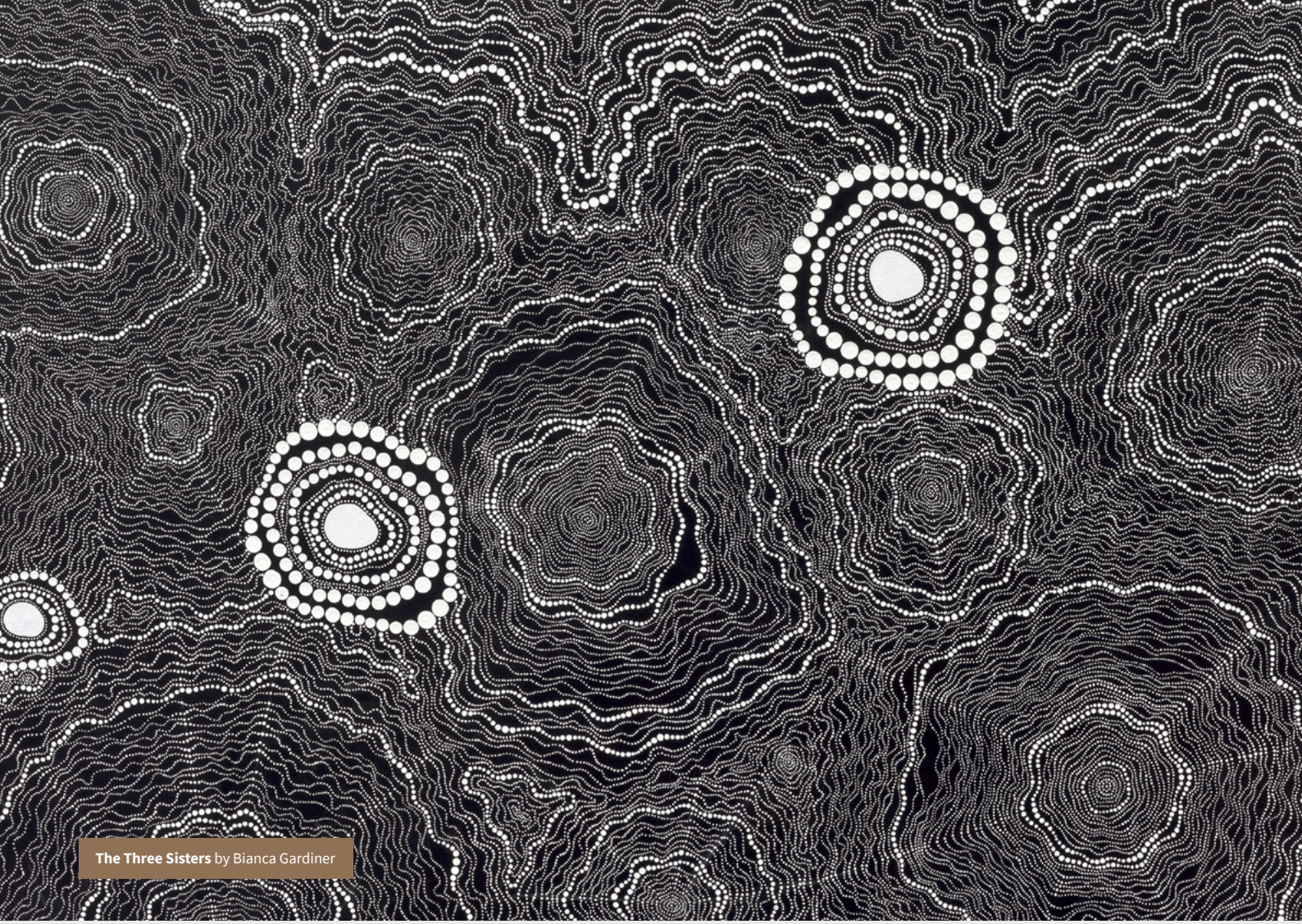


The Three Sisters by Bianca Gardiner

PRIVACY ANNUAL UPDATE 2022

OCTOBER 2022

KING&WOOD MALLESONS
金杜律师事务所

CONTENTS

KEY TAKEAWAYS

Progress has been slow on major Australian privacy law reforms originally initiated more than 2 years ago.

