2021 Annual Privacy Law Update

KING&WOOD MALLESONS
金杜律师事务所

1 Introduction

Continuing the theme from recent times, the past year has been another bumper year for privacy law in Australia and around the world, with an array of developments capturing the attention of privacy law enthusiasts like us.

From an Australian perspective, the iceberg on the horizon is the federal Government's wide-ranging review of the Privacy Act. The somewhat slow-moving review was originally prompted by the ACCC's landmark Digital Platforms Inquiry but has significant implications for the economy as a whole. While in this update we look at the current state of play at the time of writing, further developments are imminent with a further discussion paper setting out more concrete details of the Government's proposed reforms soon to be released.

Apart from the Privacy Act reform process, there have been plenty of other legislative developments of note from a privacy perspective, perhaps the most notable being the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 that proposes to confer a range of new warrant powers on law enforcement agencies. This is emblematic of an ongoing challenge our law-makers face around how to balance individual privacy interests against other countervailing concerns, such as enabling law enforcement and national security agencies to effectively investigate and counteract harmful activities that take place online. These aren't easy matters to solve and we expect there will be ongoing tension in this area for some time to come.

More broadly, we have seen growing interest from a range of regulators in privacy- and data-related matters. Most prominently, the ACCC has been very active in pursuing organisations that it considers are misleading consumers about their data management practices. Along with a more active OAIC, this is a sign we have moved into a new phase of more aggressive enforcement of privacy laws in Australia.

There is no better illustration of this than the recent determination made by the OAIC against global ride-share giant Uber. This determination has put global technology businesses on notice that the Commissioner intends to hold them to account under the Australian privacy regime, even if they don't have a significant (or indeed any) on-the-ground presence here.

All this, and so much more, awaits you in the pages ahead, dear reader. In a rapidly changing global environment, it's been a strange, wonderful, challenging year and we are pleased to capture all of the highlights in this latest edition of our annual Privacy Law Update. As always, if you would like to understand how any of the issues discussed below may affect your organisation, please get in touch with one of KWM's privacy experts.

2 Review of the Privacy Act

We are, figuratively speaking, settled in at base camp anticipating with some trepidation the challenges associated with scaling the Everest of privacy law reform that lies ahead.

The Attorney-General first foreshadowed that there would be a major review of the Privacy Act, the centrepiece of Australia's privacy law framework, in December 2019 as part of the Government's response to the ACCC's Digital Platforms Inquiry. However, it was not until October 2020 that we saw the release of the first 'issues paper' for public comment (read more about that here). The issues paper was intended to help the Government refine its reform agenda, based on the themes first identified by the ACCC, with a more detailed 'discussion paper' promised to follow in early 2021. The discussion paper is expected to seek feedback on more specific options for reform. However, at the time of writing, it has not yet been issued (though all indications are that it is imminent). Nonetheless, while the steeper slopes still lie some way ahead, it is worth reviewing the path this reform process has followed to date.

Potential scope of reforms

It is clear from the issues paper alone, and the wide range of public submissions made in response, that the potential scope for reform is extensive, with implications reaching right across the economy and far beyond the online platform operators that were the focus of the Digital Platforms Inquiry. For example, the issues paper contemplates changes to foundational concepts such as the definition of 'personal information', clarifying (or expanding) the extra-territorial reach of the Act, strengthening consent and notification frameworks, introducing possible 'no go' zones in the form of uses of personal information that would be prohibited even if consent is obtained, revising rules on overseas data transfers, introducing new certification regimes, introducing direct rights of action for individuals along with a new statutory tort for invasion of privacy (an oft-discussed reform proposed in past reviews), and arming the OAIC with a wider range of enforcement powers with higher maximum penalties.

The response period for the issues paper formally closed at the end of November 2020, and submissions were published on the Attorney-General's Department website in stages from December 2020 through to June 2021. Feedback was extensive and detailed across a wide variety of government, public sector, commercial and civil society entities, as well as from individuals. In particular, the OAIC's submission ran to 150 pages and is worth reading in its own right for a detailed insight into the Commissioner's perspective on the future of the law and areas in most need of reform. In addition to the detailed responses on the issues put forward for comment, the OAIC in its submission also advocated for a range of additional operational accountability requirements, including a positive obligation for organisations to adopt a 'privacy by design' and, perhaps more importantly, 'privacy by default' approach to their management of personal information. This could drive significant operational changes within many organisations, including by requiring the implementation of an ongoing privacy management program and the completion of privacy impact assessments before undertaking new initiatives that may have a privacy impact.

The OAIC also advocated for a range of changes to the notifiable data breach regime, including hard deadlines for reporting breaches, civil penalties for not complying with prescribed timeframes, and positive obligations to mitigate the impact of a breach on individuals (while still acknowledging that a notifiable breach may arise where there is no fault).

Broad cross-section of responses

The broad cross-section of submissions in response to the issues paper shows the potential significance of these reforms, and the different vested interests that lie across the economy. However, a review of the responses shows that on a range of issues the views are not consistent – even within sectors – and a number of submissions raised new issues for consideration that were not contemplated in the issues paper.

To take just one example, there was significant disagreement among the submissions on whether to retain or amend the definition of 'personal information' – clearly a critical feature of the Act. A number of submissions advocated aligning the definition with the definition of 'personal data' under the GDPR. The rationale for this is that it may help to avoid some of the ambiguity that has arisen in relation to the interpretation of the current definition used in our Act (particularly as to when information can be said to be 'about' an individual) while also giving consumers comfort that their data will receive a consistent level of protection across jurisdictions, with Australia aligning to the high watermark that many consider the GDPR to represent.

