maybe even get you that well deserved promotion from your company!

Have you been thinking about getting an IAPP Certification but don’t know where to start? Here’s a run-down on what you need to know about certification and some practical tips to help you get there.

**What IAPP Certifications are available to IAPP-ANZ members?**

The IAPP offers a number of Certification programs to its members, they include:

- Certified Information Privacy Professional (“CIIP”) – for certification in privacy laws, regulations and frameworks across a number of different jurisdictions including the United States, Canada, Europe, Asia, and very soon, Australia & New Zealand;
- Certified Information Privacy Manager (“CIPM”) – for certification in the day-to-day management of an organisation’s privacy function; and
- Certified Information Privacy Technologist (“CRIPT”) - certification for IT professionals in their knowledge of data privacy requirements worldwide.

**Choose the IAPP Certification which is right for you.**

Having a CIPP Certification demonstrates your understanding of the privacy laws and regulations applicable in your jurisdiction. The IAPP-ANZ team are currently working with our counterparts in the United States to develop the necessary Body of Knowledge and examination questions for an Australian and New Zealand CIPP Certification, so make sure you watch this space for more information when this certification becomes available. In the meantime, if your organisation has operations in the United States, Canada, the EU or Asia, or deals with individuals from these locations who are customers or suppliers, you should consider obtaining a CIPP certification for that jurisdiction.

You don’t need to lead the global or national privacy function of your organisation in order to obtain the CIPM Certification. Obtaining your CIPM will demonstrate to your supervisors and peers that you have an in-depth understanding of the way in which data privacy laws and regulations impact on your organisation’s daily operations. It will help you to establish the baseline of your organisation’s current privacy program, identify any gaps in the program, build and implement your organisation’s privacy program framework and measure performance of the program through selected privacy metrics.

If you work in an IT Services function within your organisation, the CIPT Certification is the right course for you. In obtaining this certification, you will develop greater knowledge and understanding of data privacy issues which impact upon IT such as privacy by design, best practices in data collection and transfer, and emerging issues in cloud computing, surveillance and facial recognition.
Prepare and Study for your IAPP Certification

Once you have chosen your certification course, the next step is to study the course materials in preparation for the exam. Details of the necessary course texts, required Body of Knowledge and Exam Blueprint are available on the IAPP’s website: [https://iapp.org/certify/](https://iapp.org/certify/). If you are having difficulty in obtaining a copy of the course textbook, feel free to reach out to the helpful IAPP-ANZ Operations team at opsmanager@iappanz.org and they can assist you to obtain a copy. The IAPP recommends that you spend at least 20 hours studying the course materials in preparation for the certification exam. This time will be best spent by reading the course textbook, summarising the important sections in examination notes and committing the content to memory (just like you did back in your old school days!). The IAPP have practice exams available on their website for each of the Certification programs. It is highly recommended that you purchase and take the practice exam (which is typically 20 multiple choice questions) as this will give you a good idea of what to expect in the actual exam and whether you have undertaken sufficient study in preparation for the exam.

Taking the Test for your IAPP Certification

When you have studied the course text, completed the practice exam and feel you are ready to sit your final examination, it’s time to register for your computer-based examination. The IAPP-ANZ Operations team can assist you with information on how to purchase and set your examination through the IAPP’s US website. You simply need to choose the date and time and the preferred location of the Kryterion Testing Centre where you wish to sit the exam. Kryterion Testing Centres are located in each capital city in Australia as well as in Auckland, Wellington and Christchurch in New Zealand. The IAPP have prepared some helpful tips on what to expect when the exam day arrives and these are available at: [https://iapp.org/certify/exam-day/](https://iapp.org/certify/exam-day/). It’s important to read these instructions in advance of your exam day so that you are fully aware of what to expect when you arrive at the testing centre.

Once you have completed the computer based exam, the good news is that you will be provided your exam results on your computer screen before you leave the testing centre and a copy will also emailed to you (so there is no nervous wait for the results to arrive in the post). You will also receive an email from the IAPP containing a link to your Certification in an online format, which can be added to your LinkedIn profile.

Maintaining your Certification with ongoing Professional Development

Once you have your certification (and congratulations on achieving that!) you will need to undertake continuing privacy education (CPE) to maintain it. This requires you to undertake at least 20 hours of CPE every two years. If you are an avid attendee of IAPP-ANZ events such as the Privacy Summit or knowledge seminars, or you contribute articles to Privacy Unbound or watch webinars on current privacy topics, obtaining your CPE points within this timeframe shouldn’t pose too much of a problem for you. **What are you waiting for?**

It’s important to keep up to date on current data privacy knowledge and training, take control of your career path and be seen by your organisation’s leadership and peers as a leader in privacy and data protection. So don’t put it off, select your preferred certification course, study the textbook and take the exam. You will be glad that you did.

The views expressed in this article are those of the author and not EY.
iappANZ is the pre-eminent forum for privacy professionals in Australia and New Zealand. We are affiliated with the International Association of Privacy Professionals (IAPP), the largest and most comprehensive global information privacy community and resource with more than 23,000 members. We work with public and private entities across all industry sectors in Australia and New Zealand as well as the Privacy Commissioners in both countries.

iappANZ offers our members a wealth of opportunities to expand their privacy knowledge, compliance, interests and networks. Our members in Australia and New Zealand represent some of the best minds in the privacy field, from large public companies and the government sector to not for profit, SMES and individuals.

CONNECTING PRIVACY PEOPLE, EMPOWERING PRIVACY PRACTICE

Join 23,000 members
A review of Australian Privacy Commissioner V Telstra Corporation Limited

BY PETER LEONARD

Full Federal Court of Australia
[2017] FCAFC 4, 19 January 2017

The Full Federal Court dismissed an application by the Privacy Commissioner seeking orders in relation to a decision by the Australian Administrative Appeals Tribunal that had overturned a determination by the Australian Privacy Commissioner granting journalist Ben Grubb access to certain data relating to Mr Grubb’s use of Telstra mobile services. The Court’s judgement clarifies that the particular context of data collection and use is relevant to determination of whether information is personal information. In this particular context (cell tower location and call usage information relating to a mobile phone) the device-related and network-related information sought by Mr Grubb could be traced back to Mr Grubb as an ‘identifiable individual’ but was not sufficiently related to that individual to be information ‘about that individual’ protected as ‘personal information’ under the Australian Privacy Act. The Court’s reasoning makes it clear that there are significant limits as to when device-related and network related information is ‘about an individual whose identity may be reasonably ascertained from the information’ - a key issue that arises for many Internet of Things (IoT) applications now entering the market - but fails to provide a methodology or useful guidance as to the point at which relevant information ceases to be ‘about an individual’.

The Commissioner considered that the question of whether an individual’s identity can ‘reasonably be ascertained’ from information required an assessment as to how unreasonably high the level of effort necessary to link an individual through to non-identifying information must be before an entity receiving an access request can say that the access that is requested is not to information from which an individual’s identity can reasonably be ascertained. It was not contended that Mr Grubb as an individual could be linked to some network data relating to use by Mr Grubb of his mobile phone through a multi-step process (requiring significant labour input and including manual matching) of tracing and matching records through multiple databases in Telstra’s systems. Although Mr Grubb’s identity was not apparent in relevant Telstra databases where relevant metadata was held, the device identifiers or IP addresses or other transactional information there held could be traced through from mobile tower records to operational and network databases and on to personally identifying databases (in particular, the Telstra customer billing database). Telstra regularly facilitated request by law enforcement agencies for lawful assistance as to use of mobile phones by persons of interest by undertaking such tracing and matching processes.

