Contents

1 / PRESIDENT’S FOREWORD
Melanie Marks

2 / AN INTERVIEW WITH 2017 WRITING PRIZE WINNER, KATRINE EVANS

3 / THE EXPANDING DEFINITION OF PERSONAL INFORMATION
Katrine Evans

4 / DATA SHARING WITHIN GOVERNMENT - DATA SHARING FRAMEWORKS
Dr. Ian Oppermann

5 / AN INTRODUCTION TO THE DELOITTE AUSTRALIAN PRIVACY INDEX 2018
FIVE QUESTIONS WITH DAVID BATCH AND TOMMY VILJOEN

6 / PRIVACY, TRUST AND MY HEALTH RECORD
Bernard Robertson-Dunn

7 / DIGITAL POLICY: A NEW SPACE FOR HARNESSING THE WISDOM OF OUR KIDS
Nicole Stephensen

8 / GDPR AND THE HEALTH CARE INDUSTRY – CONSENT, ERASURE & AUTOMATED DECISION MAKING
Jennifer Wills

9 / THE PAGEUP DATA BREACH – EMPLOYEES, SERVICE PROVIDERS AND THE PRIVACY ACT
Lyn Nicholson

10 / AI, ALGORITHMS AND PERSONAL INFORMATION: A RIDDLE, WRAPPED IN A MYSTERY, INSIDE AN ENIGMA
Frith Tweedie

11 / LEGISLATION CORNER AU AND NZ

12 / UPCOMING EVENTS
Author Guidelines - subject to the discretion of the editor

Criteria for articles

1. An original article – one that is different and reworded from any article that you have published to a broad audience on this topic AND has a different heading than any article you have published on this topic, but may be based on an earlier published article.

2. Generally, between approximately 600-2500 words. This broad range notes that subject matter may vary from technical and complex to short and topical.

3. For a longer, more technical article, we may publish by instalments.

4. For articles that have been broadly published, we may publish a summary and link to full text.

5. We cannot accept images sourced from the internet due to copyright. Images from ATMOSS or ADDS will be accepted.

Copyright and Licence

1. Copyright in the article at all times remains with the author.

2. No fees are payable by iappANZ.

3. Author grants to iappANZ a world-wide royalty-free non-exclusive licence to publish the article in material form and online to reproduce the article for those purposes and to edit as is reasonably required by iappANZ for publication purposes.

4. The author may republish the article elsewhere once it has been published in the journal.

Acknowledgement

1. iappANZ will use all reasonable endeavours to ensure that the author’s name is published with the article.
I’d like to start this month’s edition of Privacy Unbound by thanking our contributors and journal committee (led by Lyn Nicholson), all of whom give their time voluntarily to compiling and delivering each edition to your inbox. One of the difficult decisions that our journal committee has faced recently is whether to keep our prized content behind a paywall, available to members only, or to make it freely available to anyone interested. On the one hand, access to content is a unique member benefit, and value shouldn’t be eroded by giving the milk away for free! But on the other, the world has changed and providing open content is a way of connecting with a broader community – both for us as an association and for our members who might like to share the things they are reading with others.

The result is a new publications page on our website, where all content will be made freely available three months after its initial delivery to member inboxes. So - members get the scoop first, and three months later, so too can others. The publications page is part of our 2018 website uplift.

The iappANZ 2018 Summit (on 1 and 2 November in Melbourne) is now open for registration. You can view the program, featuring speaker bios and presentation topics and you can register on our Summit website. At the date of writing, earlybird rates were still open (but I’m told on good authority, are closing imminently!) We would love to see you there.

Now on to this edition of Privacy Unbound...

In this edition, Katrine Evans, our 2017 writing prize winner and former New Zealand Assistant Privacy Commissioner shares her insights and experiences as a privacy professional and lover of the Marlborough region (who isn’t!) Read on for Katrine’s award-winning article on the expanding definition of personal information.

Deloitte’s Tommy Viljoen and David Batch give us some insights to the Deloitte Privacy Index 2018. Now in its fourth year, the report outlines how Australia’s 100 top brands fare in relation to privacy and transparency.

Next, we hear from Dr Bernard Robertson-Dunn on the topic de jour, the My Health Record system. If you have been wondering how the system works and what the fundamental privacy and security questions are, this is an excellent primer.

Nicole Stephenson visits her roots back in Prince Edward Island to bring back the story of the new Joe Alhadeff Youth Digital Policy Center, a collaborative venue for children to work alongside and coach world experts in digital policy.

The GDPR, consent, automated decision making and healthcare. What combination of terms could evoke greater complexity in law and ethics? Jenny Wills draws on her experience as the Chief Privacy Officer at Orion Health to bring us her insights.

Lyn Nicholson, editor in chief and general counsel, presents an analysis of the PageUp data breach which tests the operation of Australia’s principles-based system, particularly where a breach occurs in the system of a service provider. In these circumstances, who should be contacting the individuals? What legal liability does PageUp and each of its customers hold?

Finally Frith Tweedie of EY takes a thought provoking look into the world of AI and how algorithms and personal information interact, or don’t.

Turn to the back of this edition for a snapshot of legislative changes impacting privacy in Australia and New Zealand in recent months.
Katrine is the winner of the 2017 iappANZ writing prize and privacy unbound asked her a few questions about her professional life, what makes her tick and her favourite spot.

Other than "keep up to date on the law reform process and get ready for it" what additional tips and suggestions would you give to fellow privacy practitioners?

I think the best privacy practitioners are those who can effectively communicate and work with experts in other disciplines. So take the opportunity to learn about topics like new challenges in information security, find out how the data dudes operate, understand what the day-to-day realities are for front-line staff, maybe track some of the social science literature. Push yourself beyond your comfort zone - you never know what you'll find.

What is your current role and how did you come to be a privacy professional?

This is career v.3 for me as a privacy professional. I started out as an academic, teaching at Victoria University Law Faculty. I'd got hooked on privacy back in 1991 during my undergrad degree so when I started teaching I ended up doing my LLM thesis in the area as well as setting up Vic's privacy course. Teaching and researching took me through to late 2004 when I moved to the Privacy Commissioner's office for ten and a half years as Assistant Commissioner and general counsel. I've been in legal practice for three years now and have had to learn to charge for my advice. That's still something I find surprisingly hard, having nattered about privacy for free for my whole professional life!

Why did you join iappANZ?

I've always been a fan of iappANZ, right back to when it was an idea in a few enthusiasts' minds. Privacy professionals can find themselves isolated in their organisations, and the work they do isn't always that well understood by folks in different disciplines (including in legal teams). So I really value having a network that encourages people to share their experience with one another, that runs events that enable us all to learn, and that provides a framework to help us know and support one another. Also, too often, the work of privacy professionals is still undervalued, I think - they don't have

Katrine is a specialist in privacy and information law at Hayman, Lawyers, Wellington.

Katrine did her first degree in languages at University College, Oxford before moving to Wellington in 1988. She then succumbed to the lure of law studies at Victoria University, including doing her first work in privacy law in 1992, and hasn't looked back since. She completed her LLB (Hons) and LLM and spent ten years indulging her delight in teaching, as a lecturer specialising in privacy, media and tort law.

In 2004 Katrine became Assistant Privacy Commissioner and was the Commissioner's legal counsel until June 2015. She gave legal advice about complaints, and represented the Commissioner in the Human Rights Review Tribunal and in court (including the Supreme Court). She managed the policy and technology team giving a wide range of advice to government and business, and advising on the privacy law reform proposals. For many years, she was also the communications manager, producing a variety of guidance material for the public, schools and businesses.

She is a member of the New Zealand Law Society's Human Rights and Privacy Committee, edits the "Privacy Interests" column of the IEEE's "Security and Privacy Journal", is a member of the Asian Privacy Scholars Network, and co-teaches the LLM course in privacy law at Victoria University of Wellington.
the influence in organisations or the ear of the C-suite in the way that they need to if those organisations are genuinely to improve their privacy performance. It's improving, but the more privacy is seen as a profession, with its own disciplines and qualifications, the more likely that is to change. iappANZ is a fundamental part of making that change happen.

Your prize-winning piece - what inspired you to write it?

I've always been fascinated by how we define "personal information" - it's something I've talked about at conferences and written about before. It's a gateway to legal protection, so what it means really matters to ordinary people at a very practical level. It can also be really hard, particularly with the increasing complexity of the information environment, and it ties in with one of the hardest questions of all: how do you define "privacy"? I like trying to puzzle out hard concepts and make them work in the real world. I also like trying to explain those concepts in a way that non-specialists might find interesting.

We all know about re-identification, big data, IOT and anonymisation - what do you foresee as the new privacy issues we will be facing in 2022?

Automated decision making, and the difficulties with creating true transparency about how those decisions are made, will no doubt be a growing concern over the next few years. It'll also be interesting to watch how effective our regulatory models are. We've got some tough new enforcement options (including significant fines) coming into play in a variety of jurisdictions - how will they be used, will they create the right incentives, and will they really make a difference to the rights of individuals?

The Privacy Act is turning 25. What's your birthday message?

It's great that the Privacy Act is being updated and several of the new provisions (like the new powers for the Privacy Commissioner) are a real step in the right direction. Let's tidy up these aspects of the Bill and pass it quickly. But this mustn't be the end of it. If we're to provide genuinely effective protection for individuals in the next decade, we need to get some further amendments drafted as soon as possible. A lot's changed since the Law Commission reported eight years ago.

Favourite place in NZ and why? Perhaps a photo of your favourite place if you have one?

My favourite place in New Zealand is probably the Marlborough Sounds. So close to home, and yet so far away from work. No cell phone connection in places. Fabulously beautiful walks.
The Expanding definition of personal information

By: Katrine Evans - Reproduced from Privacy Unbound Edition 77, 2017

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

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

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

Developments in the information landscape

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

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

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

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

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

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

What the statute says

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

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

- information
- about
- an identifiable
- individual

Information

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

The importance of the term is therefore not that it limits what “information” covers – it is that there is no limitation. “Information” goes beyond documents or particular formats. It includes information in a person’s memory and in conversations as well as tangible documents or electronic records. It is not restricted to sensitive information – the blandest, most public items are still “information”. The other elements of the definition create...
the limits. All three are needed before something is personal information. For instance, the contents of a file with someone’s name on are not necessarily all personal information. The information might be linkable to an individual and be retrievable by reference to them, but it might not all be “about” that individual.

