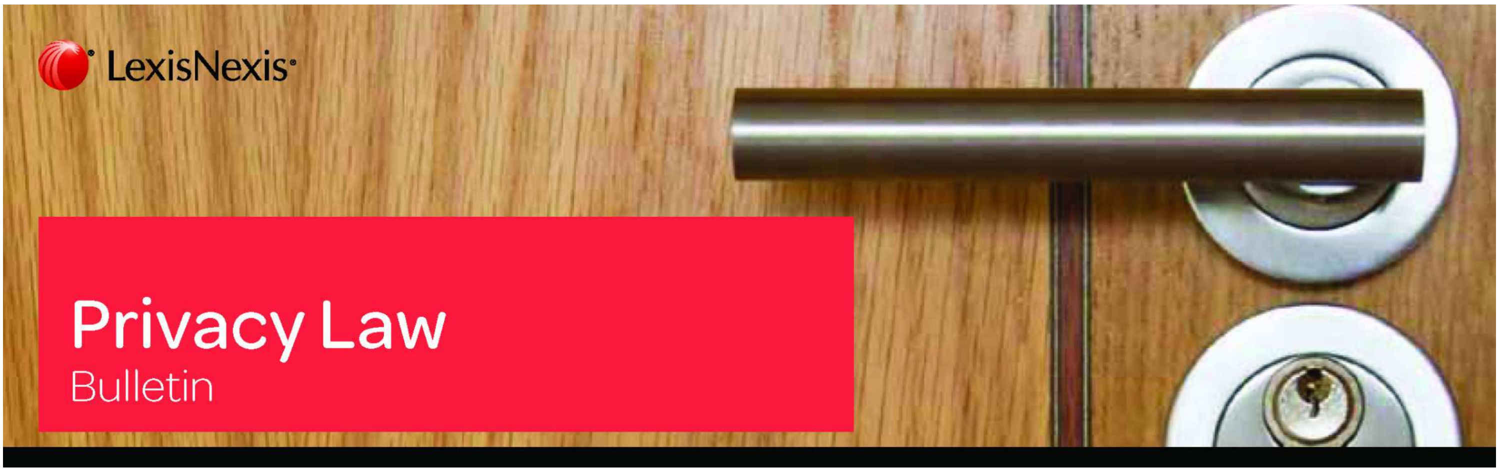


Privacy Law
Bulletin

2021 . Vol 18 No 5

Contents

Information contained in this newsletter is current as at August 2021

LexisNexis®
Butterworths

Privacy for victims of domestic violence? Privacy breaches can add fuel to the fire

Sionea Breust SCB LEGAL

In recent times, we have seen an increase in victim's information being shared or even leaked. The protection of victims is paramount, yet we continue to hear about victim's safety being jeopardised to the point where they are forced into hiding.

This article will examine the relevant privacy laws for the victims of domestic violence.

Tips:

- Inform the client that when a report is made to Police, even if no Statement is provided, or no charges or an Apprehended Domestic Violence Order is applied for, the Police will still make a referral to the Women's Domestic Violence and Court Advocacy Service and the client will receive a call from them.
- Whatever material your client gives to Police will likely be shared with the perpetrator if they plead not guilty to a criminal offence.
- Speak with Police to ensure that any identifying information is redacted prior to being provided to a perpetrator.
- If you are providing advice or representing a client that has separated from a former partner that is dangerous, you should advise them to immediately contact Centrelink and Medicare to de-link their account from the perpetrators account.
- Advise your client to change all passwords to ensure that their ex-partner cannot access their accounts including MyGov.
- Advise your client not to provide their full name when accessing support services such as 1800RESPECT as these records can be subpoenaed or obtained through a Freedom of Information Request.[1]

Information sharing

In 2014, the It Stops Here Pathway (Safer Pathway) was introduced by the government.

Once a domestic violence report has been made to Police, victims are automatically referred to the Central Referral Point (CRP) which is administered by Victims Services.[2] The victim's information is then referred to a domestic violence service provider in their area. In NSW, this is the Women's Domestic Violence Court Advocacy Service (WDVCAS).

In 2014, Pt 13A was introduced into the Crimes (Domestic and Personal Violence) Act 2007 (NSW), as part of the legislative amendments to support the *Safer Pathway* initiative.

The new Pt 13A allows information about victims and perpetrators to be shared between agencies and services. Section 98K clearly states that Pt 13A prevails over any privacy legislation.[3]

Part 13A

As part of the introduction of the new Pt 13A, the Domestic Violence Information Sharing Protocol (the Protocol) was introduced.[4]

Agencies and service providers that collect, use or disclose victims' or perpetrators' information must comply with the Protocol.[5]

Pursuant to s 98M, the Privacy legislation does not apply and agencies and service providers are permitted to share information about the victim and perpetrator without the consent of the victim or perpetrator where "the agency believes on reasonable grounds that":

> (a) the particular dealing is necessary to prevent or lessen a domestic violence threat to the person or any other person, and
> (b) the threat is a serious threat, and
> (c) the person has refused to give consent or it is unreasonable or impractical to obtain the person's consent.[6]

Whilst it is the case that consent is not required to be obtained, the Protocol states that the agencies and/or service providers should obtain the victim's consent to share personal and health information.[7] Despite this, it is the authors experience, that in most cases, the Police do not inform the victim that their information is automatically sent to the CRP and a referral will be made.

The victim is often unaware that their information has been shared until they are contacted by the service provider.

In situations whereby Pt 13A does not permit the sharing of information, s 27 of the Privacy and Personal Information Protection Act 1998 (NSW) exempts NSW Police from complying with the Information Protection Principles set out in Pt 2 Div 1 of that Act thereby allowing the Police to share this information.

Section 18 also allows information to be shared without the consent of an individual if that "disclosure is directly related to the purpose for which [it] was collected".[8]

Case study

As part of the author's work as the duty solicitor for the Women's Domestic Violence Advocacy Service (WDVAS), she met many victims of domestic violence who had their personal information shared with the service.

One of the female clients was in an extremely abusive, controlling, and coercive relationship. Her partner had connected their phones so that any calls, messages, emails etc she received would also go through to his mobile phone.[9]

The victim was not informed by Police that a referral would be made to the WDVCAS and therefore she did not have the opportunity to object to her information being shared.[10] This meant that when the Police shared her information, her partner became aware of this causing further abuse and trauma.

Of course, it was claimed that her information was shared for the "purpose for which it was collected" ie protecting a victim of domestic violence and that the Police "reasonably believed that the disclosure" was "necessary to prevent or lessen a serious and imminent threat to the life or health" of the victim.[11]

In this particular situation, what it did do was worsen the situation causing more of a risk to the life and health of the victim. This particular victim did not give permission for the WDVCAS to contact her or share her information to avoid angering her partner. She did seek assistance and support, but she advised them that she would contact the service when she was able to do.[12]

Disclosure vs privacy

Where a perpetrator pleads not guilty, the Police are required to serve them with a brief of evidence.[13] The legislation specifically states that the brief of evidence must consist of any statements obtained from witnesses they intend to call and "copies of any document or any other thing" that has been identified in those statements as a proposed exhibit.[14]

Whilst the legislation limits the information that is to be provided as part of the brief of evidence, the Prosecution's Duty of Disclosure requirements extend this scope to include all information/material which is or may be relevant to an issue in the matter,[15] all information obtained during the investigation and all material that may assist with the defence case.[16]

In the case of domestic violence, this may include text messages between the victim and witnesses, social media messages between the victim and other people, images, telephone call logs etc obtained from the victim's phone or other electronic device.

> I actually did fall to my knees because I knew this was huge and I knew this was going to really affect my life and this was going to shift it drastically.[17]

Section 187 of the Criminal Procedure Act 1986 (NSW) does allow the court to make an order that the brief or parts of it, need not be served provided "there are compelling reasons for not requiring service".[18] The Prosecution Guidelines state that where disclosing the material "may pose a threat to the personal safety of a person", with the approval of the Director or the Deputy Director, such material may withhold.[19] These provisions are rarely utilised and the Police quite often do not redact the information which potentially exposes victims and witnesses to further risk.

Take the case of Sophie Spittles for example. Ms Spittles separated from her former partner, after experiencing ongoing violent and abusive behaviour. In the media report, Ms Spittles said:

> I had a safety plan with a friend set up, that if anything out of my control was to happen and we were at risk, I was going to message him and he was going to call the police on my behalf . . .[20]

When she finally got the courage to leave him, Ms Spittles was horrifically assaulted, leaving her with a large laceration to her head, broken teeth, multiple bruises, a dislocated shoulder and dislocated jaw.[21]

The Police told Ms Spittles that they would only save the messages from that evening however, she later found out that the Police downloaded 11 years' worth of her phone records and provided it to the perpetrator as part of the brief of evidence.[22] When she confronted the Police, Ms Spittles recorded the conversation. She said, "You've given a senior bikie full access to my phone".[23]

The officer, who was not involved in releasing her private data said, "I don't know what you want me to say Sophie . . . He shouldn't have got it. The cops have f***ed up. We're going to investigate it".[24] But investigating it would not reverse the conduct of Police nor would it prevent the perpetrator from using her private data to further taunt the victim.