Deputy President S A Forgie, in the Administrative Appeals Tribunal’s Decision ([2015] AATA 991 (18 December 2015)) overturning the Privacy Commissioner’s Determination, stated (at para 97) that where an individual is not intrinsically identified in information, a two-step characterisation process should be applied. The first step is determining whether relevant information is ‘about an individual’. The second step is working out whether an individual’s identity ‘can reasonably be ascertained from the information or opinion’. If relevant information is not ‘about an individual’, the second step must be applied. DP Forgie stated (at para 112, cited with approval in the appeal decision):

“Had Mr Grubb not made the calls or sent the messages he did on his mobile device, Telstra would not have generated certain mobile network data. It generated that data in order to transmit his calls and his messages. Once his call or message was transmitted from the first cell that received it from his mobile device, the data that was generated was directed to delivering the call or message to its intended recipient. That data is no longer about Mr Grubb or the fact that he made a call or sent a message or about the number or address to which he sent it. It is not about the content of the call or the message.
The data is all about the way in which Telstra delivers the call or the message. That is not about Mr Grubb. It could be said that the mobile network data relates to the way in which Telstra delivers the service or product for which Mr Grubb pays. That does not make the data information about Mr Grubb. It is information about the service it provides to Mr Grubb but not about him.”

The Full Federal Court understood the Privacy Commissioner to assert that if there is information from which an individual’s identity could reasonably be ascertained, and that information is held by the organisation, then it will always be the case that the information is about the individual. By so construing the Commissioner’s contention the Court (at para 63) had little difficulty in rejecting it:

“The words “about an individual” direct attention to the need for the individual to be a subject matter of the information or opinion. This requirement might not be difficult to satisfy. Information and opinions can have multiple subject matters. Further, on the assumption that the information refers to the totality of the information requested, then even if a single piece of information is not “about an individual” it might be about the individual when combined with other information. However, in every case it is necessary to consider whether each item of personal information requested, individually or in combination with other items, is about an individual. This will require an evaluative conclusion, depending upon the facts of any individual case, just as a determination of whether the identity can reasonably be ascertained will require an evaluative conclusion.”

Or as the Court later put it (at para 73), “this appeal concerned only a narrow question of statutory interpretation which was whether the words ‘about an individual’ had any substantive operation. It was not concerned with when metadata would be about an individual”. This then left the Court able to elect not to go on to elucidate a methodology to determine when facially device-related or network related information should nonetheless be considered to be information ‘about an individual’. The Court noted that in “some instances the evaluative conclusion will not be difficult. For example, although information was provided to Mr Grubb about the colour of his mobile phone and his network type (3G), we do not consider that that information, by itself or together with other information, was about him. In other instances, the conclusion might be more difficult”.

Without any prior case law guidance or a methodology to work out when metadata would be about an individual, Australian lawyers would usually seek to construe the statute having regard to its legislative objects and by reference to analogous decisions in comparable jurisdictions. However, the Court did not accept arguments by the Australian Privacy Foundation and the New South Wales Council for Civil Liberties, made by those bodies in seeking leave to be heard as amici curiae, that in working out when metadata would be ‘about an individual’ reference should be made to policy underpinning the Act. Although the Privacy Act referenced Australia’s accession to the International Covenant on Civil and Political Rights (ICCPR) and its commitment to adopt such legislative measures as may be necessary to give effect to the right of persons not to be subjected to arbitrary interference with their privacy, home or correspondences, the Court said that these commitments took ‘aspirational form’ and should not advance the substantive evaluation of the specific statutory provision. The Court also distinguished the statutory context in which arguably analogous matters had been determined in other jurisdictions, most notably the decision of the Canadian Federal Court of Appeal in The Information Commissioner of Canada v The Executive Director of the Canadian Transportation Accident Investigation and Safety Board and NAV Canada [2007] 1 FCR 203; 2006 FCA 157. That case concerned refusal by the relevant Canadian Board to disclose records of air traffic control communications concerning four aviation incidents. In that case Desjardins JA was called on to consider whether conversations between air traffic controllers and pilots revealed information about the relevant individuals, and reasoned (at par 53):

“The information at issue is not an individual … the content of the communications is limited to the safety and navigation of aircraft, the general operation of the aircraft, and the exchange of messages on behalf of the public. They contain information about the status of the aircraft, weather conditions, matters associated with air traffic control and the utterances of the pilots and controllers. These are not subjects that engage the right of privacy of individuals.”

The Full Federal Court then noted that the provisions in the Canadian statute were substantively different from those in the Australian regime, although the relevance of those differences was not explained. The Court also noted that the Canadian regime is concerned to protect from disclosure the personal information about an individual in order to preserve the privacy of the individual, without considering how the Australian Privacy Act clearly reached beyond creation of rights of access to records of personal information, to require transparency as to collection, use and disclosure of personal information in order to protect the privacy of individuals. Nor did the Court consider the carefully reasoned New Zealand precedents involving similar questions in the context of a closely analogous statute, notably including CBV v McKenzie Associates HRRT 020/04 (30 September 2004) and Apostolakis v Siewwrights HRRT 44/03 (14 February 2005), the Article 29 Data Protection Working Party’s Opinion 4/2007 on the concept of personal data, or the relevant post Durant English jurisprudence, notably the Information Commissioner’s Data Protection Technical Guidance: Determining what is personal information (August 2007), Information Commissioner v Financial Services Authority & Edem [2012] UKUT 454 (AAC) and Google v Vidal Hall & Ors [2015] EWCA Civ 311.
The Court’s election not to go on to elucidate a methodology to determine when facially device-related or network related information should nonetheless be considered to be information ‘about an individual’ leaves a fundamental question of Australian privacy law unanswered. There is no objectively determinable point at which information that has multiple subject matters (for instance, relating to a thing, or the operation of a network or a device, and also relating to an identifiable person) engages the right of privacy of that person. Determination of that point requires a subjective assessment of the particular context of collection and use of that data and whether that collection and use engages the right of privacy of that individual. But the reticence of the Court to apply the ‘aspirational’ policy objects in considering the substantive operation of the definition provides an adviser with no guide to the conduct of the necessarily conceptual evaluation. Consider this example: let us assume that a person that is a property owner has three properties, two listed on a property letting website and another not so listed. The information on the listing website and available lettings is about the property, although information as to the identity of the host (owner) and the identity of guests is information about those individuals. Is information about which of the three properties is not let information about the host, given a possible inference that the property may be the host’s residence? Is information about periods of past lettings also information about the individuals that let the property in those periods? Any answer necessarily requires consideration of the context of the relevant enquiry and whether that context engages the right of privacy of an affected individual. Inevitably, the policy objects of the Privacy Act must be applied to the substantive evaluation of what is ‘personal information’, but we are given no assistance as to when to apply or how to interpret those policy objects.