However, other submissions considered that the current definition used in our Act does not require amendment, while yet others considered that the current definition could be tweaked or clarified in another manner without needing to adopt the GDPR drafting. For example, while the issues paper queried whether changes should be made to clearly capture technical data and inferred information, several submissions noted that the current definition is already sufficiently broad and flexible to encompass those types of information. For its part, the OAIC advocated for a broader definition of personal information, though stopped short of recommending that technical data automatically be included and instead suggested that the scope of the definition could be clarified via guidance and explanatory materials.

The range of views expressed on this core concept alone illustrates the challenges that the Government will face in crafting reforms that strike the right balance between competing interests and perhaps explains the delay in releasing the much-awaited discussion paper.

What's next?

As yet, it is not clear how the Government will respond to the various issues ventilated in the submissions made in response to the issues paper. However, given the diverse range of views that have been expressed, there may be less appetite for the Government to push through radical changes on a sweeping basis. Notably, at the same time as the general reform process, the Government and the OAIC are also working on a framework for the introduction of a new code of practice that would apply specifically to social media and online platform operators. Some may consider it odd that such targeted reforms would be considered before the general baseline has been settled. However, the narrower scope of the code may allow freedom to push through more radical changes for some sectors that would prompt stronger opposition if applied more broadly. If that is the case, then we may expect more of the same in the future. For example, a separate paper by the Department of Home Affairs on cyber security released in July 2021 proposed the introduction of a code of practice under the Privacy Act (potentially targeted to "specific kinds of technology, sectors or kinds of data") to define new cyber security standards for personal information.

In any event, the forthcoming discussion paper will likely reveal much more about the expected direction for the Privacy Act review and the specific reforms that will be considered in the scope of that review. We have our crampons and ice picks ready for the coming ascent.

3 The ACCC's penchant for privacy continues

A key trend over the past few years, best encapsulated in the Digital Platforms Inquiry, has been the increasing interest of the ACCC in privacy-related matters. It is clear from both from the privacy-related recommendations in the 2019 Digital Platforms Inquiry report (read more on that here), and from subsequent enforcement actions, that the ACCC sees privacy as a key consumer protection issue. It is also clear that the ACCC is not content to wait on privacy law reforms to address the concerns that it has identified, and that it will use its powers under the Australian Consumer Law (ACL) to take action against what it considers to be misleading data handling practices.

ACCC takes action

One of the first cases of this type brought by the ACCC was in mid-2020, against HealthEngine, an online health marketplace. We covered this case in last year's privacy law update but – for those readers who may not immediately recall the details (a small minority, obviously) – in summary, HealthEngine was found to have misled consumers in breach of the ACL in relation to its provision of personal information to private health insurers and its publication of online patient reviews. In that case, HealthEngine accepted its conduct was misleading, notwithstanding various disclosures made in its privacy policy, because it was not sufficiently clear that third parties would be provided with personal information. HealthEngine also accepted that it had breach the ACL by selective publication of only positive patient reviews. In total, HealthEngine was ordered to pay $2.9 million in penalties for these contraventions.

ACCC v Google

Evidently the HealthEngine case was just a sign of things to come. In the wake of that success, the ACCC has brought a number of subsequent actions under the ACL targeting what it considers to be misleading data management practices. And the ACCC has not shied away from taking on big targets, with a number of actions targeting the same global online service providers that were in the ACCC's crosshairs during the Digital Platforms Inquiry. In one such action, the ACCC alleged that Google misled users about the collection and use of personal location data from Android mobile devices. In April 2021 the Federal Court issued a judgement that, at least in part, agreed with the ACCC. The ACCC considers this decision a "world-first" in the area of privacy and data collection by big tech companies.

The factual details of the Google case are complex. However, essentially the issues centred on whether users of Android mobile devices were properly informed about the collection and use of location data. The ACCC case centred around two particular settings on Android devices: the 'Location History' and 'Web & App Activity' settings. While the Location History setting was by default turned 'off', the Web & App Activity setting was defaulted to 'on'. With the Web & App Activity setting turned 'on', Google could still obtain, retain and use certain types of personal location data. The ACCC said this was misleading. Google argued that it provided adequate information about these settings on a range of different options screens, which linked through to Google's privacy policy, where further detail about data collection practices was available. The ACCC disagreed.

In his judgment, Thawley J accepted that if users read all of the relevant screens, or read the privacy policy, then they may not have been misled. However, Thawley J also found that it was not reasonable to expect that all users would have read all of the screens or the privacy policy – that is, not everyone would have taken the time to click on all the links necessary to gain a full understanding about what would happen with their location data. In that context his honour found that some reasonable users would have been misled. This delivered the ACCC a partial victory, though on a number of other claims it was unsuccessful. The matter is continuing before Thawley J, and it is yet to be confirmed whether Google will appeal.

While the judgment in this case is fact-specific and, therefore, somewhat narrow in scope, it highlights the need to consider how information provided to users, the context in which that information is provided, and whether the information made available would be misleading if not read with further information which is also available but in a separate location. It clearly is not enough for organisations to cover everything in their privacy policy and then trust that all users will be diligent enough to read the policy in detail. Reasonable users may exhibit a range of different behaviours and privacy disclosures need to be designed to ensure that all reasonable users – including those who may not take the time to click through to read all available information – are adequately informed about what may happen with their data.