Not only did this expose the victim to further risk of harm, but it also allowed the perpetrator to access information and telephone numbers of witnesses thereby allowing him to make threats of harm to these people.[25]

One of the biggest issues when it comes to privacy protection is that the Police represent victims and therefore victims do not have their own legal representative. In these circumstances, the victim does not have an advocate that can ensure that all identifying information is redacted prior to it being shared with the perpetrator. As such, it is on Police to ensure that they have the victim's safety at the forefront of their mind and to act more prudently when preparing a brief of evidence.

When one considers the privacy laws, one must question whether a perpetrator's right to a brief of evidence outweighs the rights and safety of the victims.

"How can any victim of domestic violence trust a police officer if they know this police officer can do what he did and not get sacked"?

What about when the perpetrator is a member of the Police force? Or the perpetrator has friends or family that are a member of the Police force?

Victims are required to keep the Police informed of any changes to their details so that they can be contacted and where necessary, subpoenaed. How does this work when the perpetrator is a member of the Police force or has friends or family that are members of the Police force, and that person has free and unlimited access to Police records?

We already know that a lot of domestic violence goes unreported but when the perpetrator is a member of the Police force, the victim is generally more inclined not to report it for fear of repercussions and lack of assistance.[26] In the case involving Senior Constable Neil Punchard, the victim had every reason to be fearful about reporting the violence. This Officer accessed the victims address and leaked it to the perpetrator, his childhood friend.[27] Senior Constable Neil Punchard successfully appealed his 2 months suspended sentence, receiving only 140 hours of community service and no conviction.[28] The Queensland Police Service appealed this decision to the Court of Appeal. The decision is pending.[29]

"My heart just sank. I felt sick" — the impact of privacy breaches.

"I did everything right when I had the strength to leave him and he found me through no fault of my own,"[30] said one domestic violence survivor. The media articles reports that this survivor was the victim of domestic violence for a whole decade.[31] She had relocated interstate to escape the abuse.[32] She was diagnosed with Post Traumatic Stress Disorder (PTSD) following the extensive abuse she was subjected to.[33] When she finally found the courage to leave the abusive relationship, her symptoms began to ease but it wouldn't be long until they resurfaced.

In June 2016, the victim informed Centrelink that she had separated from her ex-partner. Regrettably, Centrelink did not acknowledge the separation as the victim did not provide the addresses of her two references.[34] Finally, in January 2017, Centrelink registered the separation but by this time, it was too late.[35]

Centrelink failed to separate the victim's records from that of her abusive ex-partner.[36]

They updated her former partner's account with the victim's new address. It was not until her ex-partner posted a photo of her new home on Facebook and wrote "Change your MyGov", that the victim became aware of this breach.[37] Her PTSD symptoms quickly returned; she will not stay anywhere overnight, she feels uncomfortable and fearful in public places and she "sleeps with a metal pole next to her bed."[38]

Services Australia was found to have "committed four breaches of the Privacy Act."[39] Services Australia was ordered to provide a written apology to the victim, pay her legal costs and compensate her in the amount of $10,000 for pain and suffering.[40]

"Services Australia acknowledges its processes failed to protect the privacy of this customer," said Services Australia General Manager Hank Jongen.

Now just a phone call away

Previously, victims had to complete a form and provide references confirming separation. Only after Centrelink were satisfied that two people had separated, would they register the separation. This is no longer the case.

Services Australia General Manager Hank Jongen said that: "Services Australia was 'acutely aware' of the heightened risks of separation for customers when family and domestic violence is a factor."[41] He said, "we have changed our process to require that we de-link a customer's Centrelink record from their partner's as soon as they tell us they've separated, without the need for paperwork".[42]

But this information is not widely known; the Services Australia website states, "You need to tell us if you separate from your partner. You can tell us using your Centrelink online account through myGov",[43] and "You can use the separation details form if you can't tell us online. If you told us you're separated as part of a new claim for a payment, you don't need to use this form."[44] The website goes on to say that a victim's former partner does not need to complete the form if it will place the victim's safety at risk.[45] Services Australia indicate that they may still require verification by a third party.[46] It is not until you get to the bottom of the page that the website informs victims of domestic violence that if they are in or have left a domestic violence relationship and are concerned for their safety, that they should contact them.[47]

The services Australia website does, however, provide victims with information about what they can do if they are experiencing domestic violence or abuse. The website states, "if someone else has access to your online accounts, you can change your passwords at any time."[48] Centrelink call records cannot be obtained by anyone other than the person requesting them.[49] The website says that the person can send an email requesting their call records.[50] This sounds all good and well, but what if the perpetrator has access to the victim's email address or creates an email address impersonating the victim? Surely, it is not as simple as sending an email and obtaining your call records.

How the law should look:

- Agencies that intend to share information involving victims of domestic violence must be required to inform the victim of their intentions.
- Agencies that intend to share information involving victims of domestic violence should obtain consent from the victim and if that consent is not obtained, make further enquiries with the victim as to why they are not giving consent. This could avoid further escalating the abuse such as in the Case Study above.
- Information should automatically be redacted from material which has the ability to locate or identify the victim and their details (subpoena material, brief of evidence for example).
- Regular audits should be conducted to ensure that Police are only accessing records that relate to their particular matter.

Sionea Breust
Principal Solicitor
SCB Legal
s.breust@scblegal.com.au
www.scblegal.com.au

Footnotes

[1] 1800RESPECT, How you do you handle subpoenas?, www.1800respect.org.au/faq/how-you-do-you-handle-subpoenas.

[2] NSW Police *Code of Practice for NSW Police Force response to Domestic and Family Violence* version 3 (2021). See also Crimes (Domestic and Personal Violence) Act 2007 (NSW), s 98F (CDPV Act).

[3] CDPV Act, above, s 98K.

[4] CDPV Act, above, s 98O.

[5] CDPV Act, above, s 98J.

[6] CDPV Act, above, s 98M(2).

[7] NSW Government, *Domestic Violence Information Sharing Protocol* (September 2014).

[8] Privacy and Personal Information Protection Act 1998 (NSW), s 18(1)(a).

[9] Based on authors experience in giving the client legal advice.

[10] Above.

[11] Above n 8, s 18(1)(c).

[12] Above n 9.

[13] Criminal Procedure Act 1986 (NSW), s 183(1).

[14] Above, s 183(2).

[15] See *R v Reardon (No 2)* (2004) 60 NSWLR 454; 146 A Crim R 475; [2004] NSWCCA 197; BC200403886 at [46].

[16] Peter Hastings QC, "Prosecutorial Ethics and Duty of Disclosure" (paper presented at Public Defenders Criminal Law Conference, Taronga Zoo, Mossman, 16 March 2013).

[17] H Cohen and R Hunjan "Police accidentally gave domestic violence victim's phone data to her attacker" *ABC* 3 June 2021, www.abc.net.au/news/2021-06-02/police-gave-domestic-violence-victim-data-to-attacker/100173270.

[18] Above n 13, s 187(1)(a).

[19] The Office of Public Prosecutions, *Prosecution Guidelines* (29 March 2021), ch 13.3.

[20] Above n 17.

[21] Above n 17.

[22] Above n 17.

[23] Above n 17.

[24] Above n 17.

[25] Above n 17.

[26] Ha Gleeson "More NSW Police officers charged with domestic violence as victims face ongoing problems getting help" *ABC* 10 May 2021, www.abc.net.au/news/2021-05-10/nsw-police-officers-charged-with-domestic-violence-2020-victims/100114114.

[27] B Smee "Julie's story: how police were part of the problem for a domestic violence victim" *The Guardian*, 5 September 2020, www.theguardian.com/australia-news/2020/sep/05/julies-story-how-police-were-part-of-the-problem-for-a-domestic-violence-victim.

[28] Above.

[29] Above.

[30] Hannah Ryan "Change your MyGov: Centrelink Breached domestic violence victim's privacy before abusive ex's taunt" *7 News,* 22 April 2021, https://7news.com.au/business/centrelink/centrelink-breached-dv-victims-privacy-c-2654545.

[31] Above.

[32] Above n 30.

[33] Above n 30.

[34] Above n 30.

[35] Above n 30.

[36] Above n 30.

[37] Above n 30.

[38] Above n 30.