Further direction from the Government is expected before the end of the year and the reform process may then gather pace.

The Office of the Australian Information Commissioner is focussed on use of facial recognition and other 'high privacy risk' technologies.

We strongly recommend organisations conduct privacy impact assessments before launching any new initiatives which make use of such technologies.

Our global colleagues agree international data transfers are an increasingly problematic area for multinational organisations.

With new restrictions imposing costs on business and creating uncertainty. From an Australian perspective at least, it is hoped that future law reforms will provide greater clarity in this area.

INTRODUCTION

In the words of former United States Supreme Court Justice William Douglas, the right to be let alone is the beginning of all freedom. While that may be overstating it for some, the privacy enthusiasts amongst us would no doubt heartily agree with the sentiment. Certainly with the ever-quickening pace of technological change, it is as vital a time as ever to look at the current state of privacy law and prepare for its next evolution.

As we reflect on developments in this area of law over the last year, top of the list for potential impact is, of course, the **ongoing review of the Privacy Act**. It remains to be seen how high it sits on the new Albanese government's agenda, but in this update we look at the current status of the review and discuss some key highlights from submissions made so far in response to the most recent Discussion Paper.

We also look at several **significant privacy-related decisions** from the past year – both in Australia and overseas – which shed useful light on some important and thorny issues. The ***CFMMEU v BHP* decision** reinforces the focus on privacy as an employment issue (and provides an interesting contrast to the *Lee v Superior Wood* decision we covered in our 2019 update. The ***7-Eleven and Clearview AI* determinations**, both of which followed Commissioner-initiated investigations, demonstrate the Commissioner's keen interest in facial recognition technology and its deployment in new contexts. This looks set to be a continued area of focus, given the Commissioner's recently commenced investigations into the use of facial recognition cameras by a number of leading Australian retailers. Meanwhile, for class action litigators the landmark decision by the UK Supreme Court in the ***Lloyd v Google* case** is essential reading.

Finally, we consider the global headache that **rules on cross-border data transfer** have become, with perspectives from Europe and China about how new compliance requirements are creating ongoing challenges for multinational businesses looking to share data across jurisdictions.

We hope you enjoy this year's privacy 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 – you can find our details at the end of this publication.

A NOTE

This publication was prepared before news of the Optus data breach broke. It is interesting (and extremely pertinent) to note how quickly a cyber security incident has become a story about privacy in the digital age, with the Government facing scrutiny alongside Optus regarding the adequacy of privacy protections. It is clear this will have an impact on the wider privacy act reform process and its underlying issues. We hope this report is a timely explanation of what needs addressing.

SWEEPING REFORMS (AND CURLY QUESTIONS)

The most significant development of the year in privacy in Australia was the (somewhat slow-moving) consultation on the Privacy Act Review Discussion Paper, which was released in October 2021. In last year's update we said we were, figuratively speaking, standing at base camp ahead of an Everest of privacy law reform. Continuing that analogy, this year we set out for the climb! Though we are yet to make it far up the steep slope that lies ahead. The many and varied views from hundreds of submissions in response to the Discussion Paper are currently being considered by the Attorney-General's Department. While there has been an understandable break in activity around the change in government in May, we don't think it will be too long until we see some more concrete reform proposals released for public consideration. In the meantime, this relatively quiet moment in the course of the review presents a useful opportunity to consider some key questions about the challenges that lie ahead.

CURLY QUESTION 1

Will the change in government have an impact?

This is the first and largest question looming in many people's minds. After all, the review is being conducted by the Attorney-General's Department, and there is a brand new Attorney-General.

On this front at least, we have a relatively clear answer: no major changes expected. Incoming Attorney-General Mark Dreyfus publicly stated at the end of June that he intends to move on the reforms during the first term of government, and that "sweeping reforms are needed to our Privacy Act" in order to keep the legislation current for the digital age.

He indicated that the final report on the proposals for reform was likely to be made public "in coming months" and that there would be a period for debate and discussion on the proposals to follow. It is in the final report that any differences in approach might begin to emerge, although given the broad bipartisan support for the reform process before the election it seems unlikely there will be any dramatic change in direction.