Key takeaways

There are a few important lessons that can be learnt from the Google case:

- **A comprehensive privacy policy is not enough!** While it is naturally important to ensure that your privacy policy is accurate and comprehensive, that may not be enough to ensure that you're compliant with the ACL. You need to consider the information you make available to consumers as a whole to ensure that they will not be misled about your information management practices. The responsibility for making sure that consumers are properly informed rests with the organisation and not with the consumer.
- **Be careful when summarising or paraphrasing.** In summarising data collection and usage practices it is not just what is said, but what is not said, that contributes to the overall representation. In the Google case, the court noted that consumers could assume that summaries will be accurate so that they may not take time to read the full detail. Again, that means that the onus is on businesses to ensure that the summaries they provide capture all key details.
- **Put yourself in the shoes of the consumer.** Review your customer collateral from the customer's perspective, taking into account the context of when a customer will be reading those materials. You cannot assume that a customer will carefully and meticulously pore over the legal terms. How you use headings and what information is emphasised will go to the overall representations made to customers.

It will be important for businesses to heed these lessons, as there is no sign of the ACCC's interest in privacy issues slackening. It has never been more important to ensure that you are communicating clearly with your customers about your intentions in relation to their data. And it is clear that detailed technical documents, like privacy policies, will not by themselves provide an adequate shield against consumer law actions.

4 National security laws raise privacy concerns

Combatting criminal activity and national security threats online has long been an important item on this Government's agenda. Over the last few years, this has resulted in a number of new laws being passed to bolster investigatory powers of Australia's law enforcement and national security agencies. However, the tension between these powers and privacy interests is obvious.

4.1 Privacy concerns relating to the SLAID Bill

The recently introduced Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (Cth) (SLAID Bill) would amend a number of existing laws to introduce a range of new investigatory powers for law enforcement, including three new types of warrant:

- a 'data disruption warrant' (DDW), which would enable the AFP and ACIC to access data on one or more computers for 'disruption' – including adding, deleting or changing the data – for the purpose of frustrating the commission of criminal activity;
- a 'network activity warrant' (NAW), which would enable the AFP and ACIC to collect intelligence on broadly defined 'criminal networks of individuals' who use the same online service; and
- an 'account takeover warrant' (ATW), which would allow AFP and ACIC to takeover a person's online account and lock that person out.

These new powers may obviously raise a range of privacy-related and other concerns. The Senate Standing Committee for the Scrutiny of Bills, and the Parliamentary Joint Committee on Human Rights have each considered the SLAID Bill and proposed a number suggested amendments. The SLAID Bill was also referred to the Parliamentary Joint Committee on Intelligence and Security by the Minister for Home Affairs, with the Committee calling for public submissions and holding a series of public hearings in the first half of 2021. The OAIC's submission was broadly reflective of the tone of many submissions in acknowledging the importance of combating serious crime, and balancing privacy interests against other policy interests, while remaining concerned about the scope of the proposals. Its submission stated:

> *"The OAIC acknowledges the importance of law enforcement agencies being authorised to respond to cyber-enabled and serious crime. However, the Bill's proposed powers are wide-ranging and coercive in nature. For example, DDWs and NAWs may authorise entering specified premises, removing computers or data, and intercepting communications. NAWs can authorise the use of surveillance devices, and both DDWs and NAWs may authorise the concealment of certain activities done under these warrants.*

These powers may adversely impact the privacy of a large number of individuals, including individuals not suspected of involvement in criminal activity, and must therefore be subject to a careful and critical assessment of their necessity, reasonableness and proportionality. Further, given the privacy impact of these law enforcement powers on a broad range of individuals and networks, they should be accompanied by appropriate privacy safeguards.

The OAIC considers that the Bill requires further consideration to better ensure that any adverse effects on the privacy of individuals which result from these coercive powers are minimised, and that additional privacy protections are included in the primary legislation.

The Committee's final report was published just prior to this publication 'going to print' in the digital sense, and contains dozens of recommendations for amendments. It remains to be seen which of these, or of the other concerns raised in submissions or by other Parliamentary committees, will be incorporated by the Government into the Bill. However, the underlying tension between protecting the privacy of online activities while still enabling law enforcement and national security agencies to do their work effectively, is unlikely to go away any time soon. Ongoing concerns about the use of encrypted communications services are another prime example – as consumers move to encrypted services to keep out prying eyes, law enforcement agencies are clearly concerned about their ongoing ability to investigate illegal activities that are coordinated via these services (having to resort to creative operations like the highly successful An0m sting in order to keep pace). These are big issues for any society to grapple with, and we expect the debate to continue for some years to come.

4.2 Use of existing assistance and access powers in practice

Several years have now passed since the introduction of the controversial industry assistance and access powers in the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (Assistance and Access Act). The manner in which this legislation was passed, with little consideration apparently being paid to the very significant weight of public submissions made in response to the draft legislation, drew heavy criticism from the technology sector and civil liberties groups (read more here). However, the way that the Assistance and Access Act has been used in practice suggests that the worst concerns have yet come to pass.

The Department of Home Affairs' annual report into the *Telecommunications (Interception and Access) Act 1979* (Cth) contains a statutorily-required summary of the number of access requests and notices (TARs and TANs) issued under Assistance and Access Act during the year, along with the of capability notices (TCNs) issued to require development of new technological capability intended to enable assistance to be provided where necessary. For the most recent data available, released in March 2021 for the prior financial year, that was a total of 11 TARs, and no TANs or TCNs:

Agency	Requests or notices given			
	Technical Assitance Request	Technical Assitance Notice	Technical Capability Notice	TOTAL
ACIC	1	-	-	1
AFP	3	-	-	3
NSW Police	7	-	-	7
TOTAL	11	0	0	11

Of the 9 TARs that weren't withdrawn, 7 related to drug offences and the other 2 to robbery and cybercrime. The relatively restrained use of the powers introduced by the Assistance and Access Act, including the fact that no compulsive notices were issued over the last reporting period (with relevant service providers cooperating with TARs on a voluntary basis), may perhaps ease privacy-related concerns. However, it also potentially raises questions about the need for this type of law – are far-reaching powers that are rarely, if ever, used really justifiable when there is a significant potential trade-off in terms of the security and privacy of online services? Of course, there are obvious counter-arguments to the effect that agencies must be armed with the right powers for when the need arises, and it is natural and appropriate to expect that the most significant powers would be only deployed when really necessary (with the fact they haven't been needed over the last year not being a reliable indication that they will never be needed). This ongoing tensions imply illustrates again the challenges that we as a society face in striking the right balance between online freedoms and online surveillance.