In summary, the reasoning of the Full Federal Court provides little guidance for Australian privacy professionals as to when facially device-related or network related information should nonetheless be considered to be information ‘about an individual’. Given the narrow, technical context in which the decision is framed, and the absence of consideration of the protection of privacy objects of the Australian Privacy Act, it is also unlikely that the decision will be regarded as persuasive in other jurisdictions. The decision illustrates the problem often confronting privacy professionals advising as to IoT deployments in determining when and how a particular context of collection, use or disclosure of information about a device that may be reasonably inferred to be in use by an identifiable individual should be regarded as information about that individual. These questions now frequently arise because personal IoT devices are becoming both more sensitively personal as well as more ubiquitous. The issues will become even more complex as services provided to share environments (such as households), or to or in shared devices (such as motor vehicles), become able to reliably distinguish patterns of usage of different individuals (i.e. distinctive driving behaviour) and analytically infer which individual is engaging in a particular activity or using the device. As the networked society and IoT continues to grow, we may be confident that cases addressing similar questions to those considered in Australian Privacy Commissioner v Telstra Corporation Limited are certain to arise for determination in many jurisdictions. The Court’s judgement usefully clarifies that the particular context of data collection and use is relevant to determination of whether information is personal information: the question cannot simply be answered by looking at whether information is of a particular type or possibly could be associated back to an identifiable individual. Unfortunately we remain unguided by the Full Federal Court when answering the question of when metadata is ‘about an individual’.

15 February 2017
Peter Leonard
Partner, Gilbert + Tobin Lawyers, Sydney
T:+61 2 9263 4003
E: pleonard@gtlaw.com.au
FEDERAL COURT INTERPRETS - 'Personal Information' What is it all about people?

BY HELEN LAUDER & VERONICA SCOTT

Kick-starting the privacy debate in Australia in 2017, the Full Federal Court has handed down its judgment in Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4.

History of appeal

The decision concerns the now infamous dispute (in the privacy world at least!) concerning the meaning of 'personal information'. A request (described by one of the judges as 'misconceived') was made by journalist Ben Grubb to Telstra in 2013 pursuant to the information access principle in the Privacy Act 1988 (Cth) (Privacy Act) for access to metadata about his mobile phone service.

While providing Grubb with some information in response to his request, Telstra had refused Grubb access to information including mobile phone network data recording IP, URL and cell tower information. Grubb complained about the refusal to the Privacy Commissioner and his complaint was upheld. Telstra then sought review of the Privacy Commissioner's decision to the Administrative Appeals Tribunal (AAT), who found (in favour of Telstra) that the information was not 'personal information' as that term was then defined in the Privacy Act. (Grubb did not participate in the AAT review or the Federal Court appeal. The Court considered the submissions of the Australian Privacy Foundation and NSW Council for Civil Liberties who had applied for leave to be heard as amicus curiae.)

Key findings

The bench of three Federal Court judges unanimously dismissed the Privacy Commissioner's appeal, making short work of the grounds of appeal, which they boiled down to (in their words) 'one very narrow question' of law. This was, whether the words 'about an individual' in the pre-2014 definition of 'personal information' in the Privacy Act have any substantive operation of their own. The Court found that they did, and that there was no appeal question before it that required re-consideration of the factual question of whether any of the metadata requested by Grubb was 'about an individual' and therefore Grubb's personal information. That said, the Court did express views on some of the information. We were also given an update on the re-identification offence Bill which will amend the Privacy Act 1988 and, which has now been referred to a Senate enquiry and Mr Pilgrim stressed the important and ongoing issue of de-identification, as well as providing an update on the activities of his Office throughout the year. He explained his role of both Privacy Commissioner and now Australian Information Commissioner and the intersection of the information laws noting the increase in people seeking access to Government information. Looking ahead Mr Pilgrim touched on the topics that his Office will be focussing on in 2017. He looked forward to the introduction of mandatory data breach notification (noting there were still many data breaches going unreported and some for long periods of time), he will be encouraging privacy by design, talking more about what the new GDPR means for Australia, developing further international cooperation in privacy governance and finally he confirmed that the Community Attitudes to Privacy Survey would be conducted. It will be launched in Privacy Awareness Week, so watch this space.

Impact

The outcome to what was the Australian Privacy Commissioner's first appeal to a superior court on the interpretation of the provisions in the Privacy Act is unlikely to be warmly welcomed, and its impact is uncertain.
The judgment also leaves Australia out of step with other countries whose jurisprudence is moving towards expanding the breadth of personal information. While confined to a very narrow question of statutory interpretation about a definition that has since been amended, the Court’s findings do not acknowledge the reality of the nature of technology driven data, and provide little practical guidance for organisations grappling with the question of when data they collect and hold will be personal information (and thus subject to the Privacy Act). This is a missed opportunity. However, it may ultimately matter little in practice, given the amended definition of personal information that has applied since March 2014 (set out in the comparison table below).

**Definitions of personal information pre and post March 2014**

<table>
<thead>
<tr>
<th>Pre-March 2014: definition considered by the Court</th>
<th>Post-March 2014: definition that applies now</th>
</tr>
</thead>
<tbody>
<tr>
<td>‘information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or’</td>
<td>‘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.’</td>
</tr>
</tbody>
</table>

(our emphasis added)

**Definition of personal information is a two-step process**

The Court effectively endorsed the approach taken by the AAT, who had decided that the metadata was not ‘personal information’ (within the meaning of the pre-March 2014 definition), because it was not ‘about an individual’. In reaching this conclusion, the AAT found there were two steps to determine whether information is personal information:

First, determine if the information is ‘about an individual’; and if so second, determine whether the identity of that individual ‘is apparent or can reasonably be ascertained, from the information or the opinion’.

Many saw this as throwing a spanner in the works, particularly as Telstra had conceded before the AAT that the metadata was about Grubb. Organisations (and agencies) that are subject to the Privacy Act have learnt to consider whether an individual can be reasonably ascertained from information, rather than focussing on whether it is ‘about’ the individual.

In appealing this finding, the Privacy Commissioner contended that splitting the question into two steps in this way was the incorrect test. Rather, if there is information from which an individual’s identity could reasonably be ascertained, then it will always be the case that the information is about the individual. In other words, ‘about an individual’ has no substantive operation itself. But the Court firmly rejected this approach, finding that ‘about an individual’ does have substantive operation.

**When information is ‘about a person’**

The Court went on to discuss and consider the required degree of connection between information and an individual for the information to be ‘about an individual’. It held that these words mean ‘the individual [needs to be] a subject matter of the information or opinion and ‘information or opinions can have multiple subject matters’.

The Court said that considering the totality of the information requested requires an ‘evaluative conclusion’ and it accepted that a single piece of information could otherwise become information ‘about an individual’ when combined with other information. Examples of Grubb’s phone colour and network type were not, it said, whether alone or together with other information, information about him. The Court did not need to consider the AAT’s conclusions that none of the metadata, such as an IP address allocated to Grubb’s mobile device, was about him, as this conclusion had not been challenged in the appeal. Had this fallen for consideration, it is not clear whether the Court, in applying the test above, would have found that the AAT erred in this regard. Its judgment suggests not.

A key difference in the current definition of personal information is that the individual does not need to be identifiable from the information or opinion. However, in relation to this, the Court stated as follows:

... whether information is “about an individual” might depend upon the breadth that is given to the expression “from the information or opinion”. In other words, the more loose the causal connection required by the word “from”, the greater the amount of information which could potentially be “personal information” and the more likely it will be that the words “about an individual” will exclude some of that information from National Privacy Principle 6.1. [para 64] (our emphasis added)

This statement could have unintended consequences for the interpretation of the current Privacy Act definition, because that definition does not include the word ‘from’. Arguably, therefore, the causal connection the Court refers to is now even looser. Although it is not entirely clear, the Court seems to be of the view that, in such circumstances, there will be more information that will not be ‘about an individual’ and therefore excluded from the scope of the Australian Privacy Principles. This is concerning.