CURLY QUESTION 2

Whose view on individual control will rule the day?

Throughout the reform process there has been debate about the level of control that individuals should have over the collection and use of their personal information. Much of the initial focus, stretching back to the ACCC's recommendations from the Digital Platforms Inquiry, was on the role that consent should play. However, in light of concerns about consent-fatigue and the risk of over-burdening consumers, the discussion has shifted towards other types of controls, such as controls on the nature and quality of privacy notices and specific legislated protections or rights. For example, the Discussion Paper proposed the introduction of a new overarching requirement that all collection, use and disclosure of personal information be 'reasonable and fair' as well as a number of new data subject rights, including rights to object to the use and disclosure of personal information and the right to request deletion of personal information. While consent is still an important issue, and there has still been a focus on the quality of consents (such as ensuring they are appropriately informed and voluntary and given on an opt-in rather than opt-out basis), there seems to be a growing acceptance that a regulatory regime centred entirely around consent would not be workable.

While most would agree that privacy regulation must be about more than consent, there are still significantly differing views about a number of the controls proposed in the Discussion Paper. For example, while many submissions in response to the Discussion Paper were supportive of the proposal for a right to object, with the ACCC strongly in favour, in many cases the level of support was carefully qualified. For example, the OAIC suggested in its submission that there should be appropriate exceptions to the right, including when personal information is necessary to provide a requested service or product. Notably, the OAIC specified that such an exception *'should not permit the ongoing use or disclosure of personal information if that information is only required to monetise the particular service or the APP entity's business model'* – a distinction that appears squarely targeted at undercutting the fundamentals of businesses supported by targeted advertising. Unsurprisingly, other industry submissions emphasised the importance of ensuring that ad-supported business models are not unduly impeded by a new right to object – after all, on one view the ultimate right to object is for a consumer simply not to use ad-supported services if they are not comfortable with the collection and use of their information for advertising purposes. Other submissions opposed the proposed right to object entirely, suggesting it is *'far too broadly stated to be considered reasonable or even practical'.* All in all – and this is just one example – there remains a significant divergence of views as to how to give individuals an appropriate level of control without unduly impeding legitimate business activities. Given the opposing views, it seems unlikely that any final reforms in this area will be to everyone's liking.

CURLY QUESTION 3

Is Australia finally getting a statutory privacy cause of action?

The question of whether individuals should be able to take direct action in the courts for invasions or breaches of privacy has long been a topic of hot debate, with the issue having been considered on several occasions over the years. After all, as the legal realists might have it, isn't the enforcement (and the remedy) what the law is really all about?

Despite the attention it has received over the years, submissions in response to the Discussion Paper illustrate that there is still a strong and significant divergence in views in this area. Perhaps understandably, given the broader context of the ongoing growth in class actions and the way privacy is being viewed increasingly through a consumer protection lens, industry submissions were generally strongly opposed to either a direct right of action under the Privacy Act or the introduction of a new statutory tort. Instead, these submissions pointed to the relative success of the existing OAIC conciliation process in resolving privacy related complaints and queried whether there was a compelling case for change.

Some submissions raised concerns about the risk of frivolous actions, and the associated burden on court resources. Others were strongly in favour, on the basis that, without a direct right of action, individuals will never be properly empowered to look after their privacy interests, and noting that such rights had found support in past reviews. The OAIC itself took a nuanced view, proposing the introduction of both a statutory tort and a direct right of action under the Privacy Act but with the direct right of action being subject to a complaint first being made to, and assessed for conciliation by, the OAIC or a recognised dispute resolution scheme (such as an industry ombudsman). Under the OAIC's approach, complainants would be able to initiate action in a federal court where the matter is deemed unsuitable for conciliation, conciliation has failed, or the complainant chooses not to pursue conciliation. The complainant would also need to seek leave of the court to make the application. The OAIC would also have the ability to appear as amicus curiae to provide expert evidence at the request of the court. These recommendations reflect the need to balance the desire to empower individuals to take control of their privacy interests against the risk of opening the litigation floodgates.

Amongst the debate, little attention appears to have been paid to how direct action claims for breaches of privacy could play out, including in terms of loss and damage (though see our item below on *Google v Lloyd* which illustrates how critical those issues can be in a privacy claim). Nonetheless, this is sure to be an area to watch as the new government's reform agenda takes shape.