5 Key privacy determinations

It has been a busy year for the OAIC dealing with a variety of privacy-related disputes. As we have in previous years, we have included summaries of some of the most significant and broadly applicable determinations made by the Commissioner here. The Commissioner's ongoing civil penalty proceedings against Facebook, relating to the historical Cambridge Analytica incident, sets an interesting backdrop for these determinations (albeit that those proceedings are still at a relatively preliminary stage and are unlikely to be resolved for some time to come) and will continue to draw attention from all observers with an interest in privacy law.

5.1 Commissioner Initiated Investigation into Uber Technologies, Inc. & Uber B.V. [2021] AICmr 34

Made in June 2021, this determination is a timely and important exposition on the OAIC's view of the extra-territorial operation of the Privacy Act. It's also a cautionary reminder to global corporations of the scope of their potential exposure to Australian privacy laws, even if there is limited or no physical activity or presence in Australia.

Background

In this determination, the Commissioner found that the US-based Uber Technologies, Inc. (Uber), and its Dutch-based subsidiary Uber B.V. (UBV), each failed to appropriately protect the personal data of Australian customers and drivers, which was accessed in a cyber-attack in October and November 2016 (Uber Data Breach).

Specifically, the Commissioner found that each company:

(a) had an 'Australian link' and therefore was within the jurisdiction of the Privacy Act; and

(b) breached the Privacy Act as each failed to comply with their obligations under APPs 1.2 (in relation to practices and procedures), and 11.1 and 11.2 (in relation to security).

Extra-territorial application of the Privacy Act

Uber and UBV are respectively incorporated in the US and the Netherlands. Accordingly, the first substantive issue for the Commissioner was whether each company had an 'Australian link' such that they would be bound by the Privacy Act in relation to activities carried on outside Australia under the relevant jurisdictional 'hook' in section 5B of the Privacy Act.

In that respect, the Commissioner was required to be satisfied that, at the time of the Uber Data Breach, both UBV and Uber each: (a) carried on business in Australia; and (b) collected or held the relevant personal information in question in Australia.

In respect of UBV, the Commissioner had no difficulty establishing, and it was not in dispute, that UBV carried on business in Australia and collected personal information from Australian users. At the time of the Uber Data Breach, UBV was, for regions outside of the US, both the data controller and licensor of the Uber app, and entered into direct contractual arrangements with both Australian riders and drivers. The Commissioner held that, despite being incorporated in the Netherlands and having no physical presence in Australia, UBV clearly had an 'Australian link'.

The equivalent analysis for Uber was less straight-forward, and Uber strongly disputed that it was subject to the jurisdiction of the Privacy Act. The Commissioner accepted that Uber did not have a physical presence in Australia, was headquartered in the US and did not have a direct contractual relationship with Australian riders or drivers at the time of the Uber Data Breach. Notwithstanding this, the Commissioner considered that Uber carried on business in Australia because it:

- installed and managed authentication, security and localisation cookies and similar technologies on Australian users' devices;
- rolled out new solutions (such as services, products, safety features, and troubleshooting) developed in the US on an international basis, including to Australia; and
- used centralised and global tools to enable UBV to carry out ad campaigns for Australian users.

The Commissioner relevantly held that it was not determinative that some or all of these acts may have been instituted or controlled remotely, or that they were done on behalf of UBV rather than on Uber's own behalf. Rather, touching upon requirements developed in previous case law on carrying on business in Australia, the Commissioner held that these activities demonstrated that Uber was engaging in activity in Australia, which was in the nature of a commercial enterprise, and which had a repetitive and permanent character.

The Commissioner also found that Uber collected personal information from Australian users in Australia. The Commissioner held that, while UBV controlled the direct relationship with those users, in practice, data from those users was transferred straight to servers controlled and owned by Uber in the US. As such, the Commissioner was satisfied that Uber collected this information at the same time as it was collected by UBV – in other words,

there was a simultaneous act of collection by the two entities. Combined with the Commissioner's conclusion that Uber was carrying on business in Australia, this meant that Uber had an 'Australian link' and was, therefore, bound to comply with the Australian Privacy Act in relation to its handling of information about Australian users.

Breaches of the APPs

The Commissioner found that both Uber companies breached the Privacy Act for failure to comply with their obligations under the APPs. In particular, the Commissioner found that both companies interfered with the privacy of the affected Australian users by failing to take reasonable steps in the circumstances to:

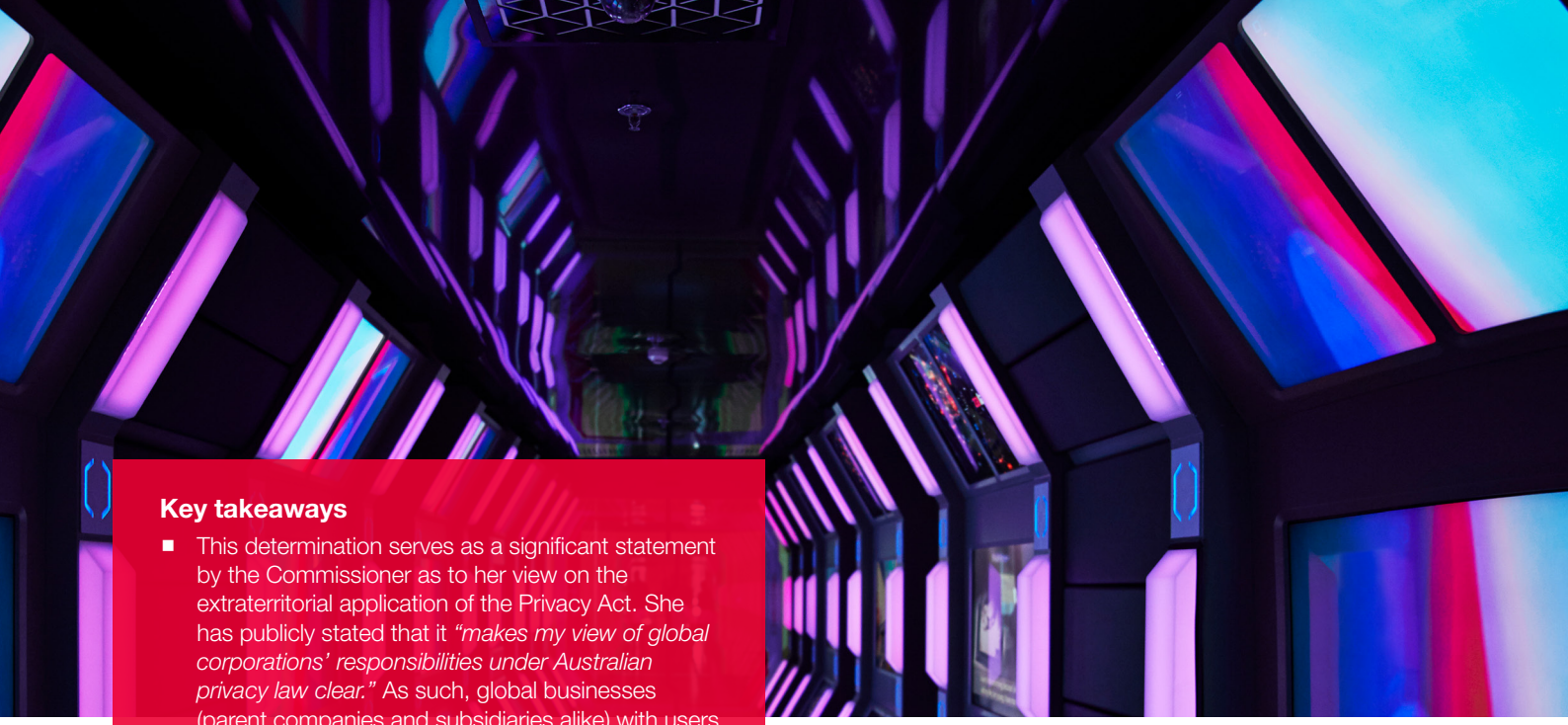
- protect their personal information from unauthorised access, in breach of APP 11.1; and
- destroy or de-identify their personal information once it was no longer required, in breach of APP 11.2.

Further, the Commissioner held that both UBV and Uber failed to take reasonable steps in the circumstances to implement practices, procedures and systems relating to the Uber companies' functions and activities, to ensure compliance with the APPs, in breach of APP 1.2.

As a result, the Commissioner ordered the companies to prepare, implement and maintain a data retention and destruction policy, information security program, and incident response plan to ensure compliance with APPs 11.1, 11.2 and 1.2 respectively and to appoint an independent expert to review, report and provide recommendations on these policies and programs and their implementation, and submit the reports to the OAIC.

The Commissioner noted that while both UBV and Uber have been subject to regulatory action in other jurisdictions, it was still appropriate and proportionate to take further action in Australia. In reaching this conclusion, the Commissioner indicated there was a public interest in making a declaration on these matters, noting that there were:

> *"complex issues that are specific to the Australian legislative context, including the application of the extraterritorial jurisdiction provisions in the Privacy Act to companies that outsource the handling of Australians' personal information to companies within their corporate group through 'data processing' agreements or similar arrangements.*



Key takeaways

- This determination serves as a significant statement by the Commissioner as to her view on the extraterritorial application of the Privacy Act. She has publicly stated that it *"makes my view of global corporations' responsibilities under Australian privacy law clear."* As such, global businesses (parent companies and subsidiaries alike) with users in Australia should be on notice that they may be required to comply with Australian privacy laws.
- In the Commissioner's view it is clear that having no physical presence in Australia and no direct contractual relationship with Australians is no barrier to international entities from falling within the jurisdiction of the Privacy Act if they otherwise have sufficient connection with business activities that take place here.
- An entity cannot outsource compliance obligations under the Privacy Act simply by outsourcing relevant data processing activities to a related entity, or indeed to any other entity. The outsourcing entity will need to maintain an appropriate level of oversight and involvement to ensure that there is no privacy breach by the service provider for which the outsourcing entity may ultimately share some responsibility.
- Global businesses may still face regulatory action in Australia, even if they have been subject to similar actions in other jurisdictions. Uber has indicated that it will not appeal the Commissioner's determination, so it remains to be seen whether the courts will agree with the Commissioner's views.

5.2 'WP' and Secretary to the Department of Home Affairs [2021] AICmr 2

In this determination made in January 2021, the Commissioner ordered the Australian Department of Home Affairs (Department) to pay compensation to over 1,297 asylum seekers for inadvertently publishing their personal information online in 2014. This was the first award for non-economic loss by the Commissioner in response to a representative action. The awards of compensation are expected to range between $500 and more than $20,000 for each class member who provides a submission or evidence that substantiates non-economic loss. This will be assessed on a 'case-by-case' basis.