These key passages in the judgement do not make easy reading and appear to be out of step with the approach that organisations, lawyers and privacy professionals have generally taken to their assessment of when data will be personal information. It is difficult to know how the Court’s approach would be implemented in practice because it separates two concepts that are, in reality, not mutually exclusive (which the new definition addresses). While it may be correct that information can be ‘about an individual’ without identifying that individual, it is difficult to contemplate circumstances where the converse will be true. If an individual is identifiable from particular information, how can it be that the information is not ‘about’ them?
Does it all really matter anyway?

More guidance would certainly be useful for organisations and agencies to better understand how they should assess when, having regard to all the information they hold, particular information becomes personal information. The current guidance given by the OAIC in the (non-binding) APP Guidelines (at B79) refers to examples of information 'about a person'. It states that:

- 'the personal information 'about' an individual may be broader than the item of information that identifies them'; and
- 'what constitutes personal information will vary depending on whether an individual can be identified or is reasonably identifiable in the particular circumstances'.

But, however confusing and concerning it is, the impact of the decision may in practice not be so significant because:

- the new definition of personal information does not invite the two step assessment;
- as far as metadata that must be retained by the telecommunications industry under the amendments made to the Telecommunications (Interception and Access) Act 1979 is concerned, the metadata is deemed to be personal information for the purposes of the Privacy Act; and
- the value of the voluminous and often sensitive data that many organisations and agencies seek to collect and hold, and the importance of customer trust, should mean that where there is any doubt, they should treat information they collect and hold as personal information and take care to protect and handle it in a transparent, secure and fair manner.
Commissioner, Office of the Children’s eSafety Commissioner

For the past two decades, I’ve been fortunate to have worked across the intersection of security, privacy and safety. Each is unique. During my time in the tech industry, security was considered mission-critical, with privacy and data protection rapidly nipping at its heels for attention. Both security and privacy have flourished as professions, established solid regulatory frameworks, and captured the attention of policymakers and regulators around the globe (for obvious reasons).

Online safety, though, which generally concerns some form of inappropriate content, conduct or contact, has tended to ebb and flow in terms of relative importance to security and privacy. I’ve observed that interest in online safety tends to peak every 10 years or so, often in response to a devastating incident that prompts Government attention. My first exposure to online safety was in 1995, through the shaping of the U.S. Communications Decency Act. The world was just coming online and it was critical that policymakers find the right balance between protecting people from online harms versus over-regulating the Internet out of existence. Fast-forward 10 years and a wave of panic emerged as MySpace brought up the issue of online child predation. Another decade on, we had UK Prime Minister David Cameron launch #WeProtect, and the Australian Government formed the Children’s eSafety Office, the only regulatory body in the world to exclusively tackle online safety issues impacting children.

Today, with the rise of social media, near ubiquitous connectivity and with the recognition that online civility is lacking, we are again seeing a heightened interest in online safety. In research released by the Office of the Children’s eSafety Commissioner (the Office) we noted that children as young as 8 years old are sharing personal data through social media including full names, phone numbers and home addresses. Beyond cyberbullying, and divulging too much personal information, other forms of technology-facilitated abuse such as ‘sexortion’ and ‘revenge porn’ also represent serious invasions of privacy. So, while there has always been a nexus between children’s privacy and online safety, I see an increasing convergence. It’s clear that privacy is paramount in online safety, and vice versa. Over the past few years, Privacy Commissioner Timothy Pilgrim and the Office of the Australian Information Commissioner (OAIC) have done a terrific job at elevating children’s privacy, including around apps and mobile, and we continue to work with the OAIC on joint initiatives. Indeed, privacy will continue to underpin many online safety concerns and permeate through the educational content, advice and support which is provided by the Office to our range of audiences: from young children to more digitally-savvy teens, adults, parents and grandparents. Our goal is to empower all Australians to explore the online world safely.

Understanding the principles of privacy is essential in achieving just that.

Education—from the ground up

As most privacy professionals would agree, good safety and privacy ‘hygiene’ needs to be taught early at home, reinforced through schools and refreshed throughout one’s career as technology changes and the threat environment evolves.

With even very young children able to swipe smartphone screens, use drawing apps and tune in to online videos, the risks can manifest themselves early. This is why we target the youngest and most vulnerable Australians on the basics—how to protect themselves, exhibit good behaviour online and to know who to turn to when they need support. Armed with solid skills, knowledge and principles, these children will be well prepared to handle the lightning-fast developments in technology and the internet happening now, and as they grow.
As children mature and their interests and experiences in the online world expand, we continue to meet their needs. Educational resources such as Cybersmart Challenge—a set of interactive, teacher-led activities—teach children about privacy issues including protective measures for dealing with strangers online and what happens when personal information ends up in the wrong hands.

Visit:
esafety.gov.au/education-resources/classroom-resources/challenge

Later again, as hormones surge and parental advice is less-heeded, we know that Australia’s teens face complex online safety challenges that they may not always have the maturity and resilience to handle. These issues might include sexting (and sometimes ‘sextortion’ and image-based abuse), harassment or social exclusion on social networking sites. As such, their need for relevant, up-to-date and targeted resources is high.

Our messages about privacy for teens are closely linked with digital reputation management. The Digital DNA video, which encourages teens to choose consciously online, highlights some of the key privacy points for this audience:

- choose privacy and security settings carefully and check them regularly
- choose friends wisely online—remember that not everybody online is who they claim to be, regularly review connections and remove people
- ask for permission before uploading pictures of friends.

Visit:
Digital DNA - vimeo.com/149348817

Research

In developing resources, and all the work the Office provides, we use a program of solid research to inform our work. This ensures our materials are comprehensive, current and offer an engaging way to look at some very serious issues. Privacy questions in our 2016 Digital Youth Participation Survey (in Research Insights: Young and Social Online), led to some interesting results. The 8 – 17 year olds surveyed confirmed that more teens than kids share personal information on their main social media account, and the way they did this varied. For example:

- Photo of face: kids - 47%, teens - 58%
- Last name: kids – 27%, teens - 45%
- Real age: kids - 21%, teens: 38%
- School/ photo of uniform: kids - 19%, teens - 27%
- Phone number/ address: kids - 6%, teens - 9%

How they managed their privacy also varied. Settings on their main social media account were private: 61 per cent, partially private: 21 per cent, public: 9 per cent, with 10 per cent not sure.

Visit:
esafety.gov.au/about-the-office/research-library

From the top down

It’s clear that parents play a significant role in educating their children about online safety. To meet their needs, the Office developed iParent—a targeted web portal enabling parents to learn about the digital environment and keep up-to-date about children’s technology use. The portal offers guidance for using safety settings on web-connected devices, tips for choosing movies and games and strategies for keeping young people safe online. Sharing directly with parents is another important aspect of what we do, so we offer parents and carers the opportunity to attend free online safety presentations tailored to their specific needs and concerns. Delivered face-to-face in-house, or by webinar, these presentations detail current technology trends and provide targeted online safety advice, delivered by experts in online safety.