THE UNCERTAIN FUTURE OF THE ONLINE PRIVACY BILL

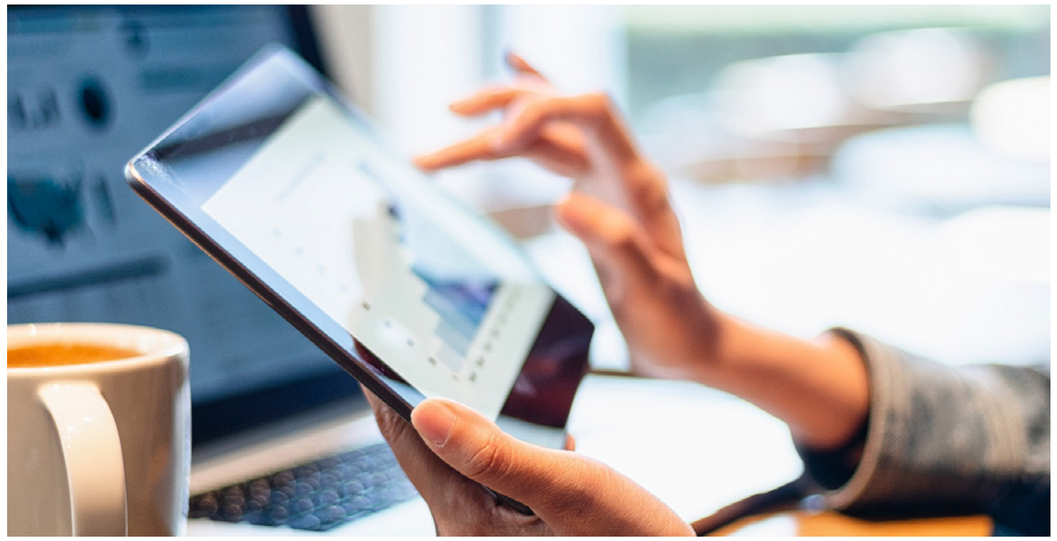
Released by the Attorney-General's Department on the same day as the Privacy Act Review Discussion Paper, the exposure draft of the Privacy Legislation Amendment (*Enhancing Online Privacy and Other Measures*) *Bill 2021* (or the Online Privacy Bill for short) was the other major development in privacy-related law reform this year, but its future is far less certain.

Following consultation in late 2021, the exposure draft of the Online Privacy Bill was not formally introduced in the previous Parliament, and it is unclear how it will develop from here. As described in our alert at the time the draft Online Privacy Bill has three main features:

It establishes a framework for the development of a binding industry code of practice that would apply to social media services, data brokerage services and other large online platforms. The purpose of the code would be to clarify how the existing Australian Privacy Principles (**APPs**) would apply to such services and also impose some additional compliance obligations on those organisations on top of the APPs.

It strengthens the enforcement options available under the Privacy Act, including to align maximum civil penalties available under the Privacy Act with those under the Australian Consumer Law (being the greater of: AU$10 million; 3x the value of the benefit obtained from the relevant contravention; and, if the value cannot be determined, 10% of domestic annual turnover).

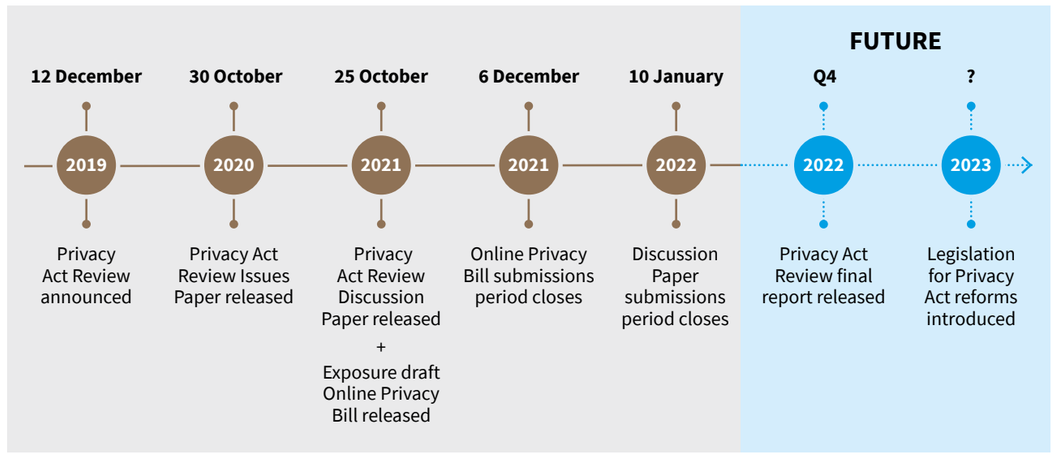
It amends the extraterritorial application of the Privacy Act to foreign organisations by removing the last limb of the existing "Australian link" test. If implemented, that change could significantly expand the current reach of the Privacy Act.