**Individual**

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

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

**Identifiable**

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

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

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

**About**

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

It tends to depend on the way in which you phrase the question. Take the case of *Apostolakis v Sievwrights*. Mrs Apostolakis’ lawyer wrote to the mortgagee of her property to say that the building’s insurance either had lapsed or was about to lapse. Was this information about the building (“this building is uninsured”) or about her (“Mrs Apostolakis has not insured her building”)? The Tribunal, and later the High Court, said that it was clearly the latter. The information was about her responsibilities in relation to the property.

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

Other examples include:

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

The upshot is that personal information is inherently contextual, which can be frustrating for those seeking a brighter line.

**Recent cases reflect the difficulties**

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

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

- The cookie ascribed a unique ID code to the device allowing tracking of website visited, times visited, time spent, etc
- Devices are generally used exclusively by a single user. Identifying the device therefore tracks the habits and interests of real individual users;
- Google’s own business model is based on ability to individuate users and target advertising;
- It is immaterial that the agency might not intend to link up the information with other information it holds. The question is whether it can do so if it wishes.
Towards the other end of the scale are recent Australian developments. Ben Grubb’s request to Telstra for his telecommunications metadata resulted in see-sawing legal opinions. The Privacy Commissioner agreed information such as times, durations and locations of calls were about him as an identifiable person, particularly as it would routinely be made available to the police if they were investigating him. The Administrative Appeals Tribunal disagreed: it suggested if the agency hadn’t collected information with the purpose of knowing something about the individual, it wasn’t “personal” — it was information about the underlying telco system. The Federal Court stepped back from that, but too narrowly suggested that the individual has to be “the subject matter of the information or opinion.” It’s probably fortunate that the new legislation is clearer and the facts are relatively easily distinguishable.

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

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

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

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

Dealing with the uncertainty

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

Most importantly, it’s only a gateway to say the Privacy Act is relevant at all. If something is personal information,

You quietly step to seeing how the privacy principles say you should be handling that information to deal fairly with people.

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

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

We can therefore be relatively relaxed about letting a lot through the gateway. The Act has its own inbuilt mechanisms to make sure that liability is limited to situations where there are genuine problems.

And if something has the capacity to materially affect someone, and cause them harm you should let it through the first gateway. It forces you to figure out how to mitigate the risks. The result will be that you have much more principled and trustworthy business practices.

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

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

Law reform solutions that will assist include:

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

We also need to invest in creating trustworthy environments, based on inclusion, control and transparency.
If we do this perhaps we can chill a bit about what personal information means – and just enjoy the collegial arguments that it inevitably creates.
Data Sharing Within Government - an overview

A Data Taskforce is exploring privacy preserving frameworks to support automated data sharing which in turn facilitates smart services. The framework will address technical, regulatory, and authorising frameworks. The intention is to identify, adopt, adapt, or develop frameworks for data governance, privacy preservation, and practical data sharing which facilitates smart service creation and cross jurisdictional data sharing between governments. The approach is to identify best practice where it is known to exist; consider existing models in an Australian privacy context or identify “whitespace” opportunities. This overview is provided in the context of the current technical whitepaper sponsored by the ACS, and current proposals for data sharing in Australia. There is no conclusion, there is ongoing work to be done, and for privacy professionals this paper provides an overview of a framework.

1. CONTEXT

Personal data covers a very wide field and is described differently in different jurisdictions. In the NSW context1: "… personal information means information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion".

The definition is very broad and in principle, covers any information that relates to an identifiable, individual living or within 30 years of death.

The ambiguity about the presence of personal information in sets of data highlights the limitations of most existing privacy regulatory frameworks. The inability of human judgment to determine “reasonable” likelihood of reidentification when faced with large numbers of complex data sets limits the ability to appropriately apply the regulatory test.

Development of standards around what constitutes “anonymised” would help to address the challenges of dealing with privacy. In all parts of the world, there is currently only very high-level guidance, and certainly nothing quantitative, as to what “anonymised” means, hence many organisations must determine what “anonymised” means to them based on different data sets.

Technology can potentially play a role to address this challenge but agreeing and then communicating what an acceptable degree of anonymisation is, and how to achieve it in quantitative terms, would also greatly improve data sharing. This clarification of existing legal frameworks needs to include quantified descriptions of acceptable levels of risk in ways which are meaningful for modern data analytics.

2. DATA SHARING FRAMEWORKS

Australian Data Sharing Framework Development

In September 2017, the Australian Computer Society (ACS) released a technical whitepaper which explored the challenges of data sharing2. This paper was the culmination of more than 18 months’ work by a taskforce which included ACS, the NSW Data Analytics Centre (DAC), Standards Australia, the Office of the NSW Privacy Commissioner, the NSW Information Commissioner, the Federal Government’s Digital Transformation Office (DTO), CSIRO, Data61, the Department of Prime Minister and Cabinet, the Australian Institute of Health and Welfare (AIHW), SN-NT DataLink, South Australian Government, Victorian Government, Western Australian Government, Queensland Government, Gilbert and Tobin, the Communications Alliance, the Internet of Things Alliance, and a number of interested companies.

Modified “Five Safes” Framework

The whitepaper introduced a number of conceptual frameworks around data sharing. One of these, the modified “Five Safes” framework3, is designed to ensure that data used for research purposes is shared in a way that maintains privacy.

The “Five Safes” framework defines the following principles:

1. Safeguard the data from unauthorized access.
2. Safeguard the data from unauthorized use.
3. Safeguard the data from unauthorized disclosure.
4. Safeguard the data from unauthorized modification.
5. Safeguard the data from unauthorized destruction.

The modified framework adds an additional layer of protection, ensuring that data is shared in a way that maintains privacy and reduces the risk of reidentification.


frameworks for practical data sharing including an adapted version of the “Five Safes” framework. A number of organisations around the world including the Australian Bureau of Statistics use the Five Safes model to help make decisions about effective use of data which is confidential or sensitive. The dimensions of the framework are:

**Safe People** – refers to the knowledge, skills, and incentives of the users to store and use the data appropriately. In this context, ‘appropriately’ means ‘in accordance with the required standards of behaviour’, rather than level of statistical skill. In practice, a basic technical ability is often necessary to understand training or restrictions and avoid inadvertent breaches of confidentiality; an inability to analyse data may lead to frustration and increases incentives to ‘share’ access with unauthorised people.

**Safe Projects** – refers to the legal, moral, and ethical considerations surrounding use of the data. This is often specified in regulations or legislation, typically allowing but limiting data use to some form of ‘valid statistical purpose’, and with appropriate ‘public benefit’. ‘Grey’ areas might exist when ‘exploitation of data’ may be acceptable if an overall ‘public good’ is realised.

**Safe Setting** – refers to the practical controls on the way the data is accessed. At one extreme researchers may be restricted to using the data in a supervised physical location. At the other extreme, there are no restrictions on data downloaded from the internet. Safe settings encompass both the physical environment (such as network access) but also procedural arrangements such as the supervision and auditing regimes.

**Safe Data** – refers primarily to the potential for identification in the data. It could also refer to the sensitivity of the data itself.

**Safe Outputs** – refers to the residual risk in publications from sensitive data.

The Five Safes model is relatively easy to conceptualise when considering the extreme cases of ‘extremely Safe’ although it does not unambiguously define what this is. An extremely Safe environment may involve researchers who have had background checks, projects which have ethics approval and rigorous vetting of outputs. Best practice may be established for such frameworks, but none of these measures is possible to describe in unambiguous terms as they all involve judgement.

The adapted model explores different, quantifiable levels of “Safe” for each of People, Projects, Setting, Data and Outputs as well as how these different “Safe” levels could interact in different situations. Figure 1 shows the dimensions of the adapted “Five Safes” model taken from the ACS Technical whitepaper.

![Adapted Five Safes Model](image)

**Figure 1. Adapted Five Safes Model**

### Personal Information and Aggregation

Personal information (often also called personally identifying information (PII) or personal data) covers a very broad range of information about individuals. In principle, it covers any information that relates to an identifiable individual (living or within 30 years of death), where identifiability is determined not only by reference to the information itself but also having regard to other information that is reasonably available to any entity that holds relevant information.

The test for personal information relates to the situation where an individual identity can “..reasonably be ascertained from the information or opinion”. The ACS Technical whitepaper uses a concept of Personal Information Factor (PIF) to describe the level of personal information in a data set or output as shown in Figure 2. A PIF of 1.0 means personal information exists, a value of 0.0 means there is no personal information.

Often aggregation is used to protect individual identity ensuring outputs are not released for cohort smaller than “N”. In principle if (N-1) other data sets can be found which relate to the cohort of interest, then the cohort of size N can be decomposed into identifiable individuals. As the aggregation levels increase (cohort sizes of N², N³ and so on for N > 1), the level of protection increases as more related data sets are needed to identify an individual within the cohort.

The definition of PIF is still to be robustly determined however the working definition is an upper bound and defined within a closed, linked, de-identified data set as:

\[
PIF < 10^\left(-\log_{10}(\text{Minimum Identifiable Cohort Size}) - \epsilon\right)
\]
The Minimum Identifiable Cohort Size is the smallest group within a data set that can be identified from the available features. For example, in one data set, there may be 100 males without beards, born in NSW. If an addition feature is included (those under 18), this number may reduce to 10. In this example, the Minimum Identifiable Cohort Size is at most 10.

For a Minimum Identifiable Cohort Size of

1, PIF is less than 1.0
2, PIF is less than 0.5
5, PIF is less than 0.2
10, PIF is less than 0.1
100, PIF is less than 0.01

As new data sets are added to an existing closed linked data set, new features are potentially identified. As a consequence, the Minimum Identifiable Cohort size will potentially reduce leading to higher PIF values.

The notion of a “bound” is important as having a cohort size of 1 is not always the same as having personal information. The term “Epsilon” in the PIF calculation is intended to reflect the fact that with deidentified data, even at Minimum Identifiable Cohort size of 1, at least one additional data field is required to map to the identified individual.

In the example above of a defined anonymised cohort, knowing there is only one male member does not provide sufficient information to identify the male individual. Depending on the exact circumstances, it is possible to imagine additional data which would allow identification. Similarly, if there were 2 males in the cohort, it is possible to imagine several additional data sets which would allow individual identification. The approach continues for 5 or 10 males in a defined cohort. The PIF is therefore treated as upper bound rather than an exact value.