Background

The underlying compliance breach occurred when the Department accidentally made public a database containing the personal information of asylum seekers held on Christmas Island and in a mainland detention facility. Information, including full names, nationalities, dates of birth, gender and boat arrivals, was accessible for eight days on the Department's website and a further seven days on Archive.com before it was removed.

The Department had already separately been found by the Commissioner to have breached the Privacy Act pursuant to an investigation commenced on the Commissioner's own motion, and the breaches had been acknowledged by the Department. The breaches that the Department was found to have committed related to unauthorised disclosure of the relevant information and failure to keep the information secure – broadly equivalent to what is now APP 6 and APP 11 (although the determination relates to an earlier version of the Privacy Act).

First class award of non-economic loss

The Commissioner determined that those asylum seekers that made submissions (1,297 out of a total of 9,250 affected) should be paid compensation for non-economic loss or damage arising from the data breach. The determination provides for a range of compensation for non-economic loss from $500 to more than $20,000 based on the level of harm suffered by each relevant individual, suggesting total compensation payable of between $650,000 and $25.94 million for the Department (and potentially more if the claimants are also able to establish they suffered economic loss). This was the first representative action where non-economic loss has been awarded.

Consistent with previous determinations made in response to individual complaints, the Commissioner has expressly adopted the AAT decision of *Rummery and Federal Privacy Commissioner and Department of Justice and Community Safety* [2004] AATA 1221 as establishing the following principles:

- where a complaint is substantiated and loss or damage is suffered, the legislation contemplates some form of redress in the ordinary course;
- awards should be restrained but not minimal;
- in measuring compensation the principles of damages applied in tort law will assist although the ultimate guide is the words of the statute;
- in an appropriate case, aggravated damages may be awarded; and
- compensation should be assessed having regard to the complainant's reaction and not to the perceived reaction of the majority of the community or of a reasonable person in similar circumstances.

In this particular case, the determination of the actual amounts of compensation that should be awarded has been prolonged for various procedural reasons. Each class member was provided with an opportunity to make submissions in relation to the harm alleged to have been suffered. For various reasons, the deadline for these submission was extended on multiple occasions. In any event, after considering the submissions and evidence, the Commissioner determined that the loss or damage that class members had suffered fell into five categories, ranging from category 1 "general anxiousness, trepidation, concern or embarrassment, resulting from the data breach" (for which compensation of $500 to $4,000 was payable) through to category 5 "extreme loss or damage resulting from the data breach" (for which compensation of greater than $20,000 was payable). Other class members, not having substantiated any loss or damage, would not be entitled to any compensation. Having identified the five categories of loss, the Commissioner determined that each claim should be assessed on a "case by case basis". This process is expected to be conducted over the 12 months from the determination. The Commissioner observed:

> *…an evidentiary basis is required to make a declaration s 52(1)(b)(iii) that a complainant is entitled to compensation. This is particularly the case in respect of non-economic loss, which is of an inherently personal nature and is not sufficiently common in this case to lend itself to a declaration that all class members are entitled to the same kind or amounts of compensation without some evidence from those class members as to their loss.*

Key takeaways

- The process outlined for determining compensation in response to a representative privacy complaint can be highly resource intensive. The process may be lengthy, potentially taking multiple years, and may require detailed evidence in relation to the particular loss suffered by individual class members. Notably, the process may be different for each case. The categories of loss identified in this determination were specific to the relevant factual matrix of this case, and while they represent a useful reference are not intended to be used as a formula for determining compensation for non-economic loss in other matters.
- The Commissioner may take a graduated view on matters relating to compensation in a representative claim, acknowledging that not all affected individuals will suffer harm of the same nature or degree (with some individuals potentially suffering no compensable non-economic loss at all). In other words, the Commissioner does not appear to assume that a breach of the Privacy Act will necessarily lead to non-economic harm, or to a consistent level of distress where such harm does arise. This approach more closely resembles traditional approaches to damages for torts and may be contrasted with approaches taken recently in other jurisdictions.

5.3 Flight Centre Travel Group (Privacy) [2020] AICmr 57 (25 November 2020)

This determination relates to an accidental disclosure by Flight Centre of customer information, including in some cases credit card and passport details, to attendees of a 'design jam' event. Although Flight Centre had intended to anonymise the data, personal details were found in free text fields that remained in the dataset.

Breaches

The Commissioner found that Flight Centre had breached APP 6.1 by disclosing customer information other than for the purpose for which it was obtained and without consent or other legal basis to justify the disclosure. In addition, Flight Centre had breached APP 11.1 by failing to take reasonable steps to protect the information from unauthorised disclosure and APP 1.2 by failing to take reasonable steps to implement procedures to ensure compliance with APPs. While Flight Centre had manually reviewed a subset of data prior to circulation, this was clearly not sufficient to protect against the unauthorised disclosure. There were other steps that Flight Centre could have taken to reduce the risk, including improved staff training and compliance checks to ensure that security policies were being properly operationalised and using technical controls to detect and prevent inclusion of inappropriate information in free text fields.

Privacy policies are not a good way to establish consent

Perhaps the most interesting aspects of this determination relate to the issue of consent. The Flight Centre privacy policy indicated that customer information was collected in order to provide the customer with various services. The policy also indicated that information may be used for other purposes, such as for "developing, improving and marketing our products and services" and that by providing information to Flight Centre customers effectively agreed that the policy would apply to Flight Centre's handling of that information. However, the Commissioner was adamant that this did not support an argument that the customers had consented to the disclosure of their information for the purposes of the design jam. In particular, the Commissioner was not satisfied that consent could be

implied simply from the act of making information available to Flight Centre and that, even if it could, any consent obtained through the privacy policy was not sufficiently specific (as it bundled together a wide range of different uses and disclosures) or voluntary (as customers did not have a genuine opportunity to distinguish between the different uses and disclosures contemplated in the policy).