Many submissions made in response to the Online Privacy Bill objected to the simultaneous running of two major reform processes on overlapping issues. The Law Council of Australia described the proposed fragmentation in the reform process as "regrettable". Others were less diplomatic. Many submissions were concerned about the potential for misalignment between the industry code contemplated by the Online Privacy Bill and future cross-economy reforms. This could cause confusion for consumers, who may not understand when different privacy rules and standards would apply, as well as businesses with both online and 'offline' operations. Overall, the broad sentiment was that privacy reform should be 'done once and done properly' and that a compelling case had not been made to push the Online Privacy Bill through ahead of the broader Privacy Act review.

It's too early to tell whether the Online Privacy Bill will be revived in 2022, either in its original form or in some different form. There is little doubt that some aspects of the Online Privacy Bill, such as the proposed increase to the maximum fines available under the Privacy Act, will continue to feature in future reform proposals. There will also continue to be pressure for lawmakers to ensure that social media and other online service providers that handle large amounts of consumer data are subject to stringent privacy compliance requirements. However, if we had to make a bet, given the level of push-back that the Online Privacy Bill received, we would say it is more likely that such changes will be wrapped up as part of a set of broader changes to the Privacy Act, rather than in a standalone piece of legislation that is to be pushed through ahead of broader reforms.