The quantification of Epsilon is still to be determined and will be contextual.

For an Epsilon of “0.01” and Minimum Identifiable Cohort Size of

1, PIF is less than 0.98
2, PIF is less than 0.49
5, PIF is less than 0.20
10, PIF is less than 0.10
100, PIF is less than 0.01

When Is Personal Information Revealed?
In this paper, a distinction is made between the level of personal information (see Figure 3):

- when linked and analysed in an analytical environment (Insights and Models level),
- when considering outputs at different stages in a project which are seen by an observer (Personal context level) and
- when outputs are made available to the wider world and may be linked to data sets in the wider world (Real world context level)

In the lowest level in Figure 3 (Insights and models), it is possible to link anonymised data sets and ensure the PIF

Figure 3. Context for determining the degree of personal information

Figure 2. Personal Information Factor and Aggregation Level
does not reach 1.0 by mathematically exploring the feature sets which describe the Minimum Identifiable Cohort size. If the smallest identifiable cohort is \( N > 1 \), then the PIF is less than 1.0. This means more independent data is needed to reach a PIF of 1.0 (personal information).

When working with anonymised data, a minimum identified cohort of 1 does not explicitly imply a PIF of 1.0 (personal identification). As discussed above, a de-identified data set with a Minimum Identifiable Cohort size of 1 may still require additional data to map to an individual. In the closed analytical environment (Insights and models level), this additional data is not necessarily available.

In the next level of this model (Personal context), any observer who views results will bring to that observation their own experience, knowledge, and perspective. It is at this point that the “reasonable” test is truly applied. At this stage, it is impossible to know the total range of interactions between the PIF developed by the linking of analytical processes and the additional information brought by Personal context of the observer. The risk mitigation required when revealing outputs at different stages of the project depends on the level of “Safety” of the observer in context of the other Safe dimensions of the project (setting, data and output). This is discussed further in the next section.

In the final level of the model (Real world context), any observer who views the results not only brings their own knowledge and experience, but also has access to a wide range of other data sets to potentially link to the project outputs. The level of protection via Minimum Identifiable Cohort size becomes increasingly important.

**With Whom Can Data and Outputs be Shared?**

In this paper, a distinction is made between concerns about project findings and privacy. A project may produce results which are challenging, however, unless there is an issue of privacy, these concerns are not considered here. This paper also acknowledges that outputs are produced at multiple stages in a project rather than at completion. This section therefore deals with Safe People and Safe Projects. The level of “Safeness” of people relates to the level of pre-qualification for inclusion in the project – from deep involvement to no vetting at all. The level of “Safeness” of project relates to the level of PIF involved in the project – from “very Safe” with a PIF of 0.0 to “Not Safe” at a level close to 1.0. The term “Not Safe” is used simply to reflect a scale which has “very Safe” at one end.

As results from different stages of an analytics project are produced, they potentially increase in PIF associated with linking of data sets, and so greater risk exists associated with sharing.

**Figure 4** shows an example of how Safe Settings may be established for combinations of different levels of Safety for People and Projects. In this example, People considered to be ‘UnSafe’ (or unevaluated) only gain access to data which is publicly available. If open data is the only data used, it is impossible to overlay governance on a project. Projects which are evaluated as ‘Not Safe’ (PIF of exactly 1.0) are excluded from this example as they require individual evaluation.

![Figure 4](image-url)
An area which is actively being developed is the technology which allows computational operations to be performed where the data is stored and return the answer to a query (and not provide access to the underlying data). The anonymised computations can be distributed, performing calculations over multiple data sources, at multiple sites, and still returning just the computed outputs. These approaches are well advanced, and while there will be a significant additional ICT burden associated with this approach, it may significantly lower privacy and legal concerns associated with use of data, and so reduce governance requirements.

Dealing with Mixed “Safe” Levels

One of the fundamental principles underpinning the challenge of data sharing is addressing the challenge of value, risk, and trust in data sharing. This can change as a data analysis (the simplest case being data sharing) project develops through the major phases of:

- Project scoping (including identification of people)
- Data collection, organisation, and curation
- Data analysis
- Results interpretation
- Release of results.

As each of these phases progresses, the ‘value’ of the outputs increases, and the potential risk may also increase. An important consideration is that projects which involve any element of discovery need periodic review depending on the level of risk which is assessed at each of the major project phases. Identification of the impact on privacy or the ethical considerations of a project will depend on what is identified, and this may not be known at the outset.

A more flexible approach to data analysis projects may allow light touch up-front assessment of privacy impact, people, and technology, and increase the frequency or intensity of these assessments as the project continues.

A summary of possible guidelines is given in Figure 5. Figure 6 attempts to map the major data analysis project phases to the risk mitigation focus for each dimension in the “Safe’s” model. The benefit of a multistage assessment for privacy and ethics is that it is no longer necessary to preconceive at the outset of the project all of the issues or risks which may arise during analysis.

3. POSITIONING PROJECTS IN THE DATA SHARING FRAMEWORK

Safe People and access to Safe Outputs

The recommendation is to adopt the data sharing frameworks described in this paper and the ACS Technical Whitepaper to allow the project to progress and to support practical data sharing.

Within the scope of a project, the major factors to consider are:

- the (potentially) increasing PIF at each stage of the project,
- the people who can access the outputs at each stage of the project and at what level of aggregation.

Following the flow of logic in Figure 4, Figure 7 shows the relevant squares highlighted for different levels of “Safe” for observers of the project:

Safe Level 5 – Highly Safe People:
Example: Researcher / Research Supervisor
- security check such as Police Check or Working
with Children Check\textsuperscript{4}  
- Qualified data analytics skills  
- Higher technical degree or working under supervision of Higher technical degree  
- Named access on relevant data sharing agreements (such as an MoU)  
- Access to de-identified, linked, unit record data  
- Access to results at de-identified, linked, unit record level

Safe Level 4 – Safe People:  
Example: Partner Agency Project Reviewer  
- Police check and Working with Children Check  
- Qualified data analytics skills  
- Named access on relevant data sharing agreement  
- Knowledge of data at dictionary level  
- No access to de-identified, linked, unit record data  
- Access to aggregated results at cohort level (increased size of MICS)

Safe Level 3 – Moderately Safe People:  
Example: Agency Partner  
- Working with Children Check  
- Named access on relevant data sharing agreement  
- Knowledge of data at dictionary level (which features are used)  
- No access to de-identified, linked, unit record data  
- Access to aggregated results at cohort level (further increased size of MICS)

Safe Level 2 - Low Level of Safety:  
Example: Unrelated Agency  
- Not named access on relevant data sharing agreement  
- No access to de-identified, linked, unit record data  
- Delayed access to more highly aggregated results (further increased size of MICS)

Safe Level 1 - Not Safe People:  
Example: General Audience  
- No security checks  
- Not named on relevant data sharing agreement  
- No access to de-identified, linked, unit record data  
- Access to aggregated results at trend level (largest MICS)

\textsuperscript{4} See Office of the Children’s Guardian  

Figure 7. Safe people and Safe projects for a Project

Examples Aggregation Levels for Outputs

The level of aggregation depends on the “Safe” level of people involved:

Researcher / Research Supervisor (Highly Safe People):  
- Access to results at de-identified, linked, unit record level  
- Minimum Identifiable Cohort size = 1  
- PIF < 1.0

Partner Agency Project Reviewer (Safe People):  
- Access to aggregated results at cohort level  
- Minimum Identifiable Cohort size = 10  
- PIF < 0.1

Agency Partner (Moderately Safe People):  
- Access to aggregated results at report level  
- Minimum Identifiable Cohort size = 100  
- PIF < 0.01

Affiliated Agency (Low Level of Safety):  
- Delayed access to aggregated results at report level  
- Minimum Identifiable Cohort size = 100  
- PIF < 0.01

General Audience (Not Safe People):  
- Access to aggregated results at trend level  
- Minimum Identifiable Cohort size = 1000  
- PIF < 0.001

In practice, the access provided to the General Audience would be a different type of document from that released to Agency Partners. In this context “Not Safe People” refers to no vetting process or assumed analytical skills.
If the PIF has approached 1.0 for any of the outputs of the different stages of the project following the flow of logic in Figure 5, Figure 8 shows the relevant squares highlighted for different “stages” of the project if the project works with and reports on anonymised data with a Minimum Identified Cohort size of 1.

To reduce the risk at each stage of the project, the Minimum Identified Cohort size can be increased before outputs are released as shown in Figure 9.

**Figure 8. Project Risk Profile for small Minimum Identifiable Cohort size**

**Figure 9. Risk Reduction in Project based on increasing Minimum Identifiable Cohort size**

**Project Risk Management based on Outputs**

In this paper, the consideration of personal information is separated from that of concerns about the significance or interpretations of outputs. The recommendation is to adopt the data sharing frameworks described in this paper and the ACS Technical Whitepaper to allow the project to progress and to support practical data sharing.

Within the scope of a project, the major factors to consider are:

- If the PIF has approached 1.0 for any of the outputs of the different stages of the project following the flow of logic in Figure 5, Figure 8 shows the relevant squares highlighted for different “stages” of the project if the project works with and reports on anonymised data with a Minimum Identified Cohort size of 1.

To reduce the risk at each stage of the project, the Minimum Identified Cohort size can be increased before outputs are released as shown in Figure 9.

Dr. Ian Oppermann is the NSW Government’s Chief Data Scientist and CEO of the NSW Data Analytics Centre. Ian has 25 years’ experience in the ICT sector having held senior management roles in Europe and Australia as Director for Radio Access Performance at Nokia, Global Head of Sales Partnering (network software) at Nokia Siemens Networks, and then Divisional Chief and Flagship Director at CSIRO.
AN INTRODUCTION TO THE DELOITTE AUSTRALIAN PRIVACY INDEX 2018 – FIVE QUESTIONS WITH DAVID BATCH AND TOMMY VILJOEN

The Deloitte Privacy Index 2018

On 18 May 2018 Deloitte released its fourth annual assessment of the privacy practices of the top 100 brands in Australia revealing that consumers choose those brands which are transparent about what they do with their data.

The rankings are below, as are the key findings.