[39] Above n 30.

[40] Above n 30.

[41] Above n 30.

[42] Above n 30.

[43] Services Australia, Your relationship status, 22 June 2021, www.servicesaustralia.gov.au/individuals/topics/your-relationship-status/30306#relationshipchanges.

[44] Above.

[45] Above n 43.

[46] Above n 43.

[47] Above n 43.

[48] Above n 43.

[49] Above n 43.

[50] Above n 43.

Uber found to have breached Australian Privacy Principles despite protest that the company does not carry on business in Australia

Martin Slattery *CARROLL AND O'DEA LAWYERS*

Key takeaway points

- Office of the Australian Information Commissioner (OAIC) determines that American-based Uber parent company Uber Technologies, Inc (UTI) and Netherlands-based subsidiary which collects data of Australian users are bound to comply with the Privacy Act 1988 (Cth) and Australian Privacy Principles (APPs).[1]
- Determination of OAIC has potential to affect any international company which has customers in Australia, creating an obligation that Australian users' data is kept in accordance with the APPs and exposing them to penalties under Australian law for any breach.
- Uber corporate practices have been the subject to international and local scrutiny for some time, this is the first example of the company's commitment to protecting user data being subject to disciplinary action under Australian law.

Ride-sharing app developer Uber has become a ubiquitous presence in Australia, pre-pandemic research shows that the company had grown from 1.3 million users in 2016 to 4.7 million users in 2019, overtaking the number of taxi users in the country.

While the company's presence in Australia and around the world has made some people uneasy in relation to its business model which disrupted principles of employment status and worker safety, with a Senate Inquiry recently recommending that a federal regulator be appointed to oversee gig-economy conditions,[2] there have also been concerns with respect to data collection and user privacy that has now culminated in a decision of the Australian Information Commissioner and Privacy Commissioner on 30 June 2021 which determined that Uber had "interfered with the privacy of approximately 1.2 million Australian riders and drivers".[3]

The decision requires that Uber update its privacy policies and practices and commission an independent expert to assist in the process but is not the first controversy the company has come into with respect to user privacy.

The controversies up to the OAIC decision

Uber's dubious usage of private information has been questioned for a number of years now: for example in 2014 Uber's in-house use of "God View" (which has now been re-dubbed the slightly less grandiose "Heaven Mode") was reported in a Buzzfeed article[4] where it was revealed that staff at Uber were able to view the movements of all passengers in real-time, with celebrities such as Beyonce and ex-partners being popular topics on the programme. Other reporters have written about Uber executives' unabashed use of "God Mode" to track their movements to meetings,[5] a party trick that had apparently been used by Uber since 2011.

More recently in April 2017, a former driver for rival company Lyft filed a class action against Uber claiming that between 2012 and 2014 Uber used its access to big-data to identify drivers that were working for both Uber and Lyft and ensure that those drivers were prioritised over drivers that were exclusively contracting for Uber so as to entice them to make the move to drive exclusively for the company.[6] This programme was dubbed by its inventor as "Hell".

Those among the growing number of Uber users might not be worried by the faux pas' that any start-up is bound to make during a phase of rapid growth, and to their credit the company has taken serious steps towards beefing up their handling of sensitive big data with a "Differential Privacy" programme[7] which ensures that staff at Uber who are analysing data are unable to identify any personal identifying data within the dataset (the company have even made the code for the programme open source so anyone can use it), the OAIC decision now calls into question whether Uber's attempts to tighten up data security are motivated by user protection or simply corporate lip service.

The OAIC decision

Background

The OAIC decision dealt with a data breach that occurred between 13 October 2016 to 15 November 2016 which saw hackers obtain the data of 57 million worldwide Uber users, including 1.2 million Australian accounts. Data accessed included the names, email addresses and mobile numbers of users as well as driver's license details of approximately 240,000 drivers registered on the app.

The decision was particularly critical of the fact that Uber took a year to disclose the fact that the breach had occurred and in the meantime had actually paid one of the hackers $100,000 to assist them in finding further data weaknesses in their system.

Uber's corporate structure

The respondents to the proceedings were Uber UTI who is the American based parent company and Uber BV (UBV) who was primarily responsible for initially collecting the data under a contractual arrangement with UTI.

In Uber's own words (taken from a submission Uber made to the Senate Economics References Committee in October 2015):

> Uber Australia Pty Ltd is a wholly-owned subsidiary of Uber International Holding BV, which is based in the Netherlands. Uber BV is in turn an indirect wholly owned subsidiary of Uber Technologies Inc.
>
> - Uber BV is responsible for the management of our international operations -- including our business strategy and development, and financial investments, including engineering.
> - Uber BV's management team sets the local business objectives for the Australian market, which are then supported by Uber Australia.
> - Uber Australia provides certain support services -- such as local marketing promotions to potential riders and drivers -- to Uber BV. Uber BV pays Uber Australia for the performance of those services.[8]

Relying on this corporate structure, UTI and UBV argued that the APPs and the Privacy Act did not apply to their operations as they said neither entity "carries on a business in Australia" under the definition contained at s 5B(2) of the Privacy Act.

Findings

The Commissioner disagreed with the submissions made by UTI and UBV, adopting the approach taken by the Federal Court in *Tiger Yacht Management Ltd v Morris*,[9] in particular looking at the following indicia:

- In order to be carrying on business, the activities must form a commercial enterprise.
- The words "carrying on" imply the repetition of acts and activities which suggest a permanent character rather than participating in a single transaction or a number of isolated transactions.
- A company may be carrying on business in Australia even though it does not have an identifiable place of business within Australia.

The decision stated that:

> [t]he fact that an activity which occurs in Australia might be controlled or facilitated by actions of the entity taken remotely and without the need for employees in Australia, does not necessarily mean that no relevant activity is performed by the entity in Australia.[10]

On that basis, the OAIC Decision determined that it did have jurisdiction to deal with the privacy breach and went on to declare that UTI and UBV had breached the Privacy Act and the APPs, namely:

> a. In the period 13 October 2016 to 15 November 2016, the Uber Companies interfered with the privacy of approximately 1.2 million Australian riders and drivers by:
>   i. failing to take reasonable steps in the circumstances to protect personal information they held from unauthorised access, in breach of APP 11.1
>   ii. failing to take reasonable steps in the circumstances to destroy or de-identify personal information they held in breach of APP 11.2.[11]

As critical as the determination is, the Commissioner stopped short of awarding compensation in respect of the breach, primarily because there was no individual complaint brought before the Commission by an affected user (perhaps because of the fact that Uber did not specifically inform affected users of the breach).

Uber has the ability to review the decision in the Administrative Appeals Tribunal although at the time of writing it is not clear whether a review will be sought.

Should Uber users be concerned?

While in many respect the horse has bolted with respect to the data breach in question, the 1.2 million users that were affected by the breach may well hold some concerns given the manner in which the company tried to deal with the breach in question. The decision found that while affected drivers were notified of the breach, the affected users were not. Instead the company relied on their public announcement of the breach and set-up a web page for concerned riders to register any concerns they may have. According to Uber, only one affected user in Australia registered a concern.

As described above, Uber also engaged with the hacker directly, offering them a contract to assist them prevent further breaches on the condition that the hacker promised not to use the data they had collected from the breach. Why this decision was made and how certain Uber is that the hacker will uphold their end of the bargain is a commercial decision for Uber, but one which affects all of the millions of affected users.

Finally, the legal approach UTI and UBV took in response to the OAIC investigation, effectively arguing that because of some creative corporate structuring that any arm of Uber that actually collects data on Australian users is immune from any obligations to comply with Australian law, raises broader questions as to whether the estimated 20% saving that Uber users enjoy when they opt not to hail a registered taxi is a saving they value more than their own privacy.

The OAIC determination is a landmark in Australia, but not the first time that Uber's data collection and handling has been legally scrutinised.

For example, serious concerns were a raised by the information provided by former Uber employee turned whistle blower Samuel Spangenberg who filed unfair dismissal proceedings against Uber. In the course of evidence in the proceedings Spangenberg filed a declaration late in 2016[12] which exposed under oath what he believed were a number of serious laxities in the way that Uber handled and used the data it collected.