Visit:
esafety.gov.au/education-resources/iparent
esafety.gov.au/education-resources/outreach/community-presentations#corporate

Broadening the scope

The need for online safety information is high across a range of audiences in Australia. At the Office, our remit is expanding—and we’re welcoming the opportunity to bring online safety information, resources and advice to a range of new audiences. In 2016 we launched eSafety Women, a website aimed at helping women take greater control of their online experiences. This initiative provides resources to help manage technology risks and abuse by providing the necessary tools to be confident online.
In 2017, the Office will take a lead role in combating image-based abuse, developing a national complaints portal to provide support and assistance to victims. Image-based abuse, a recent hot media topic, highlights how closely intertwined online safety is with privacy. Sam’s story, a video case study based on real life, is a strong reminder of what can happen when privacy is not respected and intimate photos are uploaded online, without consent.

Visit:
esafety.gov.au/women/take-control/case-studies
/sams-story

Events and sharing
At the Office, education and awareness raising activities are key to what we do, and with allied stakeholders and friends, we seek to communicate our online safety messages as widely as possible. February’s annual global online safety event—Safer Internet Day (SID)—provides one valuable opportunity to raise awareness. SID highlights emerging online issues and promotes safer and more responsible use of technology and mobile devices, especially among children and young people. This year the event’s theme is ‘Be the change: Unite for a better internet’. The Office is the Australian national coordinator of SID, producing a range of free resources and activities for schools and the wider community. Through this, we look to profile issues affecting young people, including unwanted contact and sharing too much information—the need for privacy. Promoted across social media, we anticipate broad support from schools, among corporates and the media.

National Privacy Awareness Week is another annual event we enthusiastically support. Working with the OAIC, our 2016 commitment included hosting event-focussed Virtual Classrooms, an eSafety Health Check poster, blog, social media content and targeted web-material. In 2017, we’ll be working on another solid program of support.

Visit:
esafety.gov.au/about-the-office/newsroom/events

Safety, security—and keeping things private
Today our world exists, in many ways, online. And with more than 80 per cent of us online and the numbers going up, there’s an increasing need for education and awareness. At the Office, we see that online safety is many faceted and that both now, and in the future, privacy will continue to be an essential, all-important part. So now, more than ever, we’re looking to harness the talents, goodwill and maturity of the privacy community to help us reach more Australians (and Kiwis, of course) and drive them to the Office’s www.esafety.gov.au resources, and complaints mechanisms. We welcome your support.

*Nielsen Online, December 2016

Julie Inman Grant Commissioner Office of the Children’s eSafety Commissioner Former Board member, IAPP ANZ
MANDATORY DATA BREACH NOTIFICATION ARRIVES IN AUSTRALIA: A REVIEW OF THE AUSTRALIAN PRIVACY AMENDMENT (NOTIFIABLE DATA BREACHES) ACT 2017
BY PETER LEONARD

On 13 February 2017 the Federal Parliament enacted the Privacy Amendment (Notifiable Data Breaches) Act 2017, inserting mandatory data breach notification requirements into the Privacy Act 1988. These provisions will replace the voluntary data breach notification guidelines as currently administered by the Privacy Commissioner and require entities subject to the Privacy Act to notify the Privacy Commissioner and affected individuals if the entity experiences a data breach of a kind covered by the Act. We review the new requirements below.

The Australian Privacy Principles (APPs) in the Australian federal Privacy Act 1988 (Privacy Act) apply to APP entities, relevantly including businesses carried on in Australia that collect or hold personal information in Australia (whether or not collected from Australian residents), Australian corporations wherever they do business and most Australian Government agencies. An entity may carry on business in Australia without necessarily having a point of physical presence in Australia and may be taken to collect information in Australia where the solicitation for collection is made from outside Australia and the information is provided pursuant to this solicitation from within Australia. As Australian privacy professionals will know, there is a small business exception to the general operation of the Privacy Act for private sector organisations in corporate groups with less than AUS$3 million consolidated group annual revenue, although this small business exception is itself subject to a number of exceptions, bringing within the Act smaller businesses that are private health service providers, that sell or purchase personal information or that are operating under Australian Government agency contracts.

Australian privacy professionals will also be familiar with the APPs unusual ‘accountability principle’. The combined operation of APP 8.1 and section 16C of the Privacy Act has the effect that generally (some limited exceptions are available in APP 8.2) an APP entity that discloses personal information to an entity outside Australia that is not itself an APP entity remains responsible for ensuring that the recipient entity complies with privacy standards equivalent to the APPs, and that APP entity is liable (accountable) to affected individuals if the recipient organisation does not. This concept had been picked up in the mandatory data breach notification provisions, such that the APP entity must make relevant notifications if the recipient entity is subject to data breach of a kind covered by the Act: in such a circumstance the APP entity is deemed to hold the information that was subject to the data breach: new section 26WC.

The core obligation as to information security arises under APP 11 - security of personal information requires APP entities to take such steps as are reasonable in the circumstances to protect personal information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure. Other provisions of the Privacy Act create equivalent obligations in relation to credit reporting information, credit eligibility information and tax file number information.

The new Act supplements the operation of APP 11 by inserting a new Part IIIC in the Privacy Act as a new mandatory data breach notification scheme for APP entities, including credit reporting bodies, credit providers and tax file number recipients. The relevant provisions are to be subject to a transitional regime and some requirements may not fully commence for 12 months after the Act commences operation: it is not yet clear just when the transition will be proclaimed as completed.

Where relevant entities experience an ‘eligible data breach’ that satisfies certain conditions, the data breach is ‘notifiable’. Only very limited exceptions will be available. These exceptions include a public interest exception of avoiding prejudicing the activities of law enforcement agencies or disclosing information where that disclosure would be inconsistent with a secrecy provision in another law.
Entities may also apply to the Privacy Commissioner for an exception from the notification requirement, either altogether or for a specific period of time. The Commissioner has an additional power to direct an entity to notify an eligible data breach.

Note that an APP entity may have fully complied with its obligation under APP 11.1 to take reasonable steps to secure personal information it holds and nonetheless be subject to a notification requirement in relation to an eligible data breach. For example, an entity may experience a eligible data breach due to human error or other circumstances that are not reasonably foreseeable. In such cases notification must be given.

An eligible data breach is where there is an unauthorised access, unauthorised disclosure or loss of personal information, credit eligibility information or tax file number information, that a reasonable person would conclude is likely to result in serious harm to any of the individuals to whom the information relates: new section 26WE(2).

Where an entity has reason to suspect that an eligible data breach may have occurred, the entity is required to undertake a reasonable and expeditious assessment of the circumstances and in any event take all reasonable steps to complete that assessment within 30 days: new section 26WH.

If an entity complies with this assessment requirement in relation to an eligible data breach of the entity and the access, disclosure or loss that constituted the eligible data breach of the entity is also an eligible data breach of one or more other entities: section 26WJ. This somewhat complex exception is intended to apply in cases where more than one entity jointly and simultaneously holds the same particular record of personal information, for example, due to outsourcing, joint venture or shared services arrangements between entities. The intended effect is that only one assessment under section 26WH needs to be undertaken into a single eligible data breach, regardless of how many entities hold the record of information. A corresponding overlap provision addresses the notification requirements and ensures that only one of the multiple entities must give notification to the Commissioner and affected individuals: new section 26WM.

In determining whether a reasonable person would conclude that an access or disclosure would or would not be likely to result in serious harm to any of the individuals to whom the information relates, specified factors to which regard should be had include the kind or kinds of information; the sensitivity of the information; whether the information is protected by one or more security measures and if so the likelihood that any of those security measures could be overcome; the persons, or the kinds of persons, who have obtained, or who could obtain, the information; if a security technology or methodology was used in relation to the information and was designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information, the likelihood that the recipients have obtained, or could obtain, information or knowledge required to circumvent the security technology or methodology; and the nature of the harm: new section 26WG.