<table>
<thead>
<tr>
<th>Sector</th>
<th>Ranking 2018</th>
<th>Ranking 2017</th>
<th>Ranking 2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information technology operations</td>
<td>1</td>
<td>9</td>
<td>7</td>
</tr>
<tr>
<td>Financial services</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Government</td>
<td>3</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Telecommunications &amp; media</td>
<td>4</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>Travel &amp; Transport</td>
<td>5</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Consumer/retail</td>
<td>6</td>
<td>7</td>
<td>10</td>
</tr>
<tr>
<td>Real estate</td>
<td>7</td>
<td>8</td>
<td>13</td>
</tr>
<tr>
<td>Health care/fitness</td>
<td>8</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>Education/employment</td>
<td>9</td>
<td>11</td>
<td>6</td>
</tr>
<tr>
<td>Energy &amp; utilities</td>
<td>10</td>
<td>4</td>
<td>3</td>
</tr>
</tbody>
</table>

Key findings

- 69% believe that trust in the brand is most important when making a decision about sharing personal information, followed by the benefits received, such as discounts, personalised service and rewards.

- Brands are more likely to lose consumer trust and damage their reputation if customer data is used for cross-selling of personal information (68%), inappropriate marketing (58%), and trading data to enable sales (54%).

- Consumers are aware that their personal information may be shared with third parties and 41% are comfortable allowing a brand to transfer their data if they trust the brand and there’s a benefit for them.

- 58% of consumers are unaware of the requirement by law to notify them of any data breach under the 1988 Privacy Act if their data is likely to be misused.

- 90% of consumers still expect to be notified if their personal details are involved in a breach.

- 76% of respondents indicated that they would be more likely to trust a brand after a breach if there was timely notification of the breach, a detailed explanation, detailed remediation plans, and ongoing notifications on progress.

A full copy of the report can be found [here](#).

Privacy Unbound asked the authors, Deloitte national Cyber Risk Services lead partner Tommy Viljoen and David Batch, Deloitte’s new National Privacy and Data Protection Lead a few questions about the index

1. Energy and Utilities have had a tough 3 years, consistently losing trust, do you have any insight on this?

This year’s Index metrics were focused on transparency around personal data handling practices, but it is not a trust Index per se. Having said this, there is strong consumer survey evidence to suggest that a lack of transparency is one of the factors that can lead to a loss of trust, so brands scoring low on this measure do need to take note.

Despite the rankings, the results this year were in a fairly tight grouping given the most heavily weighted inputs for the Index were based on publicly available information on individual brand’s privacy practices. One of the observations from the results was that industry sectors that have more brands operating in the digital space tended to score higher on
transparency measures. Whilst utilities have online channels supporting their product, the online channel is ancillary to their product. This may explain why the same amount of effort hasn’t gone into communicating their privacy practices with the public, and their consumers online, as brands that only operate in the digital space.

2. **Education seems to rank low – was there any theme in that result?**

It was a surprise to our research team that top education brands were not strong in this field. We can only theorise as to why, but again it may be because online and public channels are not their primary means for communicating to individuals that engage with them. Having said this, the defacto standard to communicate privacy practices with the public in 2018 is through online public channels, and should be available to the public before they engage with an education brand, so it’s probably time that the education sector made some improvements in this space.

3. **Trust is important. Do your findings indicate the social licence is becoming equally or more important than strict legal compliance?**

The research on consumers’ views in this space was clear: the legal thresholds for consent, notice and transparency are far lower than what consumers expect. If you want trust you must go beyond what the law requires when handling personal data. This includes making more transparent disclosures about how data will be used and treating your customer’s data like it was information about you – would you lose trust in a brand if you found out it was doing the things with your data you are doing with your customers’ data?

4. **Social media profiling is one of those items that sometimes falls short of involving privacy breaches but can breach the transparency and trust standards, did consumers share this concern?**

We didn’t ask consumers about this specifically, but the research findings regarding data being used for purposes other than what it was provided is clear: consumers expect to be told how their information will be used and expect to be able to make an informed decision about the who, what, when and where questions that surround the handling of their personal data.

5. **Finally, were there any big surprises for you in this 4th report?**

To be quite honest, there weren’t too many surprises in the outcomes of this year’s research. Probably the most interesting finding was that brands that operate in the digital space make better attempts to communicate how personal data will be handled. What would be really interesting is further research around how their claims actually stack up in practice, so perhaps we will look at something a bit more along those lines in a future Index.
Introduction
Dr Bernard Robertson-Dunn is an electronic and automation engineer, has a PhD in modelling the electrical activity in the human small intestine and has had over forty years modelling, architecting and designing large scale information systems, mostly in government environments.

These include the Departments of Health, Finance, Immigration and Defence. Bernard has been following the progress of, and has contributed to, the debate on the My Health Record for over ten years. He has no association or affiliation with any vendor or government organisation. Bernard is chair of the Health Committee of the Australian Privacy Foundation.

The views in this article are his considered opinion and are provided to Privacy Unbound to provide a broad contextual analysis of the issue surrounding health records and My Health Record in particular.

A Medical Record primer
Back in the day, when General Practitioners wrote on paper with black ink about the consultation they had just had with their patient, there was an implied joint contract and mutual trust. The doctor wanted to remember what their patient’s symptoms were, what he (they were nearly always he in those days) had prescribed and his musings and guesses as to what you were suffering from. You didn’t have to know or remember what you were suffering from. You both had an interest in the existence of the record. It was written by and for the doctor, you never saw it and it was called a medical record.

There was a reasonable balance between two parties with different but compatible and complementary objectives. You trusted your GP to keep your data confidential and do their best to make and keep you well; the GP wanted to stay in business and he valued his reputation.

Automation
Then along came computers. Initially all they did was store the same information in the same manner as did the paper records. There was the odd downside; computers are more expensive than pen and paper; GPs had to learn how to use a keyboard and how to operate a computer. The relationship between patient and GP didn’t change much.

The GP probably spent more time looking at a computer screen than they did when they used pen and paper, but that was seen as a small price to pay for improved record keeping.

It was a similar situation in those hospitals that implemented electronic health records, although there are some horrendous tales of failed IT projects, but that’s not particularly uncommon in such complex environments.

With early computerisation, the situation regarding privacy, confidentiality and trust between patient and health care provider was largely unchanged. The IT systems were more prone to single points of failure, to ransom-ware and to data breaches but they were issues that could be solved with proper management and attention to technology.

There were, and still are, some major problems with the access to, and management of, health care information. Much data is transferred via fax, only a small amount of information is interchanged, sometimes data exists but this is unknown to health providers who could benefit from having it available.

However, the old medical record systems did have one advantage. Only those involved in a particular aspect of a patient’s care had access to a patient’s data about that care. Poor sharing of data was a two edged sword. It was privacy enhancing but there were clinical downsides.

When it comes to addressing some of the problems facing data management in the health care system – better access to health information dispersed throughout a large, multifaceted industry - there are two potential approaches. These can be summarised as decentralised or centralised.

Distributed Health Eco-systems
A decentralised, or distributed system would create a mechanism for identifying the location of a patient’s health data and allowing a health provider to access that data. There would need to be a mechanism for implementing a need to know principle – i.e. a health provider could only see that data they needed to in order to treat or advise their patient. The holder of that information would be responsible for granting access to the data.

All data could remain where is was; thus not complicating data consistency, which would occur if data were copied
from one system to another. However, there may be a good argument that there should be a single source of truth, which would logically be the patient’s primary health provider – their GP.

A distributed system has the added advantage of being far more resilient and thus reliable than a centralised one which is at risk of being overloaded in times of high usage e.g. in an epidemic or bio-hazard situation, or prone to failure due to power or communication loss. It is far less risky to have clinical systems located as close as practical to the point of care.

A distributed system has the characteristics of a virtual health ecosystem, rather than a health record. Additional capabilities at the health provider level can include such integrated functions as appointments, repeat prescription requests and a patient portal access to relevant information. Such systems are being implemented overseas.

The result would be an ecosystem of health information in which a virtual medical record existed. This record, although distributed, could be made available to systems that could undertake complex analysis and predictive functions that would assist health providers in their diagnosis and treatment of the patients. The major characteristics would be flexibility, coexistence of a variety of capabilities and a platform for small scale innovation that would scale or find a niche if useful or atrophy if not.

The privacy, trust and confidentiality issues would not be unduly challenged; the symmetry of need between patient and health provider would be retained. The health provider would be responsible for maintaining patient privacy and the patient would only need to trust a single party.

Centralised Health Records

The alternative is a centralised system such as My Health Record. This requires a database at the hub and a system which acquires and stores data. If it only passed on the data and did not retain it, it would functionally be the same as a distributed system.

A centralised system results in the database becoming the defining feature of the health information ecosystem. Innovation is stifled because compatibility with the database is essential. In a distributed system, local innovation is possible and preferable – it can be tested and assessed locally. Change in a centralised system is totally dependent on the hub and would need to happen globally.

The primary issue of a centralised system is “who owns the database in the hub?” Ownership bestows significant privileges; the owner runs the system and any access rules do not apply to the owner.

This single characteristic completely changes the dynamics of the health data environment.

Now there are three parties – the patient, the health provider and the system owner. In the case of My Health Record, this is the Australian Digital Health Agency, an Australian government entity that both reports to, and is funded by, the Federal Minister for Health.

What was a symmetry of needs between the patient and their health provider is fundamentally altered. Not just changed but distorted.

If the health provider is a GP, then a number of changes are introduced into the interaction between the GP and their patient. My Health Record is an additional, summary system over and above the GP’s clinical support system. Uploading data into My Health Record is not a simple matter of a few clicks. The AMA has produced a set of guidelines [1] that GPs are supposed to follow. It is a 27 page document and following it takes time out of a consultation to manage a patient’s My Health Record.

In addition, and this is a significant issue, the government, through a variety of mechanisms, pays the GP to provide the patient’s data. It could be argued that this is “selling” patient data to the government. This may or may not be a valid description, but it does introduce a real or perceived conflict of interest. The patient suffers from less attention; the GPs is paid for something that does not involve treating the patient. The patient may not be happy with the financial arrangement and may perceive a conflict of interest. This issue has the potential to have a negative impact on the trust between the patient and their GP.

The relationship between the GP and the government is primarily financial. The GP gains little or no benefit, they already have the data. The GP still gets data from other providers via the traditional mechanisms - fax, or emails. Data that is not provided to GPs may or may not be uploaded to My Health Record. Patients have the option of requesting that pathology labs or specialists do not upload data. There is no guarantee that data that a new GP or an A&E department would like to see is in My Health Record. In short, it is unreliable. There are also reports that data is sometimes incorrect or uploaded to the wrong patient resulting in either compromised treatment or the need for a patient to spend significant time and effort correcting the error, if they discover it.