More generally, the Commissioner expressed a clear view that privacy policies are not an appropriate mechanism for establishing privacy consents:

> *A privacy policy is a transparency mechanism that, in accordance with APP 1.4, must include information about an entity's personal information handling practices including how an individual may complain and how any complaints will be dealt with. It is not generally a way of providing notice and obtaining consent. If the respondent had intended to disclose credit card details and passport information to third parties for this purpose, and I accept it did not intend to in respect of the Event, given the sensitive nature of this kind of information, I would expect a request for consent to clearly identify the kind of information to be disclosed, the recipient entities, the purpose of the disclosure, and for consent to be sought separately, not as part of a Privacy Policy.*

Key takeaways

- While the Privacy Act leaves the concept of consent relatively open (allowing for both express and implied consent), the Commissioner is clear in her views that privacy consents cannot easily be inferred and that to be valid a consent must amongst other things be properly informed, voluntary, current and specific. It is likely that these or similar requirements will be confirmed as part of the Privacy Act review that is currently in progress.
- While many organisations may ask that customers "agree" to comply with their privacy policy – whether in a customer contract or otherwise – that will not necessarily be effective to establish that the customer has validly consented to the matters covered in the policy. Given the views expressed by the Commissioner in this determination, it is highly unlikely that she will consider that any consent purportedly established in this way to be insufficiently specific or voluntary.

5.4 Other determinations of note

- In *'WG' and AustralianSuper Pty Ltd* [2020] AICmr 64, the Commissioner sets out her view in some detail regarding the APPs on disclosure. The facts are complex, and relate to the disclosure of information to a complainant's prior law firm after changing to another law firm in an insurance dispute. However, the determination is chiefly of interest due to the Commissioner's explanation of how to discern what the 'primary purpose' of collection is for the purposes of applying the rules on use and disclosure under APP 6. The Commissioner reiterated her view that the primary purpose of collection "*should be determined, where there is ambiguity, narrowly rather than expansively*" but that even so it may still include disclosure to third parties. The Commissioner commented that "*characterising the primary purpose is about discovering the reason for the collection of personal information and then determining whether the subsequent use or disclosure of that personal information departed from the primary purpose*". In this case, the primary purpose for which the information was collected was to process an insurance claim. That purpose encompassed various ancillary matters, including checking whether the claimant has the relevant insurance cover, recording the claim, notifying the insurer where relevant and arranging for the claim to be sent to a third party administrator that was responsible for providing assessment and investigation services. Provided the use and disclosure remained within the scope of the primary purpose, including these ancillary matters, it was not necessary to consider whether consent or another exception under APP 6 may have applied.
- *'WC' and Chief of Defence Force* [2020] AICmr 60 and *'VQ' and Secretary to the Department of Home Affairs* [2020] AICmr 49 serve as two timely reminders that the OAIC has jurisdiction over several provisions in the *Crimes Act* 1914 (Cth) relating to conducting background checks and the disclosure of spent convictions. Criminal background checks are a common feature of hiring and resourcing procedures for many organisations, but there are specific provisions on when a conviction is 'spent' and restrictions on use of information about spent convictions. Section 85ZZA of the Crimes Act allows an individual to complain to the Privacy Commissioner about an act or practice of another person, or of a Commonwealth authority or State authority that may be a breach of these provisions. In the WC determination, this led to an award of $6,000 for non-economic loss and $4,850 for reasonably incurred expenses, following disclosure of spent conviction information which was used to terminate the complainant's employment. There have been several other determinations in the past year relating to these provisions, indicating active enforcement by the OAIC in this area.

6 News bites from the OAIC

- **Commissioner reappointed for another term**

  Angelene Falk has been reappointed to her dual role as Australian Information Commissioner and Privacy Commissioner for a further 3 years (until August 2024). In a statement on her reappointment, the Commissioner said:

  > *This is a pivotal time for both privacy and freedom of information. Over the next 3 years we will uphold and advance these rights to enable citizens and businesses to safeguard personal information and harness its benefits, for individuals and the economy, while we encourage an open-by-design approach to information access across government.*

  With the current Commissioner now locked in for another term – one that may prove very eventful, with the Privacy Act review likely to be completed and implemented within this timeframe – we expect the policy positions and strategic approach of the OAIC to largely remain unchanged in the near term.

- **Reporting on complaint outcomes**

  The OAIC has started publishing a record of anonymised complaint outcomes, dating from March 2020 onwards.

The OAIC has previously published links to determinations, enforcement outcomes and investigation reports on its website. However, from this year, the OAIC will also publish information on broader complaint outcomes. The OAIC website notes:

> *Resolving a complaint through negotiation and conciliation can result in a positive and innovative outcome, and parties demonstrate a high level of satisfaction with the outcome. Some of the main remedies achieved include the amendment of a record, access provided, an apology, and/or compensation. This page features a selection of de-identified complaints to demonstrate the outcomes achieved with the assistance of the OAIC and to provide guidance to* parties regarding potential outcomes.

This will provide an interesting insight into how lower-level privacy complaints are typically resolved and the role that the OAIC plays in facilitating these outcomes.