Spangenberg's declaration annexed the data which Uber had collected on him as a user of the service and according to some analysts showed a wide ranging grab for data which was being used for a number of unclear purposes and that despite assurances made to date by Uber, including Assurances filed with the Attorney General of New York to put a hold on the company's use of "God Mode",[13] there is evidence of ongoing laxity towards privacy and data among staff at the company.[14]

The fact is that big data is being recognised more and more as a revenue generating asset for companies that can collect and leverage it,[15] Uber is well aware of this and has been making inroads into commercial partnerships through the sharing of user date with companies such as hotels for some time.[16]

Further, the company continues to diversify into food and freight delivery services, giving it more data and insights into the habits of its customers; it is not an exercise in speculative science fiction to imagine Uber having access to information about all of its users' daily habits and practices as the company continues to diversify and expand its presence in the market. In fact, last year a complaint was registered with the Victorian privacy commissioner over a practice in which it is alleged Uber required Uber Eats drivers to keep a copy of user's drivers licenses when they ordered alcohol.[17]

Beyond the issues already identified in this article, Uber has been reprimanded by Apple for breaching the tech giant's terms of service by designing a programme which deliberately hid from monitors at Apple that Uber was continuing its practice of collecting user's data after those users had elected to delete the app.[18] Uber has also been known to avoid investigation by authorities through a number of measures including "Greyballing", a programme designed by Uber that identified city officials and prevented them from accessing the app properly and therefore were unable to monitor it[19] and allegedly destroying evidence while under investigation for tax evasion in Quebec.[20]

While the OAIC decision and its implications will be relevant to many tech companies that have customers but no physical presence in Australia, it is also another in a long and increasing list of questionable examples of Uber's commitment to maintaining user privacy.

Martin Slattery
Partner
Carroll and O'Dea Lawyers
mslattery@codea.com.au
codea.com.au

Footnotes

1. *Commissioner Initiated Investigation into Uber Technologies, Inc and Uber BV (Privacy)* [2021] AICmr 34.
2. N Zhou "Call for federal regulator for Australia's gig economy after sixth delivery rider death revealed" *The Guardian* 26 June 202, www.theguardian.com/australia-news/2021/jun/27/call-for-federal-regulator-for-australias-gig-economy-after-sixth-delivery-rider-death-revealed.
3. Above n 1, at [2].
4. J Bhuiyan and C Warzel "'God View': Uber investigates its top new york executive for privacy violations" *Buzzfeed* 18 November 2014, www.buzzfeed.com/johanabhuiyan/uber-is-investigating-its-top-new-york-executive-for-privacy?utm_term=.tqjjn5EOBx#.gs4Rx5vVlb.
5. R McCormick "Uber allegedly tracked journalist with internal tool called 'God View'" *The Verge* 19 November 2014, www.theverge.com/2014/11/19/7245447/uber-allegedly-tracked-journalist-with-internal-tool-called-god-view.
6. J C Wong "Uber's secret Hell program violated drivers' privacy, class-action suit claims" *The Guardian* 25 April 2017, www.theguardian.com/technology/2017/apr/24/uber-hell-program-driver-privacy-lyft-spying.
7. K Tezapsidis, Uber Releases Open Source Project for Differential Privacy, 13 July 2017, https://medium.com/uber-security-privacy/differential-privacy-open-source-7892c82c42b6.
8. Uber, *Corporate tax avoidance* Submission 123 (October 2014) at p 4, www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Corporate_Tax_Avoidance/Submissions?main_0_content_1_RadGrid1ChangePage=13.

9. *Tiger Yacht Management Ltd v Morris* (2019) 268 FCR 548; 366 ALR 410; [2019] FCAFC 8; BC201900446.
10. Above n 1, at [57].
11. Above n 1, at [1].
12. *Declaration of Samual Ward Spangenberg file in opposition to defendant's motion to compel arbitration* (2016) www.documentcloud.org/documents/3227535-Spangenberg-Declaration.html.
13. *Investigation by Eric T Schneiderman, Attorney General of the State of New York of Uber Technologies, Inc* Assurance No 15-185 (2016) www.documentcloud.org/documents/3227663-NY-Attorney-General-Uber-AOD.html.
14. W Evans "Uber said it protects you from spying. Security sources say otherwise" *Reveal* 21 December 2016, www.revealnews.org/article/uber-said-it-protects-you-from-spying-security-sources-say-otherwise/.
15. B Marr "Big data facts: how many companies are really making money from their data?" *Forbes* 13 January 2016, www.forbes.com/sites/bernardmarr/2016/01/13/big-data-60-of-companies-are-making-money-from-it-are-you/#1ac3fd462d8f.
16. R Hirson "Uber: the big data company" *Forbes* 23 March 2015, www.forbes.com/sites/ronhirson/2015/03/23/uber-the-big-data-company/#5f25bf2218c7.
17. J Taylor "Uber Eats drivers told to take photos of ID for alcohol orders raising privacy concerns" *The Guardian* 30 October 2020, www.theguardian.com/technology/2020/oct/30/privacy-concerns-as-uber-eats-drivers-start-taking-photos-of-id-for-alcohol-orders.
18. L H Newman "Uber didn't track users who deleted the app, but it still broke the rules" *Wired* 24 April 2017, www.wired.com/2017/04/uber-didnt-track-users-deleted-app-still-broke-rules/.
19. K Hill "Uber doesn't want you to see this document about its vast data surveillance system" *Gizmodo* 19 May 2017, www.gizmodo.com.au/2017/05/uber-doesnt-want-you-to-see-this-document-about-its-vast-data-surveillance-system/.
20. W Evans "Uber said it protects you from spying. Security sources say otherwise." *Huffpost* 14 December 2016, www.huffingtonpost.com/entry/uber-said-it-protects-you-from-spying-security-sources_us_58506b9fe4b0a464fad3e498.

Australian
Trade Mark
Opposition Law
2ND EDITION
Andrew Sykes
LexisNexis
Butterworths

Privacy Law
Bulletin

"Oh my goodness. Shut me down. Machines making machines. How perverse"[1] — automated decision making in Australian law

Joshua Charlton *and* ***Toby Blyth*** *COLIN BIGGERS AND PAISLEY*

Automated decision-making systems raise serious privacy challenges. The General Data Protection Regulation (GDPR) shows one method as to how they may be regulated.

Automated decision-making (ADM) has become an increasingly prevalent facet of modern society. Both globally and within Australia, ADM increasingly permeates both the public and private spheres, regulating an ever-expanding scope of our lives. This article canvasses the use of these systems within Australia and globally and considers the privacy implications that they can have.

Kerr J of the Federal Court of Australia recently remarked in relation to these systems that: "What was once inconceivable, that a complex decision might be made without any requirement of human mental processes is, for better or worse, rapidly becoming unexceptional".[2]

A host of executive departments and agencies across Australia's federal jurisdictions utilise advanced computer systems to support government decision-making — these include the Australian Taxation Office (ATO), Centrelink, the Department of Family and Community Services and the Australian Department of Defence.[3]

Similarly, ADM systems are increasingly relied upon within the private sector through the following:

- Programmatic advertising is used by online platform operators in order to automatically generate advertising content based upon view data.[4]
- Automated bidding and purchasing software are utilised on online currency platforms to make buy and sell decisions.[5]
- Automated face-scanning software is being touted as a viable measure by which the suitability of job applicants can be determined.[6]
- Pricing algorithms are routinely employed in underwriting decisions.[7]

While ADM is not expressly prohibited in Australian law, and Australian law does not have the GDPR off-ramp (yet), there are relevant legal regimes in Australian law, which are dependent on the form of the decision and who is ultimately responsible for the decision-maker, for example:

- government action — administrative law
- commercial conduct — contract, consumer protection law and anti-discrimination law
- employment conduct — employment law and anti-discrimination law

None are a perfect fit but this area of the law is developing fast.

The rise of ADM

Throughout the globe, increasing calls have been made to regulate the use of ADM. Much of this attention has arisen within specific contexts — for example, in response to specific concerns that ADM may entrench and perpetuate existing bias,[8] in relation to the intersection between administrative law and ADM,[9] or within the context of discrimination law where concerns continue to mount that ADM could even be creating new and novel categories and classes of persons which may be, by nature, beyond human comprehension, and to potentially detrimental effect.[10]

However, within the specific context of privacy and data protection law attention has been somewhat less focussed.

As highlighted in a report released in 2018 by Privacy International, the aggregation of data can lead to powerful, and deeply private, insights that could cause damage when misused (either intentionally or, as is often the case with ADM, unintentionally) — for example:

> . . . when someone calls their best friend, visits a website of the National Unplanned Pregnancy Advisory Service, and then calls their doctor, we can assume that this person is probably thinking about an abortion, or is likely to have an abortion soon.[11]

The intersection of ADM and privacy law as an issue worthy of consideration in its own right for the simple reason that as ADM evolves (and eventually approaches the level of artificial intelligence), the ability to gather, interpret and utilise personal information in a manner which can intrude on privacy interests increases to a capacity never before seen.

International privacy jurisprudence — the GDPR off-ramp

Internationally, the regulation of ADM has largely fallen within general privacy legislation. Most notable among these regimes is the European Union's General Data Protection Regulation, more commonly known as the GDPR.