The relationship between the patient and the Federal government, a funding agent, is totally un-necessary for the delivery of health care. However, it represents a real and potential problem for the patient. Why does the Federal Government want such detailed health data? This is a question that has never been answered satisfactorily. There is an argument that the government needs aggregated data in order to develop policy, but there is no rationale for more detailed data. Furthermore, there is a suggestion that it could match detailed health data to its existing payment data looking for patterns of health care decisions by health providers; but this is only supposition. However, this uncertainty does nothing to engender trust.
The existence of a centralised database means that data from different providers will be stored in a single location; data which is available to anyone authorised to see the record. The inherent privacy advantages of a distributed system, where only the originating health provider has access, are nullified. In order to retain the trust levels inherent in a distributed system there needs to be an access control mechanism that, at a minimum, mimics that of the old system. My Health Record does not provide this. My Health Record has a complicated, poorly implemented set of access controls that require the patient to take responsibility for monitoring and managing access controls. In a similar way that automation has failed to help GPs manage input and usage of data in their clinical system, My Health Record has introduced extra responsibilities into the management of a patient’s health data. This is a responsibility that most patients are unaware of, and are potentially unable to take on. If they don’t, their privacy is at risk from third parties.

Privacy and My Health Record

The symmetry of the original relationship between patient and GP has now been destroyed. To some, there is now the feeling that there is a spy in the consulting room – the government. In addition, the effort required by the patient to manage their own data has been increased. Hardly an improvement.

The government introduced legislation in 2016 that set the scene to make the system opt-out. Australians now have a three month window in which to tell the government they do not want to be automatically registered for a My Health Record.

In order to enable an opt-out approach the government has had to remove the need to obtain explicit consent to register people and to acquire and disseminate their health data.

Because of the change to My Health Record from opt-in to opt-out, the legislation, especially that in Section 70 has recently become a major issue.

Section 70 includes a wide range of circumstances where it can release or make available My Health Record data. These include providing data to courts, tribunals, coroners and to other government agencies “in the protection of the public revenue”. This last item has never been defined by the government but appears to be related to investigation of fraud and applies to any government, state or federal, that is able to impose fines.

The courts have long been able to subpoena health data from a health provider but, according to a report from the Parliamentary Library [2], the ease with which documents can now be obtained has been significantly increased.

This report contradicts the Health Minister’s claims that a warrant is necessary to obtain information under Section 70. The library also makes the observation that the legislation is a major weakening of existing protections around health records. The Minister has also been contradicted by the Queensland Police union [3]. That the Minister for Health, himself a lawyer is seen to be (allegedly) misrepresenting the legal standing of My Health Record is not adding to the trust Australians might have had in the system.

The minister did not add to a feeling of trust or enhance his credibility when the Parliamentary Library withdrew the original document and replaced it with another, revised version.

Even the Human Rights Commissioner has concerns about confidence in the privacy and security of the system and wants the government to improve privacy protections. "I think we can do better. We definitely are saying that there are problems with My Health Record." He told the ABC [4]

Conclusions

Unfortunately, there are significant consequences from having the government both own the system and set the laws and regulations that govern it. The big problem is that a government in the future could change the rules that permit easier access to My Health Record data.[5] What these are is a matter of guesswork and supposition, but is likely to be unsettling to a population that has already rejected several Identity Card/Number initiatives.

Privacy seems to matter to many Australians and they are not routinely likely to trust government initiatives, especially after problems with the recent census and the so called Robodebt debacle the result of the ATO and Centrelink sharing and linking data, something the government has expressed a desire to do with data from other agencies, including Health, more often. We do not know if that will include My Health Record data, but it could, in the future.

How the My Health Record initiative will all turn out is a matter of conjecture. What is certain is that My Health Record, if widely adopted by patients and health providers will have major consequences for the dynamics of health care system in Australia. Patients will need to become more involved in the management of their own summary health data; GPs will need to spend more time managing health record systems – their own and the governments; and the government will need to continue funding, maintaining and operating the system as well as protecting the data for the foreseeable future. The cost of this system is currently over $AUD2billion; what the return on this investment will be is not yet known.

Even if the issue of government ownership is resolved, there are other characteristics of a centralised system that make its use and effectiveness problematic and questionable. In summary these include:
• The security of a system that is attached to the internet;
• The system is designed to promote data being downloaded to other systems with fewer controls and less visibility;
• The responsibility for accuracy, currency and completeness lies with the patient;
• The significant cost and effort required by patients and GPs to maintain the system.

These are significant obstacles to making any centralised system acceptable for clinical use.

From a privacy and trust perspective, the distributed approach has much to recommend it. The simple yet important relationship between a GP and their patient is a significant driver in the maintenance of a high degree of privacy. Both have a lot to lose. The introduction of a third party, the federal government, apart from distorting the privacy trust relationship is also an asymmetry of power. Taking on the government is no trivial task and only one has a lot to lose.

My Health Record, even after six years operation is still very much a work in progress. The government is currently going through a market testing process that is looking at completely revamping system. This is an implicit acknowledgement that the system as it exists is not fit for purpose.

It is possible, even likely, that over the opt-out period public reaction will result in the government changing its mind regarding such things as the legislation that protects the privacy of My Health Record users. Unfortunately there are two characteristics that cannot be changed.

1. My Health Record means the government acquires and keeps highly personal health data. It can also potentially track the behaviour and performance of health providers.

2. The government has already changed the legislation from opt-in and a need to get a patient’s consent to opt-out and no need to get consent. At the end of the second week of the opt-out period, the government has been forced by statements made by the AMA and the Queensland Police to change the legislation to “remove ambiguity” and improve the protection of Australian’s privacy.

What has the potential to totally destroy any trust people may have in the government is the reality that in our political system there is nothing is to stop this or future governments from further changing the privacy protection.

Not only is My Health Record a work in progress, so is the government’s attempt to persuade Australians to adopt this scheme. Unfortunately for the government the twin problems of a lack of a guarantee regarding future governments and the reality that there is a better, cheaper, more flexible system with inherently better privacy protection means they have a difficult job ahead.

References
[2] Law enforcement access to My Health Record data Both the original and revised versions and a comparison are available through this site: https://privacy.org.au/campaigns/myhr/
Prince Edward Island, Canada, is widely acclaimed for Anne of Green Gables, red sand, roadside dairy bars, oysters and the world’s most delicious potatoes. It is also the home of Canada’s first talks on confederation and some of the most exceptional people you will ever meet. Due to the tireless work of Parry Aftab – globally renown expert in digital privacy and security law, champion for children’s privacy and online safety, cyber-bullying expert, award winning columnist and excellent human being – the Joe Alhadeff Youth Digital Policy Center (Center) will soon be added to the Island’s long list of accomplishments.

I first met Parry in an online forum where the comments of colleagues (and their colleagues) resulted in the shaking of our virtual hands – our common interest being the privacy of children and our responsibility as privacy mavens to promote awareness of privacy and security in digital environments. Discovering that we both have ties to the Island was a serendipitous bonus!

While in Canada in June and early July of this year, I visited the Island and my family’s historic home there. And, of course, I contacted Parry to see if we could put our privacy heads together in person. To my delight, Parry and her husband Allan (a force in children’s privacy and cyber safety himself) arranged to show me the site of the Center, for which construction had just broken ground. At first glance, the Center (nicknamed “Joe’s Place”) is a beachfront haven on the Island’s east coast. Its purpose, however, makes it so much more.

The Center provides a collaborative venue “where children as young as 8 can work alongside and coach world experts in digital policy.” And it’s not intended to be a day trip. As Parry showed me the site, which will include a meditation labyrinth and guest accommodation inspired by the children who are central to Parry’s vision, it became evident that the Center is intended to be a place of reflection and innovation, concern and collaboration, frank discussion and robust policy creation. (My daughter was asked to be the head of the Australia Youth Taskforce being established as part of the Center’s ethos and to collaborate on the design of the “Australia room” – after which an explosion of

---

1 https://www.aftab.com/the-joe-alhadeff-center
possibilities were crafted on Young Miss’ iPad, including surfboard beds and wave blankets! It was quite wonderful!).

The point of having a place like this – as opposed to relegating digital policy (cyber safety, privacy, security, ethics) to online forums and one-person “expert” invitations to sit on boards, committees and the like – is to include the very people who know exactly how to achieve meaningful and lasting outcomes in this arena: our youth! Parry has long advocated for empowering tweens and teenagers in online environments, which includes assisting victims of cyber-bullying and harassment. Indeed, it is the insight of kids (their experiences, concerns and clever ideas) that is so often missing from the digital policy debate. The Center is the next step: by bringing together our young people and the world’s policy makers, legal experts and law enforcers, there is a true opportunity to influence and improve the construction and use of the world’s digital environments.

I look forward to seeing Joe’s Place again once building works are complete. In the meantime, as a member of the Advisory Board for the Center, I hope privacy professionals here in Australia will take a few moments to consider online privacy and safety and the great work being done here and abroad to ensure our interactions with digital environments are positive ones.

Author’s note: Joseph Alhadeff, the Center’s namesake, passed away in 2017. He was a formidable privacy mind and “a recognised authority on internet, electronic commerce and privacy policy issues”.

---

[Author's note: Joseph Alhadeff, the Center’s namesake, passed away in 2017. He was a formidable privacy mind and “a recognised authority on internet, electronic commerce and privacy policy issues”.]

---

Nicole Stephensen is a Privacy Specialist with extensive local and international experience in operational and strategic privacy matters. She is Principal Consultant at Ground Up Consulting, a boutique firm she established in 2001. Nicole is a member of the IAPP, as well as iappANZ where she sat for three consecutive terms on the Board.

---

The EU General Data Protection Regulation (GDPR) enhances a number of provisions from the former EU Data Protection Directive (Directive) which cement Europe’s reputation as the champion of information privacy protection. Here we will focus on the change to consent, an improved right to erasure and stricter requirements for automated decision-making, all of which will have an impact on the health care industry.