If an entity has reasonable grounds to believe they have experienced an eligible data breach, after an assessment or otherwise, the entity must notify the Information Commissioner and affected individuals. Reasonable grounds may be either direct evidence or indirect inference: for example, a pattern of complaints may provide the entity reasonable grounds to believe that an eligible data breach of the entity has occurred.

An exception applies where an entity can determine with a high degree of confidence that it has taken action to remediate the harm arising from an eligible data breach before that harm has occurred, such that a reasonable person would conclude that the access or disclosure would not be likely to result in serious harm to any of the individuals to whom the information relates: new section 26WF.

The form of notification to the Privacy Commissioner will be a ‘subparagraph 26WK(2)(a)(i) statement’. Required information includes the identity and contact details of the entity; a description of the eligible data breach that the entity has reasonable grounds to believe has happened; the kind or kinds of information concerned; and recommendations about the steps that individuals should take in response to the data breach. The recommendations are intended to provide individuals whose information has been compromised in an eligible data breach with general advice about steps they should take to mitigate the harm that may arise to them as a result: for example, recommending that individuals request a copy of their credit report if an eligible data breach might result in credit fraud.

Notification of the contents of the subparagraph 26WK(2)(a)(i) statement must also be given to affected individuals. There are three alternative requirements or options, subject to ‘practicability’. Practicability involves consideration as to the time, effort or cost of a particular form of notification, when considered in all the circumstances of the entity and the data breach. An entity must either:

- if it is practicable to do so, take such steps as are reasonable in the circumstances to notify each of the individuals to whom the relevant information compromised in an eligible data breach relates, or
- if it is practicable to do so, take such steps as are reasonable in the circumstances to notify those individuals who are considered to be ‘at risk’ of serious harm from the eligible data breach, or
- if it is not practicable to notify via either of the above two methods, notify the statement by publishing the statement on the entity’s website and taking reasonable steps to publicise the statement. For example, if it is reasonable to do so, an entity could take out multiple print or online advertisements (which could include paid advertisements on social media channels), publish posts on multiple social media channels, or use both traditional media and online channels.
An entity might choose to notify a statement under the first option if it would require an unreasonable volume of resources for the entity to assess which affected individuals are ‘at risk’ from an eligible data breach and which are not. An example might be an eligible data breach involving unauthorised access to a customer database containing varying amounts of personal information about a large number of individuals, where only some of those individuals might be ‘at risk’ due to the eligible data breach. Notification to the entire cohort of individuals may reduce the cost of compliance for the entity, and would also allow each individual who is notified of the contents of the statement to consider whether they need to take any action in response to the eligible data breach.

An entity might choose to notify a statement under the second option when the entity is able to ascertain with a high degree of confidence that only some particular individuals are ‘at risk’ from the eligible data breach. For example, if the entity was able to determine that the only likely result of serious harm from the eligible data breach would involve payment information stored in relation to a specific subset of the broader ‘cohort’ of individuals such that only that subset is ‘at risk’ from the eligible data breach, the entity might choose to notify the contents of the statement to those individuals only.

Entities must comply with the obligation to notify individuals as soon as practicable after preparing the subparagraph 26WK[2][a][i] statement and providing it to the Privacy Commissioner. Where an entity normally communicates with an individual using a particular method, any notifications provided to the individual may use that method. Where there is no normal mode of communication with the particular individual the entity must take reasonable steps to communicate with him or her. Reasonable steps could include contact by email, telephone or post.

The Commissioner has a constrained power to grant an exemptions in the public interest from the requirement to provide notification to affected individuals: new section 26WQ. Examples of such public interest are where there is a law enforcement investigation being undertaken into a data breach and notification would impede that investigation, or where the information concerns matters of national security.

The mandatory data breach notification scheme is connected to the existing enforcement framework under the Privacy Act. This means that the Privacy Commissioner’s existing investigatory powers will apply in the event that an entity breaches a requirement of the scheme. The Commissioner may investigate possible noncompliance with the mandatory data breach notification scheme and potentially make a determination requiring the entity to remedy such noncompliance. In the case of serious or repeated noncompliance, the Commissioner may also apply to a court to impose a civil penalty.

The Privacy Amendment (Notifiable Data Breaches) Act 2017 was significantly amended from earlier draft bills following criticism of drafting deficiencies and ambiguities in these earlier drafts. The mandatory data notification scheme as enacted is easier to understand and apply. Australian privacy professionals will know that the Office of the Australian Information Commissioner already receives voluntary data breach notifications and has extensive experience in assessing such notifications. The Commissioner has issued a Guide as to the Commissioner’s expectations as to such notifications: OADC, Data breach notification — A guide to handling personal information security breaches, August 2014. That Guide also sets out a data breach response process which can be expected to continue to be the Commissioner’s view as to the process of triaging data breaches, as now supplemented by these additional mandatory requirements. Although the Commissioner’s Guide was based upon a different threshold (‘real risk of serious harm to an individual’), it should be readily capable of adaptation to this new scheme. We may expect to see new guidance from the Commissioner over forthcoming months.

Peter Leonard
Partner, Gilbert + Tobin Lawyers, Sydney
T:+61 2 9263 4003
E:pleonard@gtlaw.com.au
I came across Cathy O’Neil at the IAPP Academy’s annual conference in San Jose in September 2016. Cathy was a keynote speaker and had just released her book, “Weapons of Math Destruction”. Her presentation struck a nerve with the audience, because by the time I was at the queue to buy her book, it had already sold out. Nevertheless, I got hold of a couple of advance copies from Amazon prior to its Australian release late last year.

I have been recommending this book as a must read and it seems to have found its way into the popular press here in Australia, with two articles I came across recently quoting from it. One was in the Sydney Morning Herald, “How Centrelink unleashed a weapon of math destruction”, 8 January and another in the Australian Weekend Financial Review, “Oh, algorithms, you don’t know me at all”, 28 December 2016 – 2 January 2017. Also, the Association for Computing Machinery US Public Policy Council (USACM) released a “Statement on Algorithmic Transparency and Accountability” on 12 January 2017 – focusing on steps to prevent algorithmic bias.

As such, I thought it was timely to give Cathy O’Neil’s book a review for iappANZ members.

Contrary to popular notion, not all data scientists are big data evangelists. Cathy O’Neil is a data scientist, has a PhD in Maths from Harvard, taught at Barnard College, worked for a hedge fund DE Shaw and worked at various startups building models that predict people’s purchases and clicks. Based on her experience, the author looks at the dark side of big data.

What is a Weapon of Math Destruction (WMD)?
Firstly, the title of the book lends itself to an unforgettable name and conjures up the nasty impacts of weapons of mass destruction in the physical world. Here is how the author classifies models and algorithms that produce automated decisions as WMDs:

<table>
<thead>
<tr>
<th>WMDs</th>
<th>Opposite of WMDs</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Opaque (we are modelled as shoppers, patients, loan applicants etc) – we see little of that modelling</td>
<td>- Transparent</td>
</tr>
<tr>
<td>- Unregulated</td>
<td>- Controlled by user and personal</td>
</tr>
<tr>
<td>- Uncontestable (without feedback a statistical engine can continue with faulty and damaging analysis while never learning from its mistakes)</td>
<td>- Shared objectives</td>
</tr>
<tr>
<td>- Have massive scale and damage.</td>
<td>- Updated</td>
</tr>
<tr>
<td></td>
<td>- Auditable</td>
</tr>
<tr>
<td></td>
<td>- Accountable</td>
</tr>
</tbody>
</table>

WMDs encode human prejudice, misunderstanding and bias and often punish individuals who happen to be the exception. People think that because a machine made the decision it can’t be biased – well that is a fallacy for a WMD.