Article 22.1 of the GDPR provides this protection by providing that a data subject is furnished the positive "right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her".[12]

> **Art. 22 — Automated individual decision-making, including profiling**
>
> 1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
> 2. Paragraph 1 shall not apply if the decision:
>   (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;
>   (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
>   (c) is based on the data subject's explicit consent.
> 3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.
> 4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Facilitating this provision is Art 21 of the GDPR, which creates a general right to object to data processing, a right which can be exercised for a number of reasons including where Art 22 is breached.

This right is not new in Europe. Though underutilised, a right to be exempt from automated decision-making has existed since 1995 by virtue of Art 15(1) of the European Data Protection Directive 95/46/EC.[13]

The effect of the GDPR provisions is to create an off-ramp of sorts, which permits the subject of an automated decision to elect to have the decision in question made otherwise than through an ADM.

This off-ramp was tested recently in the District Court of Amsterdam by various claims brought by the App Drivers & Couriers Union against Uber Technologies (ADCU Case).[14] In the ADCU case, the union challenged the dismissal by Uber of four drivers who were dismissed primarily due to decisions made by Uber's ADM systems.

In three instances, this came about where Uber's ADM system detected (incorrectly) irregular trips associated with fraudulent activities. In the other, an ADM system was installed and utilised with the intention and effect of manipulating the driver's Uber app which led to their dismissal. In all instances, the drivers were dismissed, given no further explanation pertaining to their dismissal, and denied the right to appeal.

Subsequently, a claim was brought on their behalf by the Union under Art 22 of the GDPR. Thus, the court was tasked with determining the extent of protection which individuals have from "decision(s) based solely on automated processing . . ."

On 14 April 2021, the District Court of Amsterdam, accepting that the decisions in question were "to be regarded as decisions based solely on automated processing, including profiling, and which have legal consequences for the plaintiffs . . .",[15] concluded that the extent of this protection was indeed quite wide. The court ordered Uber's ADM decisions reversed, ordered that Uber undo the deactivation of the drivers' accounts, and ordered that Uber bear nearly €3.5 million in the Plaintiffs' costs.

It appears therefore that, at least in the wide array of European countries subject to the GDPR, the off-ramp created by Arts 21 and 22 provides significant protection from ADM systems.

Within the context of data protection and privacy law, this off-ramp may provide protection prospectively by permitting a person to circumvent a known unlawful system from the outset.

It may also provide protection retrospectively where private information or data is misused by an ADM system — in turn, creating a normative effect which protects others by incentivising the creation and use of compliant ADM systems. Effectively this brings ADM within the realm of existing privacy law, ensuring consistency between the privacy standards expected of human decision-makers and non-human decision-makers.

Australian Privacy Principles

In contrast to the European position, Australia does not have legislation which specifically addresses the privacy issues posed by ADM.

A right equivalent to Art 22.1 simply does not exist either within the state or commonwealth privacy regimes,[16] nor does any Australian human rights legislation contain a provision of similar effect.[17]

Certainly, there have been opportunities for the legislature and Australian regulators to consider whether such a right should be engrained in legislation. For example, more than a decade ago, in the Australian Law Reform Commission's (ALRC) Report 108 *For Your Information: Australian Privacy Law and Practice* the ALRC noted that there is: "research that indicates that computer software and hardware may not necessarily produce accurate and reliable results"[18] and that "the OPC should provide guidance on when it would be appropriate for an agency or organisation to involve humans in the review of decisions made by automated mechanisms."[19]

Whilst these concerns do not approach the level of suggesting that ADM systems could lead to privacy breaches through the sophisticated collation and use of data, they are alive to the idea that ADM systems may lead to inaccurate or unreliable results — a similar issue in that the person the subject of the decision is treated contrary to law.[20]

Whilst the ALRC did suggest there should be some form of guidance on these types of decisions providing human oversight to them (eventually enacted through the likes of the commonwealth ombudsman's "Automated decision-making better practice guide"[21]) the enactment of statutory rights to protect against the misuse of ADM were not suggested.

A more recent opportunity to consider the role of these ADM systems, and the potential privacy issues they pose, was the ACCC conducted "Digital Platforms Inquiry", released in July 2019.[22] However, whilst this inquiry does comment on the use of these systems, particularly within the private sector, no comment is made with respect to privacy or data protection principles.

The result of this, as it stands, is that a person aggrieved by an ADM decision can challenge the ADM system's decision only on ancillary grounds, rather than utilise an off-ramp which provides an as-of-right ability to object to an ADM decision purely on the basis that it was made by an ADM system.

It may appear that a need to provide such a right is premature. However, this is simply not the case. The various issues presented by ADM systems have already been brought before the courts, highlighting the insufficiencies of existing legal principles to cope with these new and novel technologies, and suggesting perhaps that legislative intervention is necessary.

ADM systems in practice: government action

The recent federal court case of *Pintarich v Deputy Commissioner of Taxation*[23] (*Pintarich*) is an example of one such case, albeit an example within the context of administrative and taxation law, where existing legal principles were showcased as unsuitable when applied to modern ADM systems.

In *Pintarich*, the ADM system in question was a system utilised by ATO to generate and send letters to taxpayers. This particular system automatically generated and sent to the taxpayer, Mr Pintarich, a letter which communicated to him that the ATO had determined to remit a certain general interest charge (GIC) from his tax bill which he would have otherwise been liable to pay ("first decision"). This letter was received by Mr Pintarich who, acting upon this letter, made a payment to the tax office which seemingly ought to have discharged his entire tax liability.

Problematically however, the ATO later confirmed that the December letter was not as conclusive as it might have first appeared.

The ATO stated that it was "issued in error . . . [and] did not include the entire amount of GIC which had accrued".[24] This error, as would later become apparent, arose when the ATO "keyed" certain information into an automated bulk letter-issuing system and that system manifested a decision entirely absent any subjective process of deliberation on their part. Accordingly, the ATO considered that Mr Pintarich still owed a tax debt and sent him a notice to that effect ("second decision").

Mr Pintarich sought judicial review of the "second decision" made by the ATO under the Administrative Decisions (Judicial Review) Act 1977 (Cth) in the Federal Court of Australia on the basis that it was made ultra vires.[25] The crux of his argument was that the original letter, produced by the ADM system, manifested a valid decision, thereby rendering the ATO functus officio[26] when it made the second decision.

Ultimately, and despite the insightful dissenting judgement of Kerr J as cited at the commencement of this article, Mr Pintarich was unsuccessful in his review. This meant that he was held liable for the greater amount.

The majority came to this conclusion based on reasoning developed within the context of human decision making in 1999,[27] a context divorced from the modern reality of ADM systems and their increasing prevalence, holding that the first decision manifested through the ADM system was in fact no decision at all as it was lacking in the requisite mental element. Therefore, according to the majority, the ATO were not functus when issuing the second decision thereby rendering it valid.

The *Pintarich* judgement only obliquely raises concerns within the realm of privacy law. However, it certainly shows the very real impact that these ADM systems can have, the insufficiency of the existing legal framework to deal with these new and increasingly prevalent systems, and therefore the pressing need for such systems to be provided for at law in Australia.

Similarly, though not litigated, the recent problems involving the Department of Human Services' now-defunct "robo-debt" system also highlights the real-world impact that these systems can have.

The robo-debt system used an automated process of data matching which is used to recover purported overpayments from Centrelink and former Centrelink recipients'.[28] Specifically, it compared to pay as you go income data reported by the ATO[29] against wage data reported to Centrelink, and determines benefit payment where there is a discrepancy between the two.[30]

Then, upon detection of a possible overpayment, robo-debt engaged in an automated process which concluded with a debt notice being rendered, which (under the legislation) the welfare recipient is required to *disprove,* not by virtue not of DHS's investigations but as a result of the action or inaction of the welfare recipient under investigation.

There are various issues associated with the ADM robo-debt system.

The main issue was that the system was (apparently) wildly inaccurate, causing erroneous debts to be communicated to vulnerable people, and causing unwarranted stress and strain to those who in actuality did not owe a debt at all.[31]

Further, scholars such as Terry Carney have noted that the manner in which the ADM system requires the welfare recipient to *disprove* the debt is an unlawful reversal of the onus of "because [DHS] is always responsible for 'establishing' the existence and size of supposed social security debts."[32]

The robo-debt system serves as an example of the real-world impact which ADM can have, as well as an example of just the type of issue which may have been resolved far more equitably and simply if, for example, the aggrieved welfare recipient had some sort of as-of-right ability to reject to their data being utilised to make a decision about them by an ADM system akin to the off-ramp enshrined in the GDPR.