These enhancements can be viewed as attempts to bridle the power of global giants like Facebook and Google as they continue to develop ever smarter ways to exploit personal information for commercial gain. Yet the law applies to all industries which process personal information, including health care, where profit is not always the driver. Given the sensitivity and potential for enormous harm to individuals if misused, it makes sense that health information is treated as a sensitive category of personal information under the GDPR. However, protecting patient privacy without creating clinical safety risk has always been a balancing act. An overly-zealous approach to GDPR consent and individual rights could well disrupt that balance.

With this in mind, the impact of these provisions, their available exceptions and alternative approaches are important to understand for any organisation which may provide products or services in support of European health care organisations. For example, Australian and New Zealand manufacturers of medical software and devices, cloud service providers, data scientists and developers of mobile applications which give access to medical records.

**Consent**

The GDPR introduces a stricter standard for consent. Where consent is relied upon by an organisation as the legal ground for processing, it now must be made via a statement or affirmative action. Individuals also have the right to withdraw consent as easily as it was to give it. By contrast, the Australian Privacy Principles state that consent may be express or implied, and New Zealand’s Health Information Privacy Code does not attach any conditions to the way that consent is delivered.

Like in Australia and New Zealand, the common law duty of confidence applies to medical professionals in the United Kingdom and Ireland. Consent of the patient to share their health information amongst health care professionals, even across multiple organisations, is generally implied if the data is shared for the purposes of direct care (e.g. diagnosis and treatment). In EU member states with civil law jurisdictions, laws equivalent to the duty of confidence and the doctrine of implied consent are generally incorporated into civil codes or other legislation.

Given implied consent is now clearly insufficient for the purposes of the GDPR, there has been some question over whether health care organisations need to fundamentally change the way they use and share patient information. Nonetheless, consent does not need to be relied upon as the legal ground for processing health information under the GDPR. Similar to the ability to use and share health information for a “permitted health situation” under Australian Privacy Principle 6, the GDPR permits the processing of health information for medical purposes (without consent), where it is carried out by a medical professional subject to the duty of confidence or equivalent member state law. Other lawful grounds are available for secondary use purposes such as public health and research. Moreover, the standard of consent for the processing of sensitive data under the Directive already required explicit consent, which remains the case under the GDPR.

Indeed, the NHS England has made it clear that NHS Trusts should avoid relying on consent as the legal basis for processing health information under the GDPR. Choosing to rely on explicit consent not only means needing to demonstrate it somehow (e.g. using a signed form), but also that patients will have the right to data portability and the right to erasure made available to them, which are both things that large organisations like the NHS will struggle to support.

Suppliers of health technology or other services for the EU market should not need to adapt their technology to support the new consent standard (for example, by requiring that explicit patient consent is obtained before a clinician can access an electronic health record). This may create unnecessary clinical risk. However, it should always remain possible for consent to the collection and sharing of information to be recorded, respected, and withdrawn.
Automated decision-making

Under the Directive, an individual already had a right not to be subject to automated decisions. The GDPR builds on this by requiring organisations to provide meaningful information about the logic behind such automated decisions in their privacy notices, as well as an explanation of the significance and envisaged consequences for the individual. In contrast, the Australian and New Zealand privacy regimes do not specifically regulate automated decision-making or profiling, aside from general requirements for transparency.

Moreover, automated decision-making now cannot take place in the EU using sensitive information, except with the individual’s explicit consent, or if processing is necessary for reasons of substantial public interest on the basis of member state law. The GDPR recitals make clear that this restriction is intended to apply to the use of predictive technology in health, although it would apply to any automated reasoning upon a person’s health information. The degree of information required to be “meaningful” is subject to much speculation, particularly in the context of the vagaries of algorithmic processing. Data scientists developing AI solutions for the health care market should consider how to best provide for transparency, and keep watch as the meaning of this develops in commentary and case law.

It would be fairly impractical to seek the explicit consent of patients to use automated technology, as it is already widely used in many forms across the health industry. For example, health care providers may deploy machine-learned algorithms to suggest cohorts of patients within their existing system at high-risk of kidney disease, generally without the knowledge of the patient. A public interest argument could perhaps be made given the potential for cost saving in public health care systems, however this would need to be demonstrable. Relying on public interest grounds also means that the patient would have a right to object to the use of their information in this way, which could cause havoc where an algorithm has already been fed a data set containing that patient’s data.

Importantly, these new conditions placed on automated decision-making only apply where the decision produces a legal effect, or other significant effect for the individual. The decision must also be based solely upon automated means, i.e. without human intervention. Any decision concerning medical treatment or diagnosis is likely to be considered significant for that individual. With the growing use of smart technology in health care which can, for example, suggest and even enrol a patient into a treatment plan based on their symptoms, it seems possible that significant decisions can effectively be “made” by software without a clinician stamping their approval or even reviewing the decision.

Consequently, healthcare technology suppliers should take special measures to ensure that their products are not designed to fully substitute the decision-making discretion of a health care professional.

The system workflow should provide professionals the opportunity to review, or better still require them to affirm software-made decisions, and permit override. This way, while a medical outcome or pathway is being “suggested” by the software, it could be said that the “decision” is being made by the professional. In order to support this, some form of information about the basis of the automated reasoning should be made available to the professional, even if it is a simple summary of the patient’s symptoms which led to the suggestion. Health care organisations should also have policies in place that require professionals to apply their own clinical judgment before proceeding with software-generated decisions. If these measures are taken, it would be difficult to say that decisions are being made “solely” by technology and there will be a strong argument that the new conditions applicable to the use of automated decision-making under the GDPR do not apply.

The right to erasure

The GDPR grants individuals a right to request that their personal information be erased in some circumstances, including where it is unlawfully processed or is no longer necessary to retain for the purposes it was collected. The right also arises where the individual withdraws consent (if consent has been relied upon as the lawful ground for processing), or if the individual has a right to object to the continued use of their personal information on the grounds of public interest. The same right already existed under the Directive, but has now been strengthened by removing the damage threshold.

The right to erasure is quite distinct from the obligation not to keep personal information longer than necessary, which also exists under the GDPR as it does under Australian and New Zealand privacy legislation. The latter gives the agency a degree of flexibility to determine their own retention cycle based on what they consider “necessary”, whereas the right to erasure may cut across legitimate reasons for wanting to keep personal information, unless one of the exceptions apply.

There is an exception which permits organisations to refuse a request to erase personal information if they need to retain it to comply with a legal obligation, for the...
performance of a task carried out in the public interest or in the exercise of “official authority” vested in that organisation. Health care organisations must retain health records for varying legal retention periods applicable at member state law. Depending on the type, legal retention periods for medical records can be 30 years from creation, or longer. Once a medical record is beyond its legal retention period, health organisations could still refuse erasure if keeping it is necessary “for reasons of public interest in the area of public health”, or for research purposes. NHS England raised early concerns with the draft GDPR text in that these exceptions do not give health care organisations a clear mandate to refuse an erasure request where fulfilling it would not be in the best interests of the individual. The final text of the regulation does not account for this either. Indeed, there are scenarios where it would seem unsafe, unethical or inappropriate to carry out the request of a patient to erase a part of, or their entire, medical record. Imagine a narcotics abuser requests a permanent wipe of his medical record in order to avoid any future issues with getting access to opioids. The unavailability of their past medical history to care providers could cause that individual serious harm. At present, it is unclear just how such a request could be refused if some or all of that person’s medical record had past its legal retention period.

The Article 29 Working Party is yet to publish official guidelines on the right to erasure, which may be key to understanding how the controversial right applies in such situations. It is also possible that member states may extend legal retention periods for some or all health records, or otherwise vest health care organisations with an “official authority” to refuse requests in scenarios where erasure would create a clinical safety risk for an individual. While the use case is undeniably limited, it remains possible that the right to erasure will in some cases be available to patients, which should be taken into account when developing systems which will store health information.

However, given the potential dangers of completely purging a patient’s medical history, technology should not be designed in a way that makes erasure possible “at the push of a button”, and it should not be something actionable by ordinary users of a hospital’s IT system. Health care organisations will need to put in place careful policies and processes to ensure that requests, and all exceptions are carefully considered before a hard delete is carried out.

Summary

The GDPR has brought significant changes to the EU’s data protection landscape in the areas of consent, automated decision-making and erasure rights. While designed to protect the rights and freedoms of European citizens, these areas could also give rise to unnecessary complications to existing health care processes, or clinical risk. Health care organisations and their suppliers need to be aware of the implications of these changes, and consider the exceptions and alternatives that the GDPR and member state laws may offer before assuming that they apply or that they must be blindly respected.

Jennifer is the Chief Privacy Officer at Orion Health, a New Zealand health care software company with customers around the world. Jennifer has a background in information technology and intellectual property law. She moved into the world of privacy after discovering a passion for the practical side of health care IT and the management of the complex privacy and clinical safety issues involved.
Background

The PageUp data breach was first notified on 1 June 2018 by PageUp to its customers. It is a significant breach in the history of recent notifiable data breaches in Australia as it tests the operation of a principles-based system, particularly where a breach occurs in the system of a service provider who may not be the company with the closest relationship to the individuals affected. The breach raises the issue of who should be contacting the individuals and specifically, the legal liability of PageUp and each of its customers.

About PageUp and its services

PageUp is a company that provides recruitment, training and other related talent management solutions through an online, cloud-based platform. It uses technology to harness tasks and simplify workflows, and it seeks to link and integrate with other systems used by its customers to create a seamless experience for the customer and their employees. Accordingly, individuals whose personal information was subject to unauthorised access as a consequence of the PageUp breach may not have been aware that PageUp had their details at all, as PageUp is a service-provider to their employer or recruitment company.

This is a significant issue in terms of whose system was breached and who had legal obligations to notify.

To further complicate the analysis, employee records as between an employer and employee (both current and former) are exempt from the Privacy Act 1988 (Cth) (Privacy Act). This exemption has existed on the assumption that employment law would make adequate provision for the subject matter. That has not happened. The result is that employees don’t have the protections of the Privacy Act as between the employer and employee. If their information is subject to unauthorised access as a consequence of the employer’s actions, is there a breach of their privacy from a Privacy Act perspective? It is an issue that arose in the Svitzer case where again significant sensitive data was leaked, including employee bank accounts and tax file numbers, which are attractive to criminals.

For PageUp, if the data breach occurred within its system then the exemption did not apply to it. For employers who used the system with contractors as well as employees, then caution was to be advised.