Real life examples – WMDs
Being an American, most of the author’s examples are US based – it would be great to see some global examples from different cultures. The author starts the book with the story of Sarah Wysocki which made the press in 2012 and about whom journalists wrote extensively. Sarah was a 5th grade school teacher, who was dismissed as a bad teacher based on a WMD. She had excellent reviews from principals, students and parents. A new scoring system called IMPACT was launched to “measure” teaching effectiveness. IMPACT measured the educational progress of students and then calculated how much of their advance or decline could be attributed to the teacher. Many complex variables effectively led to random outcomes. Sarah was fired and the next day hired by a private school.
Another example is University rankings generally that lead to perverse incentives and outcomes. In particular, the author focused on the US News Best Colleges Ranking example. Rankings force everyone to shoot for the same goals, which creates a rat race and lots of harmful unintended consequences. In that particular example, she writes about the cost of tuition not being included – hence a contributing factor to skyrocketing costs of education in the USA. Since then, according to the author the US Department of Education has intervened to try to address this problem.

The prison and police systems also offer interesting WMDs. The author highlights the models that determine the risk of recidivism (re-offending) in determining jail sentences for convicted persons. She argues that the model itself contributes to a toxic cycle and helps to sustain it. The algorithms use proxies – like what the family of convicted persons do, where they live, previous offences, people like them, etc. This is where “people like you” that are deemed to be “you” has serious consequences. Price optimization is another area in which WMDs are used. The author provides an example from AllState Insurance which offered discounts of 90% off the average rate to 80% increases. It massively varied the cost of premiums, based on analyzing consumer and demographic data to determine the likelihood that consumers would shop for lower prices. A consumer deemed less likely to shop for lower prices would be charged more. The author states that every person had a different experience, and the models were optimized to draw as much money as they could from the desperate and ignorant.

Social media platforms and search engines are another minefield for WMDs. Platforms, like Facebook make judgments about which friends see what posts. They determine what we see and learn, much like search engines. These platforms are massive, powerful and opaque. As an aside, a new blog on the harmful privacy policies of Facebook was released in the New Year and writes about getting off Facebook to save your relationships with your friends.

Studies into search engines have tested undecided voters to see if they can be swayed in a particular direction depending on the search results they see. The author refers to a study into undecided voters in the USA and India, where these individuals were asked to use search engines to learn about upcoming elections. The search engines they used were programmed to skew search results, favouring one party over another. Those results shifted voting preferences by 20%. Pew Research shows that 73% of Americans believe search results are “accurate and trustworthy”, which in my view would place massive accountabilities on those providers (much like the press). Indeed, Angela Merkel complained about the lack of search engine transparency endangering debate in The Guardian late last year.

**Good examples of automated algorithms/models**

It would have been remiss of the author had she not included what a good automated algorithm/model looks like. Here, the author provides the well-known example of baseball (think about the movie Moneyball).

In baseball, predicting who will win, understanding how to put a winning team together or how to play your best against upcoming opposition can all be fed by data. These models are generally:

- **Transparent** - fans, players, managers have access to the statistics (home runs, strikeouts) and can more or less understand how they are interpreted
- **Continually updated** - new games are fed in and mistakes to models corrected
- **Relevant** - Assumptions and conclusions are transparent ie: data is highly relevant to the outcome that is trying to be predicted
- **Direct sources** - Statistics come from direct sources, not proxies: ie: actual footage of games and scores
- **Shared Objectives** - People being modelled understand the process and share the model’s objectives, for example winning and predicting baseball games

**Lessons learnt**

The top takeaways, in my view, from the book are as follows:

- **Human decision making, while often flawed, has one chief virtue – it can evolve (it will be interesting to see how effective machine learning algorithms become)**
- **We have to explicitly embed better values into our algorithms, creating big data models that follow our ethical lead**
- **Standards can protect companies that want to do the right thing – because their competitors have to follow the same rules**
- **Like doctors, data scientists should pledge a Hippocratic Oath, one that focuses on the possible misuses and misinterpretations of their models**
- **Today the success of a model is often measured in terms of profit, efficiency or default rates - fairness and common good resist quantification. As such it is necessary to impose human values on these systems, even at the cost of profit or efficiency.**
- **The impact of models needs to be measured and audits of algorithms need to be conducted and feedback loops built in. Models must deliver transparency, disclosing the input data they’re using as well as the results of their targeting.**
Conclusion

It is great to read a practical book from someone who knows how to build algorithms and models and knows their dangers. We certainly have moved a long way from “nobody knows you’re a dog on the internet” to being ranked, categorized and scored on the basis of our data trails (whether accurate or not).

Annelies Moens
Deputy Managing Director
Information Integrity Solutions
Former President of iappANZ and Founding Treasurer
amoens@iispartners.com
2017 has opened with a raft of developments with privacy impacts - from new mandatory data breach notification laws in Australia, to the US use of executive orders (and their impact on US Federal privacy practices), to the Federal Court’s decision in the Telstra case, to the proposed criminalisation of “re-identification” of previously de-identified data held by the Australian public sector.

There’s also the prospect of law reform in New Zealand, and many iappANZ members working in organisations with a global reach or global customers are coming to terms with the impending General Data Protection Regulation (GDPR) in the EU - and what that means in this part of the world.

We’ve asked our iappANZ board members some subcommittee members to provide us with some headline thoughts about one or more of these things, and what they may mean for privacy professionals in 2017 ....

On GDPR: Marta GANKO: It’s time for ANZ organisations to start moving towards one of the most consumer-centric data protection regulations in the world. While many fear the compliance obligations, others are embracing the competitive opportunities that will be made available such as incentives for individuals to port their data from competitors, potentially exposing the shortcomings of other organisations should this not be possible. New provisions around consent management, portability and understanding where data is at all times will challenge organisations to get their data management house in order operationally. With most of these changes requiring technology changes to achieve sustainable compliance, May 2018 is a looming deadline.

Chris Rogers: With just over 15 months until the EU General Data Protection Regulation (GDPR) becomes enforceable, organisations which have operations within the EU, which carry out business with EU resident customers or which monitor individuals in the EU will be busy in 2017 getting their “house in order”. Compliance with the GDPR includes activities such as the appointment of data protection officers within an organisation, establishing a data breach notification process so that data breaches are reported to the relevant data protection supervisory authority without undue delay, establishing a process for conducting privacy impact assessments, and updating privacy policies and notices so that they include required content and also present to recipients concisely and in clear plain language. A failure to comply with the GDPR carries with it significant penalties, data protection authorities can impose fines of up to 4% of a corporate group’s total annual worldwide turnover. The Article 29 Working Party, the group which represents EU data protection authorities, has been issuing guidelines to help organisations get prepared for the GDPR. These are available on the European Commission’s website and privacy professionals would be well advised to monitor and review these guidelines as they prepare for the commencement of the GDPR.