Ultimately, a recent class-action brought to challenge the validity of the robo-debt system was settled out of court (for $112M),[33] meaning that we are yet to see how the Australian courts would have reacted to such a system.[34]

However, the fact that the law will need to grow and change as these ADM systems continue to prevail was recently judicially acknowledged in the nearby common law jurisdiction of Singapore in *B2C2 Ltd v Quoine Pte Ltd (Quoine)*.[35]

ADM systems in practice: business

In *Quoine,*[36] the Singaporean International Commercial Court considered the doctrine of contractual mistake within the context of a trading error made on an ADM cryptocurrency trading platform operated by Quoine.

Specifically, the court was asked to determine whether an ADM platform could enter a transaction that had a legally binding effect, and if so, how knowledge could be attributed to the ADM platform to ascertain whether such an agreement was in fact entered in mistake.

The alleged "mistake" in question was a trade initiated by B2C2 of its existing Ethereum cryptocurrency for Bitcoin which, due to a supposed error in the programmatic system, was traded at approximately 250 times the market rate at that time (to the benefit of B2C2).

While the court held, un-controversially, that ADM platforms could enter binding contractual relations, it is the latter part of its inquiry that is of most relevance within the context of ADM platforms.

In determining what knowledge could be attributed to the system, Thornley LJ held that with respect to relatively uncomplicated and rule-based "deterministic systems", that is, ADM systems which follow clear and understandable pre-programmed rules, that the relevant knowledge should be that of the programmer at the time that they wrote the program.[37] On this basis, he found in favour of the now-considerably-more-wealthy B2C2.

However, and problematically, he suggests that such a simple and common-sense approach would not necessarily translate with respect to more complicated ADM systems and that the legal system will be forced to develop as more complicated ADM systems arise:

> . . . the law in relation to the way in which ascertainment of knowledge in cases where computers have replaced human actions is to be determined will, no doubt, develop as legal disputes arise as a result of such actions. This will particularly be the case where the computer in question is creating artificial intelligence and could therefore be said to have a mind of its own.[38]

For example, with an advanced ADM system it would not be suitable to refer back to the knowledge or intentions of the programmer in question as it was in *Quoine*, because the relevant intention at the time may be far surpassed by the "intention" of the automated system borne out of their original lines of code.

This is because, unlike rule-based deterministic systems which rely upon the *application* of pre-programmed rules, advanced automated systems can operate by inferential reasoning. That is, these systems operate by *creating* the very rules upon which they operate through a continual process of inference based on historical data inputted into and then generated by, the system.[39]

This process is termed machine learning,[40] a method of programming synonymous with the rise of artificial intelligence and one in which the true nature of the ADM system changes and "evolves" with each inference.

In this instance, in much the same way as it may be impossible to understand an alien language, it may be impossible to understand the complicated and not-necessarily-human internal language of the complicated ADM system. It would be similarly impossible to ascertain the relevant knowledge of the ADM system.

This is an idea known in the technical community as the "black box problem" — expressed simply, the problem that "many of the computing systems programmed using Machine Learning are opaque: [and therefore] it is difficult to know why they do what they do or how they work".[41]

Obviously, this creates a number of legal issues but most relevantly, it will likely pose significant issues with respect to privacy and data protection law — if we are not even sure how a system is operating, how can we know if it is creating outputs in a manner compliant with existing privacy principles?[42] Further, how can existing legal principles understand, interpret and analyse this system so as to ensure it is utilised within the scope of the existing legal protection of individual privacy?

Australian legal response to the rise of the robots

Whilst the Australian legislature has had the opportunity to consider the enactment of express legislation to deal with the unique and complicated issues associated with ADM systems it has, to date, decided not to. We think that perhaps now the time is ripe that it ought to.

Australian courts have shown themselves to be quite adept at the use of old forms in new areas. For example, in *Thaler v Commissioner of Patents*,[43] the Federal Court determined patent ownership within the context of an extremely new and highly complicated AI program that it found was "invented" by an AI program:

> In my view, Dr Thaler, as the owner and controller of DABUS, would own any inventions made by DABUS, when they came into his possession. In this case, Dr Thaler apparently obtained possession of the invention through and from DABUS. And as a consequence of his possession of the invention, combined with his ownership and control of DABUS, he prima facie obtained title to the invention. By deriving possession of the invention from DABUS, Dr Thaler prima facie derived title. In this respect, title can be derived from the inventor notwithstanding that it vests ab initio other than in the inventor. That is, there is no need for the inventor ever to have owned the invention, and there is no need for title to be derived by an assignment.[44]

However, despite the ability of the common law to apply old principles in these new contexts, direct legislative intervention may be required to provide protection against ADM systems. *Pintarich* shows that established legal orthodoxy is sometimes not agile enough to apply cohesively to this complex and new technology. Similarly, the "robo-debt" saga shows the pressing and real impact that these systems have, and poignantly *Quoine* contemplates the reality that the law must develop to meet the new and novel challenges of adapting ADM systems, particularly artificial intelligence systems.

It seems then that a good starting point would be for Australia to take Europe's lead and adopt an explicit privacy "off-ramp" which permits a person to object to the processing of their data by an ADM system.

Whilst this does not solve all of the many and varied issues that this technology has and will create, it will be able to be utilised to help both businesses and individuals by providing a much-needed safeguard and by extension consistency and legal certainty.

Joshua Charlton
Solicitor
Colin Biggers and Paisley
joshua.charlton@cbp.com.au
www.cbp.com.au

Toby Blyth
Partner
Colin Biggers and Paisley
toby.blyth@cbp.com.au
www.cbp.com.au

Parts of this article relating to automated decision-making technologies, the Pintarich case and the "robo-debt" issue draw on an honours' thesis entitled "Executive 'Decisions' in An Era of Automation: The Once Inconceivable Rapidly Becoming the Unexceptional" submitted by Joshua Charlton to the University of Wollongong in fulfillment of his LLB(Hons) degree.

Footnotes

[1] C3PO, *Star Wars 11: Attack of the Clones.*

[2] *Pintarich v Deputy Commissioner of Taxation* (2018) 262 FCR 41; (2018) 108 ATR 31; [2018] FCAFC 79; BC201804205 at [47].

[3] Administrative Review Council *Automated Assistance in Administrative Decision Making* Report No 46 (2004) p 57–63.

[4] Australian Competition and Consumer Commission (ACCC) *Digital Platforms Inquiry* Final Report (June 2019) www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf.

[5] *B2C2 Ltd v Quoine Pte Ltd* [2019] SGHC(I) 03.

6. D Harwell "A face-scanning algorithm increasingly decides whether you deserve the job" *The Washington Post* 6 November 2019 www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/.
7. See for example B McGurk *Data Profiling and Insurance Law* 1st edn, Hart Publishing, 23 March 2019.
8. N T Lee, P Resnick and G Barton "Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms" *Brookings* 22 May 2019 www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/.
9. T Scassa "Administrative Law and the Governance of Automated Decision-Making: A Critical Look at Canada's Directive on Automated Decision-Making" (2021) 54(1) *UBC Law Review*.
10. B Mendoza, M Szollosi and T Leiman "Automated decision making and Australian Discrimination Law" [2021] 4 *ANZCompuLaw Journal* 93; J Gerards and F Z Borgesius "Protected Grounds and the System of Non-discrimination Law in the Context of Algorithmic Decision-making and Artificial Intelligence" (Draft, 2 November 2020) forthcoming in the *Colorado Technology Law Journal*.
11. Privacy International *Data is Power: Profiling and Automated Decision-Making in GDPR* (April 2017) p 2 https://privacyinternational.org/report/1718/data-power-profiling-and-automated-decision-making-gdpr.
12. General Data Protection Regulation, Art 22.1.
13. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* L 281/31

    > Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

14. District Court of Amsterdam Case C / 13/696010 / HA ZA 21-81; R English "Amsterdam Court orders reinstatement of Uber drivers dismissed by algorithm" *UK Human Rights Blog* 18 May 2021 https://ukhumanrightsblog.com/2021/05/18/amsterdam-court-orders-reinstatement-of-uber-drivers-dismissed-by-algorithm/.
15. Above.
16. Privacy Act 1988 (Cth); Privacy and Personal Information Protection Act 1998 (NSW); Health Records and Information Privacy Act 2002 (NSW); Privacy and Data Protection Act 2014 (Vic); Information Privacy Act 2009 (Qld); Personal Information and Protection Act 2004 (Tas).
17. B Mendoza, M Szollosi and T Leiman, above n 10, at 10.
18. Australian Law Reform Commission *For your Information: Australian Privacy Law and Practice* Vol 1 Report 108 (May 2008) para 10.83.
19. Above, para 10.84.
20. As to the lawfulness of facial recognition technology, see for example *R (on the application of Bridges) v Chief Constable of South Wales Police (Information Commissioner and others intervening)* [2020] EWCA Civ 1058; J Fasman *We see it all: Liberty and justice in an age of perpetual surveillance*, 2021, Public Affairs;
21. Commonwealth Ombudsman, Automated decision-making better practice guide, www.ombudsman.gov.au/publications/better-practice-guides/automated-decision-guide.
22. Above n 4.
23. Above n 2.
24. Above n 2, at [110].
25. *Pintarich v Deputy Commissioner of Taxation* [2017] FCA 944; BC201708129.
26. For an exploration of the doctrine of functus officio see, eg, Sn Moloney "Finality of Administrative Decisions and Decisions of the Statutory Tribunal" (2010) 61 *AIAL Forum* 35, 37; see also R Orr and R Breise "Don't think twice? Can administrative Decision Makers Change Their Mind?" (2002) 35 *AIAL Forum* 11; E Campbell "Revocation and Variation of Administrative Decision" (1996) 22(1) *Monash University Law Review* 30; *Walter Construction Group v Fair Trading Administration Corp* [2005] NSWCA 65; BC200501383.
27. *Semunigus v Minister for Immigration and Multicultural Affairs* [1999] FCA 422; BC9901855 at [19] affirmed by the Full Federal Court in *Semunigus v Minister for Immigration and Multicultural Affairs* (2000) 96 FCR 533; 60 ALD 383; [2000] FCA 240; BC200001115 at [11], [55] and [101].
28. Community Affairs References Committee, Senate *Design, scope, cost-benefit analysis, contracts awarded and implementation associated with the Better Management of the Social Welfare System initiative* (2017) para 1.6.
29. PAYG data comprises employee income figures which are reported to the ATO under compulsory reporting requirements in ss 12 to 35 of the Taxation Administration Act 1953 (Cth).
30. Above n 28; L Macleod "Lessons learned about digital transformation and public administration: Centrelink's online compliance intervention" (2017) 89 *AIAL* 59.
31. Eg S Medhora "Over 2000 people died after receiving Centrelink robo-debt notice, figures reveal" *ABC News* 18 February 2019 www.abc.net.au/triplej/programs/hack/2030-people-have-died-after-receiving-centrelink-robodebt-notice/10821272.
32. T Carney "Robo-debt illegality: The seven veils of failed guarantees of the rule of law?" (2018) 44(1) *Alternative Law Journal* 2.
33. Gordon Legal, Robodebt Class Action Settlement, https://gordonlegal.com.au/robodebt-class-action/.
34. However, compare the Office of the Australian Information Commissioner decision in *"WP" and Secretary to the Department of Home Affairs (Privacy)* [2021] AICmr2.

35. Above n 5.
36. Above n 5, at [205] and [208]–[211].
37. Above.
38. Above n 35, at [206].
39. M Zalnieriute, L B Moses and G Williams "The Rule of Law and Automation of Government Decision-Making" (2019) 82(3) *The Modern Law Review* 425, 432.
40. Above.
41. C Zednik *Solving the Black Box Problem: A Normative Framework for Explainable Artificial Intelligence* https://arxiv.org/ftp/arxiv/papers/1903/1903.04361.pdf#:~:text=The%20Black%20Box%20Problem%20is,problems%20in%20AI%20are%20opaque.&text=Unlike%20their%20colleagues%20working%20within,the%20relevant%20problems%20are%20solved; F M Alexandre *The Legal Status of Artificially Intelligent Robots: Personhood, Taxation and Control* (June 2017) https://ssrn.com/abstract=2985466; and L DL Carvalho "Spiritus Ex Machina: Addressing the Unique BEPS Issues of Autonomous Artificial Intelligence by Using 'Personality' and 'Residence'" (2019) 47(5) *INTERTAX* 425; book review: A Legal Analysis of NGOs and European Civil Society by P Staszczyk Alphen aan den Rijn: Wolters Kluwer 2019 pp 425–443.
42. See for example S Zuboff *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power,* Public Affairs, 2020
43. *Thaler v Commissioner of Patents* (2021) 160 IPR 72; [2021] FCA 879; BC202106774.
44. Above, at [189].

You can’t ask that: vaccination status

Andrea Beatty, *Chelsea Payne* and *Shannon Hatheier* PIPERALDERMAN

As the COVID-19 vaccine continues to roll out across Australia, entities regulated under the Privacy Act 1988 (Cth) (Privacy Act) should be conscious of their obligations when collecting, using or disclosing an employee’s vaccination status. In anticipation, the Office of the Australian Information Commissioner (OAIC) released guidance to assist regulated entities to comply with the Australian Privacy Principles (APPs) when handling health information related to COVID-19. The OAIC’s guidance addresses the limited circumstances in which regulated entities can collect information about an employee’s vaccination status and the process for collecting and storing such information correctly.

Australian Privacy Principles

Health information is classified under the Privacy Act as “sensitive information” and is accordingly subject to more stringent privacy protections. The collection of sensitive information, such as an employee’s vaccination status, is not permitted under APP 3 unless an exception applies. APP 3.3(a) permits a regulated entity to collect sensitive information about an individual where that individual consents to the collection of the information and the information is reasonably necessary for one or more of the entity’s functions or activities. Although the OAIC indicated that this exception will apply in limited circumstances, the regulator did suggest that “preventing or managing COVID-19”[1] may constitute a reasonably necessary function or activity of a regulated entity.

The OAIC equally recognised the possible applicability of the exception under APP 3.4(a), which permits the collection of sensitive information without an individual’s consent where its collection is required or authorised by Australian law. Relying on this exemption, state and federal rules were recently introduced requiring individuals working in healthcare, public transport and hotel quarantine to be vaccinated. Though presently limited to high-risk sectors, the Australian Industry Group predicts there will be other areas where proof of vaccination will be necessary, particularly among workplaces involving a high degree of contact with vulnerable people.[2] However, until such public health orders are put in place, Australian Council of Trade Union Secretary Sally McManus warns against allowing entities to collect vaccination information about their employees.[3]

Australian Industry Group proposal

Concern surrounding employers’ access to vaccination data was raised following a proposal by Australian Industry Group Chief Executive Innes Willox to speed up Australia’s vaccine rollout.[4] Specifically, Willox recommended allowing large employers to act as vaccination hubs by having nurses administer the vaccine within the workplace. However, entities have expressed concern over potential liabilities that may arise if an employee has an adverse reaction to the vaccine. To overcome this complication, the government would need to indemnify employers who encourage or mandate vaccination.

Despite concerns raised surrounding privacy obligations, Willox believes employers should have a legal right to collect data on the vaccination status of employees to manage COVID-19 outbreaks and identify those who may be more at risk. Due to less stringent privacy obligations and a higher rate of vaccination, companies in the United States have taken a more proactive approach to the vaccination rollout. Listed below are some prominent examples:

- *Amazon*
  E-commerce giant Amazon initially partnered with government leaders to vaccinate over 20,000 of its warehouse and grocery store employees. It has subsequently established on-site vaccination facilities as more doses continue to become available and are offering a cash incentive of US$40 per vaccine to frontline staff who opt for offsite immunisation. New recruits are also reportedly given a bonus US$100 on their first day at fulfilment centres if they produce their vaccination record.
- *JPMorgan Chase and Morgan Stanley*
  Wall street bank, JPMorgan Chase requested all its employees to receive the COVID-19 vaccine before returning to the office. The bank is also exploring the possibility of making vaccination mandatory among staff however, is reportedly experiencing significant backlash from staff resistant to disclosing their vaccination status to the company. Similarly, Morgan Stanley have barred their employees from returning to the office until vaccinated and require employees to disclose their vaccination status to the company.

- *Starbucks and McDonald's*
  Starbucks and McDonald's have chosen not to mandate vaccination but rather have opted to encourage employees to get immunised by offering up to 4 hours of paid time off for when staff receive the vaccine. Starbucks have also offered an additional 4 hours of paid time off to staff who experience vaccine-related side effects within 48 hours of having received each dose. McDonald's stated that they have no intention of making vaccination mandatory but will nevertheless do its best to "encourage vaccination and connect employees to trusted, third-party experts"[5] who can guide them through the process.

Therapeutic Goods Administration Regulations

In light of the success of company-based initiatives and incentives, Australia has made efforts to follow suit. On 9 July 2021, the Therapeutic Goods Administration (TGA), who regulates the advertising of therapeutic goods, introduced temporary regulations[6] to allow businesses to advertise as well as offer incentives to people who have been fully vaccinated under the government's national COVID-19 vaccination program. Under the new regulations, businesses are allowed to create their own content promoting COVID-19 vaccines so long as it is consistent with current Commonwealth health messaging regarding the national COVID-19 vaccination program. Businesses are also authorised to offer cash and other rewards, excluding alcohol and tobacco, to individuals who have received two doses of a COVID-19 vaccine. Airlines QANTAS[7] and Virgin Australia[8] have both announced incentive programs, offering frequent flyer points and free flights to Australian residents who get vaccinated. Companies including Domain, Zip and the Big 4 Banks have also offered employees paid vaccination leave to make it easier to attend vaccination appointments. The temporary regulations are due to expire on 31 December 2022.