- **Ongoing COVID-19 challenges**

  The COVID-19 pandemic has presented many different challenges across all areas, with privacy law being no exception. In particular, from a privacy perspective, there have been difficult issues about how businesses can keep their workers safe while still at the same time respecting their privacy. On top of all the other difficulties they face, the lack of clarity in this area (despite some well-meaning guidance from the OAIC) has been the cause of some frustration. In a welcome development, the Government recently announced the release of further guidance to the effect that employers can ask workers to disclose their vaccination status. Of course, this doesn't mean that employers can require their workers to be vaccinated, but by being able to gather information about whether or not particular workers have been vaccinated, employers should be able to better protect customers and other workers against infection risk (e.g. by reallocating unvaccinated workers to duties that do not involve direct interaction with other people). Further guidance on vaccination in the workplace is available from the Fair Work Ombudsman here. The OAIC has previously released a range of other COVID-19 advice and guidance, which is available here.

- **The Online Safety Act and cooperation with the eSafety Commissioner**

  The new *Online Safety Act 2021* (Cth) was passed at the end of July 2021, after a consultation period earlier in the year which some commentators criticised as rushed given the small number of amendments made afterwards. The Act aims to improve and promote online safety for Australian users, including by consolidating and upgrading a range of existing laws dealing with harmful online behaviour (e.g. online bullying and sharing of non-consensual intimate images). A number of features of the Act have potential privacy implications, including in relation to new powers for the eSafety Commissioner to require production of end-user identity information and contact details. The OAIC made a brief submission as part of the consultation process, largely to advocate for closer consultation and cooperation between the OAIC and the eSafety Commissioner, including in relation to information sharing and the development of industry codes of practice that may intersect with privacy and data protection issues. This is consistent with the OAIC's recent practice of close collaboration with other regulators, such as the ACMA and the ACCC, in order to ensure there is a consistent approach taken to regulation of online activities.

7 Privacy reforms multiply across APAC

Australia is far from the only country considering major privacy law reforms. Many jurisdictions across the APAC region are in the process of introducing new privacy laws, or revising existing privacy laws, adding to the regulatory complexity already faced by many online and other multinational businesses.

To take just a few examples:

- Across the Tasman, New Zealand's new Privacy Act took effect on 1 December 2020, bringing with it a host of updates. The new Act closely follows the introduction of New Zealand's mandatory data breach notification scheme, and the accompanying regulations contain further detail on the practical operation of that scheme.
- India has taken significant steps towards a relatively radical overhaul of its privacy laws, inspired by the GDPR, in the form of its proposed Personal Data Protection Bill. The Bill would see the introduction of new compliance requirements for a wide range of personal data, the establishment of a central data protection regulator, the implementation of new data localisation requirements for some forms of 'critical' sensitive data, and, of course, heavy penalties for noncompliance.
- Singapore has implemented major changes to its Personal Data Protection Act as part of a general 'uplift'. Changes taking effect in February 2021 include a new mandatory data breach notification scheme, new criminal offences for data misuse and some data harvesting practices, and a new private right of action for privacy breaches.
- Vietnam has released a draft Decree on Personal Data Protection for consultation, with a target date for finalisation by the end of 2021. The comprehensive draft has a number of familiar features – such as a distinction between regulatory obligations of data controllers and data processors, a narrow consent regime, and turnover-based penalties – as well as some more unique aspects, such as permit requirements for processing sensitive data and for cross-border transfers.
- China has adopted a new Data Security Law, which will take effect in September 2021. The new law will be broadly applicable to all parties doing business in or with China that engage in processing of all types of data (though with different rules applying to different categories of data, with stricter management and protection requirements applying to categories that are considered to be more sensitive). The Data Security Law will work in tandem with the existing Cybersecurity Law, which applies to critical information infrastructure operators. Both laws will impose different levels of data localisation requirements, which will need to be considered by international businesses that may need to transfer information to or from their Chinese operations.

These changes are only the tip of the iceberg for privacy in our region. Most interestingly, many of the developments we are seeing impose new restrictions on the flow of data between jurisdictions. The potential for disharmony between national privacy laws and other barriers to the free flow of data – as has been seen with the issues that have beset the Privacy Shield regime under the GDPR and the potential threat that poses to data sharing across the Atlantic – will likely continue to present significant challenges for multinational businesses. ■

We've got you covered
KWM National Team

Kirsten Bowe
Partner, Brisbane
Corporate M&A
T +61 7 3244 8206
M +61 409 460 861
kirsten.bowe@au.kwm.com

Bryony Evans
Partner, Sydney
Tech and IP
T +61 2 9296 2565
M+61 428 610 023
bryony.evans@au.kwm.com

Annabel Griffin
Partner, Canberra
Corporate M&A
T +61 2 6217 6075
M+61 408 847 519
annabel.griffin@au.kwm.com

Patrick Gunning
Partner, Sydney
Tech and IP
T +61 2 9296 2170
M +61 418 297 018
patrick.gunning@au.kwm.com

Cheng Lim
Partner, Melbourne
Tech and IP
T +61 3 9643 4193
M +61 419 357 172
cheng.lim@au.kwm.com

Michael Swinson
Partner, Melbourne
TMET, IT & Data
T +61 3 9643 4266
M +61 488 040 000
michael.swinson@au.kwm.com

Cal Samson (Editor)
Solicitor, Melbourne
T +61 3 9643 4166
M +61 437 652 995
cal.samson@au.kwm.com

Clea Dunham
Solicitor, Brisbane
T +61 7 3244 8112
M +61 436 360 536
clea.denham@au.kwm.com

Luke Hawthorne
Senior Associate, Sydney
T +61 2 9296 2114
M +61 437 515 203
Luke.Hawthorne@au.kwm.com

Oceane Pearse
Law Graduate, Brisbane
T +61 7 3244 8066
M +61 438 913 432
oceane.pearse@au.kwm.com

Special thanks to Cal Samson for his role as editor.

www.kwm.com

Asia Pacific | Europe | North America | Middle East

King & Wood Mallesons refers to the network of firms which are members of the King & Wood Mallesons network. See kwm.com for more information.