Timeline and background

According to the PageUp website, a public information update released on 5 June 2018 reported that on 23 May 2018, PageUp detected unusual activity and commenced a forensic investigation. On 28 May 2018, the investigation indicated that client data may have been compromised. PageUp engaged an independent third party to assist its investigation, and on 1 June 2018 notified its customers about the data breach, giving them guidance about what they could do and what to tell staff who were affected.

The PageUp website published an update on 12 June 2018 which set out further information regarding the ongoing forensic investigation and the limited access that had been gained. It also listed data elements that were not affected.

Further, PageUp provided an email address for affected individuals to contact, along with a series of FAQs dealing with the technical issues. PageUp’s responses included what individuals could do if they feared their personal information had been subject to unauthorised access. The FAQs also detailed the regulatory organisations with whom PageUp was liaising in relation to the incident. On 17 June 2018, they updated the information page and FAQs with further information including the results of the forensic investigation and what information had been accessed.

So who is responsible for investigating and responding to a breach?

Section 13 (4A) of the Privacy Act provides:

If an entity (within the meaning of Part IIIC) contravenes subsection 26WH(2), 26WK(2), 26WL(3) or 26WR(10), the contravention is taken to be an act that is an interference with the privacy of an individual.

Subsection 26WH(2) deals with the initial obligation to make an assessment of a suspected eligible data breach. It provides:

(2) The entity must:

(a) carry out a reasonable and expeditious assessment of whether there are reasonable grounds to believe that the

Privacy Unbound | 29
It was after the 17 June 2018 PageUp update that a joint statement by the Australian Cyber Security Centre (ACSC), the OAIC and IDCARE was issued. The press release is interesting in that its tone is almost congratulatory of PageUp for self-identifying the suspicious activity and notifying the relevant agencies (as this is its legal obligation). The release indicates the result of the investigation in that, while personal information was accessed by an unauthorised third party, there was no evidence to suggest it was exfiltrated. That is, no information appears to have actually been stolen. Mention was made that IDCARE had been working with impacted organisations and individuals in relation to the incident.

The head of the ACSC commended PageUp on demonstrating “a commendable level of transparency” in communicating the incident and “advising impacted organisations and individuals if there are any new findings to arise as they complete their investigations”. It is in the sharing of the information that the issue arises for PageUp and its customers. Different customers had different responses to the notifications they received from PageUp. It was reported that some customers took the view that they needed to independently notify the OAIC of the breach, and notify their staff separately and independently, sometimes incurring significant costs in the process.

If organisations have not fully turned their mind to the notifiable data breach provisions in their contracts, then it is unlikely that they will have any mechanism or protocol for dealing with such situations. In addition to dealing with the crisis of the breach, there is the issue of dealing with the allocation of responsibilities for various tasks in terms of notifying and keeping affected parties informed. It may well be that employees are “spooked” where they receive twice as much information as necessary, as each party involved seeks to meet their legal obligations to provide affected individuals with information.

Outcome

The outcome and the lesson learnt is that, in addition to being prepared for a breach of your own data, each organisation needs to consider who in its supply chain it shares personal data with, and how it would respond to a breach of that organisation’s systems, which would in turn impact its personal data. As well as running breach simulations for your own data and systems, considering information that is held, hosted or managed by third parties is a key issue.

The final vexed issue to arise out of the PageUp breach is a consideration of the employee record exemption. While organisations may not be at risk of a breach claim from their employees under the Privacy Act, this begs a further question - if employers are not applying the same standards in terms of security to employee data that they are with other data then are they negligent? Are the standards applicable under the Privacy Act to be treated as a basic standard and a minimum?

Regulator statements

It was after the 17 June 2018 PageUp update that a joint
No doubt there will be more to come on this breach as PageUp users reassess their service relationships.

Lyn Nicholson is an iappANZ board director and a General Counsel in the corporate and commercial group of Holding Redlich. Lyn’s specialist areas include data & privacy, Government and corporate & commercial law.

https://www.holdingredlich.com/people/lyn-nicholson
The algorithms fundamental to artificial intelligence have huge potential to help society in many ways. But how can we ensure transparency and accountability around the use of our personal information in algorithms and how can we avoid biased outputs?

Algorithms and artificial intelligence (AI) play a key role in our data-driven world. An increasing number of important decisions once made by humans in both the public and private sectors are now made solely by algorithms, often powered by our personal information. This raises a number of issues, such as:

- Are we handing over too much power "to the machines"?
- Ensuring we understand how our personal information is being used in automated decision making processes and that appropriate decisions are being made?
- What is the key to help unlock and understand otherwise opaque algorithmic processes?

This article looks at the risks associated with algorithmic decision making and some of the potential solutions, including algorithmic transparency, legislation and government initiatives.

WHAT ARE ALGORITHMS?

Algorithms are one of the foundational elements of computer science – self-contained, step-by-step sets of operations usually performed by a computer. Put simply, an algorithm is a series of instructions, like a recipe or a flowchart. They can be used for calculation, to identify patterns in data and to automate decision making.

While algorithms can be applied to any sort of data, risks relating to a lack of transparency, bias and poorly managed data become particularly pertinent in relation to personal information.

HOW AND WHERE ARE ALGORITHMS USED?

Algorithms are ubiquitous in modern life. On a prosaic level, they give us access to vast amounts of information on the internet with quick, relevant and tailored results. They decide which online ads we see and make the “you may also enjoy” suggestions we get courtesy of Amazon, YouTube and Netflix.

Algorithms and AI can also help make sense of vast amounts of data to drive improved health outcomes, automate tedious or dangerous work, support decision making with speed and accuracy, reduce business costs and optimise business processes.

Gartner forecasts that global business value derived from AI will total US$1.2 trillion in 2018, an increase of 70 per cent from 2017. AI-derived business value is forecast to reach $3.9 trillion in 2022, according to figures released in April by the analyst firm.

WHEN ALGORITHMS GO BAD

Despite the obvious benefits, questions are increasingly being asked about the far-reaching impact of algorithms on our lives. More decisions using our personal information are influenced by algorithms, including what jobs we are offered, whether we get a mortgage or credit card, what medical treatment is recommended and whether the police are likely to regard us as potential criminals.

Is our increasing dependence on algorithms making us increasingly vulnerable? How many of us really understand how or why certain decisions are made? How can we know when to correct errors and contest decisions if we don’t know why an algorithm produced the result it did? And as reliance on AI - and in particular machine learning - grows, how can we be sure that the right decisions are being made based on our personal information?

A range of studies and examples indicate that these concerns are not unfounded and that the following risks must be addressed.

1. **Bias and discrimination**

   - An investigation into machine bias found that the algorithms used by criminal justice systems across the United States to predict future criminals were biased against black people.
   - Studies have found that facial recognition technology misidentifies black people, women and young people at higher rates than
Inadequate training of AI systems leading to incorrect outputs

A Carnegie Mellon University study showed that Google ads for high-paying jobs were shown more often to men than to women.

Poor quality data

“Garbage in garbage out” or “GIGO” is a term well known in computer science. A system is only as good as the data it learns from. Microsoft issued a public apology after its Tay chatbot turned into a holocaust-denying racist following corruption by Twitter trolls. And Google’s problem of search keywords like “gorilla” and “chimp” returning images of African-Americans still isn’t fixed.

Inadequate training of AI systems leading to incorrect outputs

A report found that IBM Watson had made multiple “unsafe and incorrect treatment recommendations” to cancer doctors as a result of incomplete training that used synthetic data instead of patient data taken from real cancer cases. In one reported instance, a doctor at Jupiter Medical Center in Florida using IBM Watson for Oncology reportedly went as far as to call the system “a piece of sh*t”.

Security threats

Attacker may exploit vulnerabilities in AI systems.

The “Malicious use of artificial intelligence” report notes that “As AI capabilities become more powerful and widespread, we expect the growing use of AI systems to lead to the expansion of existing threats, the introduction of new threats and a change to the typical character of threats” including cybercrime, political disruption and even physical attacks.

Proprietary technologies

Organisations may be reluctant to share the internal workings of their algorithms for fear of disclosing trade secrets and sources of competitive advantage. Google’s search algorithm is now a more closely guarded commercial secret than the recipe for Coca-Cola. That makes it hard to monitor and challenge decisions and other outputs, as illustrated when a US appeal court was asked to decide whether sentencing judges should be able to take into account the results of a set of algorithms designed to predict an individual’s risk of recidivism. The accused argued that the proprietary and confidential nature of the algorithms meant that the details of how it worked, and what information went into it, were kept secret from both the sentencing judge and the accused.

WHAT CAN BE DONE?

Algorithmic transparency

The principle of “algorithmic transparency” requires creators of AI to report and justify algorithmic decision making and to mitigate any negative social impacts or potential harms.

But algorithmic transparency can be challenging to implement because of commercial secrecy and the often impenetrable "black box" nature of forms of AI like machine learning and deep learning.

“Machine learning” is a technique that allows algorithms to extract correlations from data with minimal supervision. Machine learning is designed to mimic our own decision-making - if you could get access to those algorithms, it would be possible to understand their reasoning.

“Deep Learning” is a subset of machine learning that is much harder for humans to decipher, relying on “deep neural networks”, or computer systems modelled on the human brain and nervous system with multiple layers. Even engineers who build systems that seem relatively simple on the surface, such as apps and websites that use Deep Learning to serve ads or recommend songs, cannot always explain their behaviour, since you cannot just look inside a deep neural network to see how it works.

So if computer engineers cannot explain the behaviour of their own creations, what hope is there for the rest of us? How comfortable should we be leaving key public and private decisions in the hands of a limited number of data scientists? The risk is that these “black boxes” will operate outside the scope of meaningful scrutiny and accountability. If it’s not clear how decisions are made, then how can they be monitored and verified and how can we predict when failures might occur?

While there is no commonly agreed answer to these questions, data governance, algorithmic impact assessments and ongoing monitoring measures may help address some of those issues.

Data governance: As privacy professionals will be well aware, having a full picture of your data enables better
management of that data and any associated risks. Comprehensive data strategies that focus on technology, data availability and acquisition, data labelling, and data governance will help manage GIGO (Garbage In, Garbage Out) and data quality risks. In addition, a set of tailored data and AI ethical principles can help organisations be clear on key privacy, data ethics and other considerations relevant to their work.