On law reform in New Zealand

Daimhin Warner: New Zealand is approaching a privacy law change that should strengthen privacy rights for NZ’ers while providing clarity to the agencies required to put these rights into practice. This reform landscape is anything but stable though, and it remains unclear when we will see a new Privacy Act. The NZ profession has known for some time to expect mandatory breach notification, new cloud computing accountability obligations and increased powers to make binding orders for the Privacy Commissioner. Agencies in NZ have had time to come to terms with these changes and plan for them.

However, in February 2017, the Privacy Commissioner made a new set of recommendations designed to ensure that the law reform process remains up to date (remember, the current direction of our new Privacy Act was set by the Law Commission in 2011 - some 6 years ago).
The Commissioner, reflecting on recent developments in the EU, is now recommending further changes to the law that will make privacy rights more robust and privacy obligations more real, including:

- civil penalties for non-compliance of up to NZ$100,000 for individuals and NZ$1,000,000 for agencies;
- an individual right to data portability;
- a power for the Commissioner to demand assurances of compliance from agencies; and
- New provisions on re-identification.

These changes, if accepted, will significantly alter the privacy landscape in NZ. They are necessary if we are to retain our EU adequacy status - an important status for a small country set on developing and providing innovative services to an international market. They will also give privacy officers and other professionals renewed impetus to drive privacy programme improvements. These are exciting times.

**On Mandatory Data Breach Notification**

Carolyn Lidgerwood: With mandatory data breach notification legislation passing through the Australian Parliament recently, Australian ‘APP entities’ have 12 months to update their processes so that they are ready to comply. Some if not many larger companies will already have internal processes in place to comply with the OAIC’s current voluntary notification requirements, but many will not. Either way, there will be work to be done in updating processes or establishing new ones. Perhaps one of the most critical steps will be educating your business teams about what ‘personal information’ actually is (we privacy professionals may ‘know it when we see it’, but don’t assume that everyone does), and what types of ‘data breaches’ need to be reported (both internally and externally to the Commissioner). Internal reporting of incidents (eg to the person responsible for your company’s privacy programme) is very important. This will mean the can ensure the incident is properly investigated, any harm to individuals is addressed, and that the required assettens (and any required notifications) are made. But they can’t do that if no-one tells them that the incident has occurred.

**On the US Executive Order**

Veronica Scott: Privacy professionals must always be alert to the potential for developments in other jurisdictions to impact on their organisations’ privacy practices and the personal information they hold. In the wake of attempts by US Federal agencies to access personal information held in overseas servers of US companies, incoming US President Donald Trump’s recent Executive Order aimed at ensuring the public safety of American people and support US immigration laws, has implications for the privacy of all of ‘aliens’ (non-US citizens).

Federal agencies are subject to the US Federal Privacy Act 1974 which requires them to meet particular minimum privacy standards for personal information of US citizens and lawful residents in their databases and which they process. The standards that have been implemented reflect the Federal Trade Commission's model Fair Information Practice Principles (FIPPs). US Federal agencies have historically applied the same approach when handling personal information of non-US citizens / lawful residents, and this was mandated for EU citizens by the outgoing Obama administration through legislation. However the effect of section 14 of the Order means that US federal agencies can lawfully ignore the FIPPs in their policies for processing personal information of Australians (and citizens of countries outside of the EU) and will change their privacy policies and practices in relation to this information. This could include making disclosures without consent, and refusing access and correction requests. This has potential implications for Australian entities who transfer personal information of non-US and non-EU citizens/residents to the US which may be disclosed to and held in the databases of US Federal agencies as agencies will not be required to handle this information in accordance with the FIPPs. The main impact is likely to be on immigration processing (for example, Australian employees who may need a visa to work in the US). It is cause for organisations to pause and consider their practices and notices in relation to cross border disclosures to the US. There also remains a question about the impact of the Executive Order on the EU-US Privacy Shield (which protects EU citizens’ data transferred from the EU to the US) as it applies to enforcement agencies. However, the EU has said there won’t be changes to this.

**On Data Privacy Officers / DPOs**

Melanie Marks: Is it time to move to Europe? The General Data Protection Regulation (GDPR) must be one of the most uttered phrases in privacy practice at the moment. For privacy professionals in Australia, the GDPR will open up new opportunities to broaden skills and work abroad.

The GDPR introduces a general EU-wide obligation to appoint a data protection officer (DPO) for controllers and processors involved in high-risk processing activities, i.e., where one of a company’s core activities is the large-scale monitoring of individuals or processing of sensitive data. After much debate (particularly from Germany), the GDPR requirement will not override stricter national requirements for a DPO in the relevant Member State. Countries requiring mandatory appointment of DPOs include Germany, Hungary, Spain and Croatia. This clearly means a period of significant growth in demand for our profession and Aussies and Kiwis with European working entitlements might take this opportunity to capitalize on the opportunities that will abound in Europe. Some have speculated that the new GDPR requirement for a DPO will require some 75,000 professionals to meet this need. Perhaps it’s time to register for IAPP training and brush off your passport?
Olga Ganopolsky: In the EU, most organisations that are in the public sector or process personal data requiring ‘regular and systematic monitoring of data subjects on a large scale’ as part of their ‘core activities’ have long accepted the need for a Data Protection Officer (DPO) and either have appointed or will soon appoint a DPO in compliance with Article 37 of the new GDPR.

The GDPR is reasonably clear as to what qualifications or qualities the DPO should have, what tasks a DPO is to perform (see Article 38) and what protections are to be afforded to the DPO by the organisation. The GDPR is less clear or prescriptive as to where the DPO role fits organisationally.

This has naturally opened a debate about a suitable organisational structure for DPOs in the EU. These considerations are also relevant to Australian and New Zealand agencies and organisations who are considering the appointment of a DPO to oversee their privacy compliance programs. So - where to put the DPO? Like many things in data protection the answer is - ‘it depends’. It can depend on its size, structure, and the nature of the organisation's data processing operations and the risks posed.

In a smaller organisations where there is appetite for multitasking, the DPO can be a combined role with another independent risk functions such as head of legal or suitably senior roles such the CISO, the COO. In customer facing data processing organisations a senior customer facing role may also work well. In larger organisations where there is an emphasis on specialisation, the function of the DPO naturally moves to dedicated roles in the traditional risk functions such as legal or compliance. Legal is typically involved in the giving of advice and compliance in the conduct of monitoring and audit activities envisaged in Article 39. These functions have a tradition of independence and can address the requirement for avoidance of conflicts of interests seamlessly.

The fact that the DPO function can be shared by entities and performed by contractors (see Article 37(6)), has also opened the possibly of an outsourced model, where external legal or risk advisers could perform the role. This can be applied to different organisations and lends itself well to multinational structures where there may be a need to bring in local expertise to support particular local needs. What do you do if the DPO can be in all or some of the functions? Once you have identified a suitably qualified individual and nominated the direct reporting line to the ‘highest level of management (per Article 38(3)), how do you make that decision? What is the key or overriding factor? The key (to me) is that the DPO is a governance role - governance of personal data. This is certainly relevant in the ANZ context too. As such, the chosen structure needs to fit within and complement the overarching duties of accountability, transparency and privacy by design. To be truly successful, in addition to the ‘expert knowledge of data protection law and practices’ (required under Article 37(5)) the DPO must by necessity focus on the protection aspects of data protection – the protection of the rights and freedoms of individuals, which are fundamental rights. There is much to weigh up but having a DPO in place will help take your privacy program forward.