PRIVACY REFORM TIMELINE



BONUS PRIVACY LAW REFORM

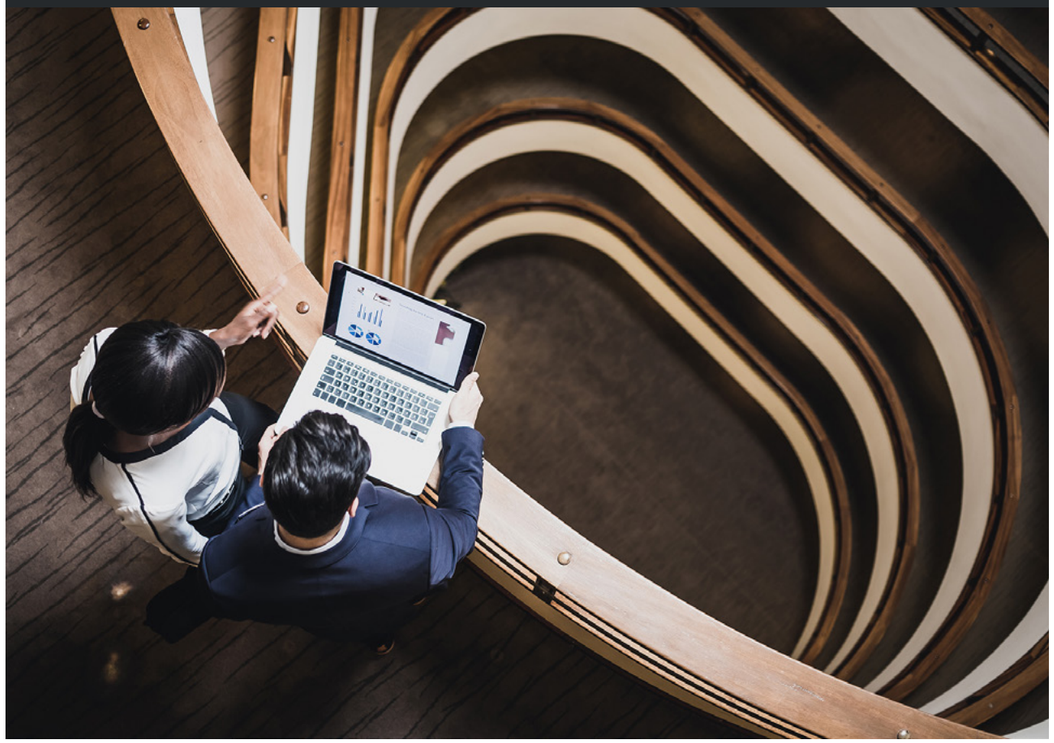
Queensland edition

In addition to the ongoing proposals for change under the federal Privacy Act and Online Privacy Bill, there are also changes on the horizon for Queensland's privacy and right to information laws.

As we covered in our recent alert, the Queensland Government has released a consultation paper on a series of proposed reforms following the *Report on the Review of the Right to Information Act 2009* and *Information Privacy Act 2009*. The Queensland review expressly carves out one of the key federal Privacy Act reforms from its purview – the proposed introduction of a tort for breach of privacy – to avoid any duplication. Likewise, the consultation paper does not cover proposed reforms to Queensland's surveillance laws, which are also under review by the Queensland Law Reform Commission.

The consultation paper addresses topics such as updating the definition of personal information to align with the federal Privacy Act, and adopting a single set of privacy principles (to eliminate the current split between principles which apply to health agencies and other agencies). It also proposes that the current requirements to take 'reasonable steps' to protect personal information be more specifically defined in line with Article 32 of the EU GDPR. Other topics of interest include enhanced powers for the Office of the Information Commissioner and the introduction of a mandatory data breach reporting scheme.

The Queensland Government is currently considering submissions on the consultation paper, after the period for public comment closed in late July.



ADVENTURES IN CONSENT, FACE OFFS WITH THE COMMISSIONER, AND THE FINER POINTS OF LOSS AND DAMAGE

OUR LOOK AT PRIVACY DECISIONS IN THE PAST YEAR

Construction, Forestry, Maritime, Mining and Energy Union & Ors v BHP Coal Pty Ltd T/A BHP Billiton Mitsubishi Alliance / BMA & Ors [2022] FWC 81

When is consent not really consent? That is the question faced by the Fair Work Commission (**FWC**) recently in a union challenge to a requirement for workers to provide evidence of their COVID-19 vaccination status, including as to the type of vaccine they had received, in order to gain access to job sites.

The vaccination status information was clearly sensitive health information, which under APP 3.3 can generally only be collected with consent. The unions argued that any consent purportedly given by workers in this scenario would be invalid, as they faced disciplinary action or termination if they did not consent – in other words the consent was only given under duress. They also took issue with the extent of the information required by BHP, arguing that it was not reasonably necessary for BHP to collect, and suggested that BHP had other less intrusive options for verifying vaccination status, including by using the Queensland Government's QR Check-in App.

In making these arguments, the unions relied upon a previous case, *Lee v Superior Wood Pty Ltd* [2019] FWCFB 2946, in which the FWC held that a consent to provide fingerprint data for the purposes of signing in and out of work was not valid where a worker was threatened with discipline or dismissal if they refused. However, the FWC distinguished the *Lee* decision on a number of bases, including that in *Lee* the employer had failed to comply with privacy compliance requirements in a range of other respects, including by not having appropriate privacy policies and notices in place, and also failed to establish that the collection of the fingerprint information was reasonably necessary rather than simply administratively convenient. The FWC's finding in *Lee* that any consent would have been vitiated by a threat of discipline or dismissal had to be considered in the context of those other failings. By contrast, the FWC found that there was no lack of compliance by BHP in any respect, with BHP having undertaken "extensive and comprehensive" consultation with unions and workers and provided detailed explanations about how the vaccination status information would be collected, stored and protected. Critically, while workers may have felt under economic pressure to consent as they may otherwise lose their job, that was not sufficient to vitiate consent in this context. Deputy President Asbury said that:

I acknowledge that the choice as to whether to comply with the direction or not, may be difficult for persons who hold strong views about the privacy of their sensitive information and that a decision not to provide the information will almost certainly result in the termination of their employment. However, the fact that employees are faced with a difficult choice, does not, in the circumstances, constitute effective lack of choice. Nor does it constitute duress or coercion that vitiates or invalidates the choice.