**Privacy by Design and Algorithmic Impact Assessments:** Applying principles familiar from a Privacy by Design approach will help encourage the development of processes that address the algorithmic life cycle from data selection, to algorithm design, integration, and live production use. Privacy, security and bias problems will be much easier to address if identified at an early stage.

Much like Privacy Impact Assessments, Algorithmic Impact Assessments (AIAs) involve a self-assessment of existing and proposed automated decision systems, evaluating potential impacts on things like fairness, justice, bias, or other concerns across affected communities.

The AI Now Institute issued a report earlier this year on AIAs that aims to provide a practical framework for the public sector. That framework is designed to “support affected communities and stakeholders as they seek to assess the claims made about these systems, and to determine where – or if – their use is acceptable”.

The report acknowledges that implementing AIAs will not solve all of the problems raised by automated decision systems. But it argues AIAs provide an important mechanism to inform the public and to engage policymakers and researchers in productive conversation.

**Monitoring and testing:** Organisations that establish processes for assessing and overseeing algorithm data inputs, workings, and outputs, including objective reviews of algorithms by internal and external parties, will be far better placed to identify and manage issues. Ethics boards can use the organisation’s previously defined ethical principles to review algorithmic-based projects and processes.

**Regulation**

**General Data Protection Regulation**

You may have heard of the GDPR? (Sorry, privacy joke.) The General Data Protection Regulation (GDPR) addresses algorithmic accountability through its focus on “automated individual decision-making” (making a decision solely by automated means without any human involvement) and “profiling” (automated processing of personal data to evaluate certain things about an individual).

Article 21 gives people the right to object to automated processing of their personal data, including profiling. Article 22 states that people will have the right not to be subject to a decision based solely on automated processing or profiling.

Data Protection Impact Assessments (DPIAs) are likely to be necessary for high-risk processing activities like automated processing. DPIAs are designed to demonstrate that risks have been identified and assessed and consideration has been given to how they will be addressed.

The GDPR also requires individuals to be given specific information about the processing, what steps are being taken to prevent errors, bias and discrimination and how individuals can challenge and request a review of the decision. That includes providing “meaningful information” about the logic involved in the decision-making process, as well as the significance and the envisaged consequences for the individual.

While the GDPR’s approach is a great starting point for achieving algorithmic transparency, it won’t necessarily assist in all contexts. For example, some predictive policing tools do not necessarily profile on an individual basis, focusing instead on locations and statistics to try to understand and predict crimes trends across geographical areas. Such tools can have a discriminatory impact even without relying on personal information.

**New Zealand and Australian privacy legislation**

While neither the New Zealand nor Australian Privacy Acts specifically address algorithmic transparency, their core principles can help to encourage greater transparency.

Under New Zealand law, individuals have the right to know what personal information agencies are collecting about them and why, and to access and correct information held about them. Reasonable steps must be taken to check the accuracy of information before it is used and the information must be appropriately stored, protected and disposed of once no longer needed.

Australian privacy laws include requirements that all processing of personal information is fair, lawful and carried out in a transparent manner.

But in a fast-changing world, is local privacy legislation keeping up? New Zealand has an opportunity to help address new risks arising out of emerging technology like AI in its Privacy Bill. Unfortunately legislators have chosen not to follow the GDPR’s lead by introducing mandatory Privacy by Design or DPIAs, much less restrictions around automated decision making and profiling.

**Government Initiatives**

**New Zealand**

In May 2018, the New Zealand government launched a
Project to assess how government agencies use algorithms to analyse people’s data.

The objective of the review is to ensure New Zealanders are informed and have confidence in how the government uses algorithms. The initial focus will be on operational algorithms that inform decisions directly impacting individuals or groups. Good practice, and opportunities to support agencies that use algorithms in decision-making will also be looked at.

The Principles for Safe and Effective use of Data and Analytics will underpin the analysis. A report with the findings of the first phase of the review is expected to be published in August 2018.

Australia

The Federal Government has announced AUD $29.9 million worth of investment to grow Australia’s capabilities in AI and machine learning.

It says investment in AI and machine learning will give Australian businesses “significant opportunities to lead the way in the development of products and services with strong export potential, leading to more local jobs.”

In addition, a new national Ethics Framework and Standards Framework will also be established, "to guide the responsible development of these technologies".

France

President Emmanuel Macron has launched a new national strategy for artificial intelligence. The French government will spend €1.5 billion ($1.85 billion) over five years to support research in the field, encourage start-ups, and collect data that can be used, and shared, by engineers.

In a fascinating interview with Wired about France’s AI strategy, Macron sets out his plans to guarantee that all of the algorithms developed by the French government will be open. He discusses increasing collective pressure to make all algorithms transparent, incentivising private players to make their algorithms public and the key role that consumers are likely to play.

“I allow you to better understand the algorithm we use and the bias or non-bias.” I’m quite sure that’s one of the next waves coming in AI. I think it will increase the pressure on private players. These new apps or sites will be able to tell people: “OK! You can go to this company or this app because we cross-check everything for you. It’s safe,” or on the contrary: “If you go to this website or this app or this research model, it’s not OK, I have no guarantee, I was not able to check or access the right information about the algorithm”.

Conclusion

The proliferation of powerful algorithms impacting all aspects of our lives will only increase. While there’s no doubt this will introduce a wide range of potential efficiencies and benefits, we also need to be careful not to overlook the potential risks, particularly to parts of society that have traditionally been marginalised.

An increased awareness of algorithmic risks among researchers, businesses, governments and consumers is required, as well as tools to challenge automated decisions where appropriate. Legislation can assist, as can structured, auditable approaches to identifying and managing risk such as Algorithmic Impact Assessments.

But we also need to recognise that AI is still a nascent and immature field. Mistakes will be made, so we must ensure we learn from those mistakes. And we cannot forget that ultimately algorithms, machine learning and the rest are simply tools programmed by humans. It is our responsibility to use them to enhance humanity, not to amplify existing problems.
As at 27 July 2018, the following updates have been made in relation to Australia’s privacy laws:

- **Office of National Intelligence (Consequential and Transitional Provisions) Bill 2018**

The Bill, which was introduced on 28 June 2018 together with the Office of National Intelligence Bill 2018, establishes the new Office of National Intelligence (ONI) and makes consequential amendments to 19 Acts to give effect to the operation of the ONI.

The ONI was first introduced and recommended in the 2017 Independent Intelligence Review for the purpose of enhancing coordination and strategic integration across the intelligence community. This new independent statutory agency, reporting directly to the Prime Minister, subsumes the role and functions of the Office of National Assessments (ONA).


- **Data Sharing and Release Legislation Issues Paper**

The Issues Paper was released on 4 July 2018 in relation to the Data Sharing and Release Bill (DS&R Bill). The purpose of the DS&R Bill is to promote and authorise the sharing and release of public sector data, with appropriate safeguards in place to maintain the integrity of the data system. The more efficient data sharing and release framework proposed will be monitored and enforced by the National Data Commissioner.

The focus of the Issues Paper is to seek views on the development and design of the DS&R Bill as the first step in the drafting of the new legislation. Comments close 1 August 2018.

- **Privacy (Credit Reporting) Code 2014 (Version 2)**

The Credit Code was approved and registered on the Codes Register and Federal Register of Legislation by the Acting Australian Information Commissioner, Angeline Falk, on 1 July 2018.

The Credit Code repeals and replaces the previous Privacy (Credit Reporting) Code 2014 (Version 1.2) to provide clarity of obligations, reflect current industry practice and ensure that provisions are aligned with the Privacy Act.

- **“Opt-out” period for a My Health Record commences**

A My Health Record allows certain medical professionals to view your health information from a secure online platform at anytime from anywhere. The initiative commenced at the beginning of the year and was made available for all Australians.

The three month period to opt-out of My Health Record officially commenced on 16 July 2018 and closes on 15 October 2018. This option is available to Australians who are yet to have a My Health Record and do not wish to have one created. For those who already have a My Health Record who no longer want one, you can cancel at any time on the My Health Record website.

- **Mandatory comprehensive credit reporting**

The National Consumer Credit Protection Amendment (Mandatory Comprehensive Credit Reporting) Bill 2008 which has passed the lower house but remains in the senate amends section 20Q. It provides a new Subsection 3 at the end of existing Section 20Q which requires a CRB to hold credit reporting information either in Australia or if not in Australia, using a service listed by the Australian Signals Directorate as a Certified Cloud Service provider or under the IRAP program or meets the conditions specified in the registered CR code.
**Credit Reporting Privacy Code 2004.** The Privacy Commissioner proposes to amend the Code. There are two proposed amendments. The first, Amendment No. 13, is simply correcting an error.

Amendment No. 14 is the result of an 18 month review by the Commissioner of the operation of the credit reporting system. In the Amendment it is proposed to (as explained by the OPC):

- Improve arrangements for individuals to access their own credit reports by providing a clearer right to credit scores and requiring access to be given more quickly.
- Enable individuals at risk of identity fraud more quickly to get a credit freeze from all three national credit reporters.
- Raise the threshold for listing small debts from $100 to $125.
- Prohibit bypassing the existing ‘no marketing use’ of credit information by credit reporters through various techniques or by use of related companies.
- Allow credit reporters to use the credit reporting system to provide a service to subscribers to trace individuals to facilitate the return of unclaimed money.
- Introduce the New Zealand Business Number as supplementary identification information.
- Impose new requirements relating to quotation enquiries and assurance reports.

Submissions on Amendment No 14 are due on 25 August 2018. Further details can be found https://www.privacy.org.nz/the-privacy-act-and-codes/codes-consultation/.

**Privacy Bill 2018.** The Bill has been referred to the Select Committee, with submissions now closed and hearings are taking place. There is broad support amongst the submitters to the Bill. The Select Committee is due to report back by 22 November 2018. It is likely that if the proposals contained in the Privacy Commissioner’s report to the Minister of Justice under section 26 of the Privacy Act 1992 (December 2016, table 2017) were to be considered as part of this Bill, further consultation would be required.
'Privacy: Handling the Seismic Shift'
Managing personal information in the era of disruption
This year, iappANZ will grapple with the SEISMIC SHIFT in privacy and data protection. We’ll explore emerging trends in privacy regulation, media, technology and innovation. We’ll hear from thought leaders from Australia, NZ and around the world.

SUMMIT: Melbourne | 1 November 2018
WORKSHOPS: Melbourne | 2 November 2018

For more info, click below
https://iappanz2018summit.floktu.com/register