The implications of the new TGA regulations on compliance with obligations under the Privacy Act are however unclear. According to the temporary regulations, businesses can only refer to COVID-19 vaccines generally when offering a reward. This is presumably intended to avoid discrimination between vaccines and limit disclosure of personal information to a minimum. The regulations however, fail to specify how verification of vaccination is to be carried out. As regulations fall within the meaning of "Australian Law" under the Privacy Act, it is possible that the regulations are covered by the previously mentioned exemption to the ban on the collection of personal information under APP 3.4(a). Provided the exemption applies, businesses will nevertheless need to comply with the notification and disclosure requirements specified in APPs 5 and 6. The OAIC also recommends businesses to accurately record the information it collects and store it securely.

Key takeaways

As Australia's vaccination rollout continues, the strict distinction between privacy obligations and a desire to keep workplaces safe will increasingly become less clear. Though incentives and rewards for vaccinations have the capacity to boost vaccination rates, it is unlikely they will emerge until vaccination is made widely available to the public.

The progression of the vaccination rollout will also raise a number of novel legal questions around whether employers can force an employee to consent to disclose information about their vaccination history. This will be of particular concern in the context of employees who cannot (for medical reasons) obtain vaccination, therefore raising the possibility of claims for unlawful disability discrimination. At present it is important for employers to remain up to date with public health orders and adapt to the requirements under the Privacy Act as they change.

Andrea Beatty
Partner
PiperAlderman
abeatty@piperalderman.com.au
www.piperalderman.com.au

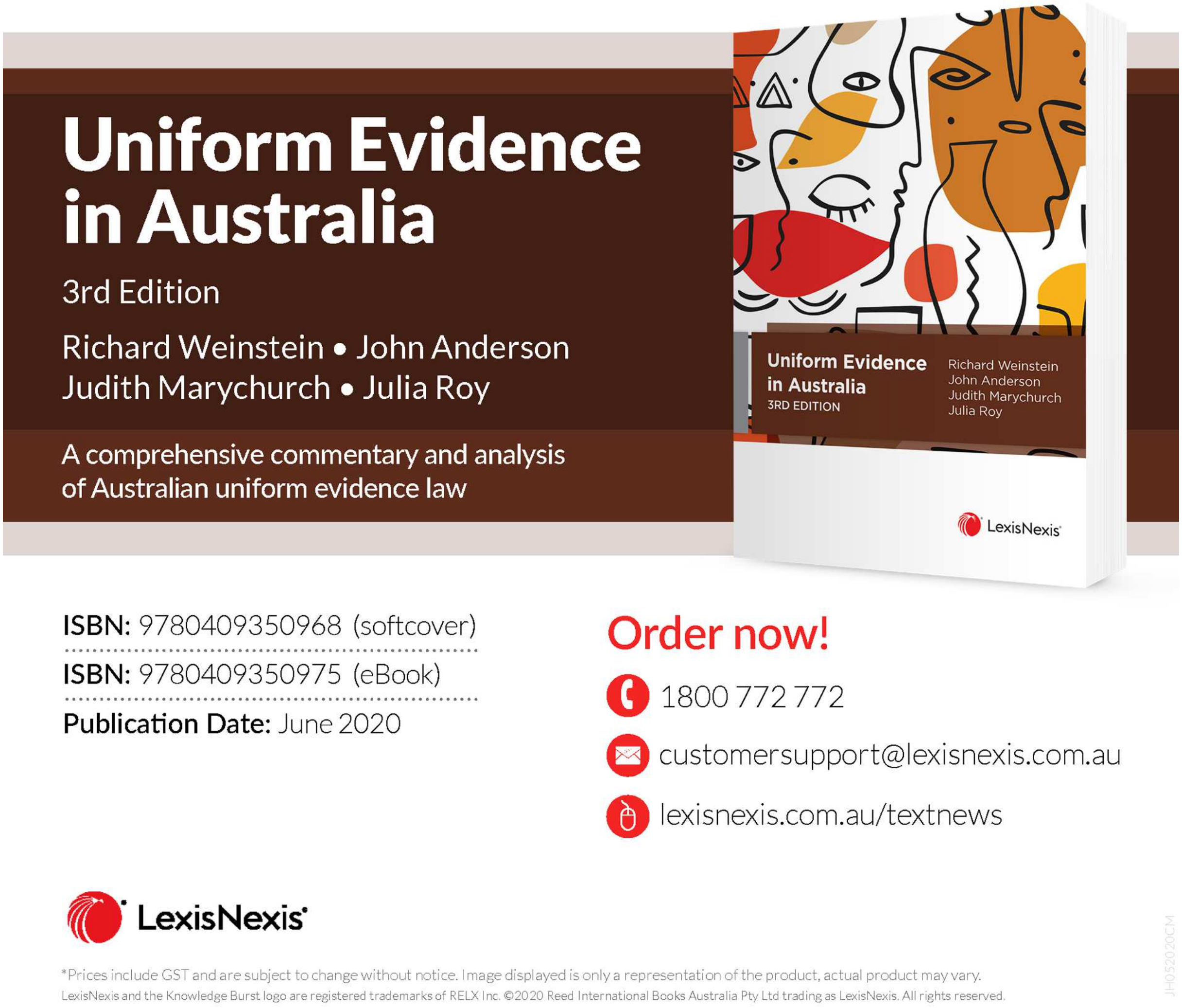
Chelsea Payne
Associate
PiperAlderman
cpayne@piperalderman.com.au
www.piperalderman.com.au

Shannon Hatheier
Law Clerk
PiperAlderman
shatheier@piperalderman.com.au
www.piperalderman.com.au

Footnotes

[1] Office of the Australian Information Commissioner, Coronavirus (COVID-19) Vaccinations: Understanding your privacy obligations to your staff, 23 February 2021, www.oaic.gov.au/privacy/guidance-and-advice/coronavirus-covid-19-vaccinations-understanding-your-privacy-obligations-to-your-staff/.

2. J Taylor "Australian unions reject unacceptable proposal allowing employers access to staff vaccination data" *The Guardian* (2 July 2021), www.theguardian.com/australia-news/2021/jul/02/australian-unions-reject-unacceptable-proposal-allowing-employers-access-to-staff-vaccination-data.
3. Above.
4. Australian Industry Group "AI Group involvement in COVID Vaccine Taskforce consultations" media release 7 July 2021.
5. K Breen "McDonald's is paying employees to get the COVID-19 vaccine" *Today* (3 February 2021) www.today.com/food/mcdonald-s-will-pay-employees-receive-coronavirus-vaccine-t207807.
6. Department of Health, Therapeutic Goods Administration, Covid-19 vaccine advertising and import compliance, 9 July 2021, www.tga.gov.au/communicating-about-covid-19-vaccines.
7. G Cockburn "QANTAS boss Alan Joyce to offer 'mega prizes' of unlimited travel for COVID-19 vaccine recipients" *The Australian* (31 May 2021) www.theaustralian.com.au/breaking-news/qantas-flirts-with-offering-incentives-to-australians-who-get-vaccinated/news-story/aa208d56a1435c9516a82e638 9899847.
8. V Croll "Virgin Australia to launch vaccination competition with one million Velocity Frequent Flyer Points up for grabs" *HeraldSun* (23 June 2021) www.heraldsun.com.au/news/breaking-news/virgin-australia-to-launch-vaccination-competition-with-one-million-velocity-frequent-flyer-points-up-for-grabs/news-story/c3779b97d0078cb0e65337e0f9110814>.



For editorial enquiries and unsolicited article proposals please contact Genevieve Corish at genevieve.corish@lexisnexis.com.au or (02) 9422 2047
Cite this issue as (2021) 18(5) *PRIVLB*
SUBSCRIPTION INCLUDES: 10 issues per volume plus binder www.lexisnexis.com.au
SYDNEY OFFICE: Locked Bag 2222, Chatswood Delivery Centre NSW 2067
CUSTOMER RELATIONS: 1800 772 772
GENERAL ENQUIRIES: (02) 9422 2222
ISSN 1449-8227 Print Post Approved PP 243459/00067

This newsletter is intended to keep readers abreast of current developments in the field of privacy law. It is not, however, to be used or relied upon as a substitute for professional advice. Before acting on any matter in the area, readers should discuss matters with their own professional advisers.