The FWC also didn't accept the argument that the detail required by BHP was not reasonably necessary. The FWC noted that BHP's objective was to lessen or prevent a serious threat to the health and safety of people at the relevant mine sites, which were matters of critical importance. Information about vaccination types that different workers had received, and the dates on which the vaccines were given, was relevant to managing associated risks. For example, it could inform decision-making if new virus strains were to emerge that were known to respond differently to different types of vaccine (there was perhaps a somewhat speculative aspect to this, but the FWC nonetheless found it a relevant consideration in assessing the necessity of collection). The information required by BHP from its workers was integral to BHP's functions and activities, including in discharging obligations to which it was subject under applicable mine safety legislation.

The FWC considered that suggested alternatives of using the QR Check-in App or other methods of verifying vaccination status at point of site entry were impractical and *"at best unworkable and at worst, chaotic."* This was yet another reason to distinguish the decision in *Lee*, where the evidence suggested there were other practical alternatives for confirming attendance at site and where the consequences of a failure to do so were not that serious, in stark contrast to the catastrophic consequences of a COVID-19 outbreak at one of BHP's sites. In short, while other verification methods, such as the QR Check-in App, may have been reasonable in other settings, they were not suitable for BHP's purposes, with DP Asbury commenting that it was *"neither safe nor reasonable to require that a coal mine operator use an access system for verifying vaccination status that is designed for hospitality and retail establishments."*

Implications for establishing consent

This decision demonstrates the challenges entities currently face in determining whether or not their privacy consent processes are effective. The Privacy Act currently does not set any prescriptive rules as to what is required to establish a valid consent. The OAIC has published guidance to the effect that, in order to be valid, a consent must be adequately informed, voluntary, specific, current and given by someone with appropriate capacity. The voluntariness of the consent was clearly in issue in this case, but the FWC ultimately held that economic pressure is not of itself sufficient to establish a lack of voluntariness – that is, a difficult choice is still a choice. Applying the same logic to other settings, the pressure that a person may face when access to a particular product or service is made conditional on giving a privacy consent (say a consent to profiling for purposes of targeted advertising) may not of itself render the consent involuntary. Provided that they have been adequately informed about what they are consenting to, the person still ultimately has a choice about whether they wish to access the product or service. That may be broadly accepted where there is an obvious connection between the subject matter of the consent and the underlying product or service (such as in the case of an ad-supported service, which can only be offered to consumers for free if the service provider is able to sell targeted ads). However, it will be more controversial where the connection is less clear. It is likely that future updates to the Privacy Act will result in more prescriptive rules around consent, including an express requirement for consents to be voluntarily given. We can only hope that any such changes are accompanied by further guidance as to how to assess the voluntariness of a consent.

KEY TAKEAWAYS

Consent can still be voluntary, even where there is some economic pressure on the individual who must make the choice.

The FWC is increasingly being drawn into the field of privacy, as organisations collect more information about employees in a variety of contexts.

Future reforms may provide an opportunity for further clarity on establishing that an effective consent has been provided for the purposes of the Privacy Act.

Commissioner initiated investigation into 7-Eleven Stores Pty Ltd (Privacy) [2021] AICmr 50 (29 September 2021; Corrigendum dated 12 October 2021)

In this determination, the Australian Information Commissioner found that 7-Eleven interfered with the privacy of its customers by collecting facial images and faceprints through an in-store feedback system. This determination illustrates the strict approach that the Commissioner has taken in relation to the use of facial recognition and other potentially privacy-intrusive technologies.

Background

Between June 2020 and August 2021, 7-Eleven deployed a customer feedback system across its store network, which included a facial recognition feature. The system comprised a tablet device with a built-in camera that took facial images of the customer as they completed a voluntary survey about their in-store experience. The facial images were uploaded to a third party service provider's system almost immediately and subsequently deleted from the in-store tablet. The facial images were later deleted from the service provider's system after 7 days.

The facial images were used to generate algorithmic representations, or 'faceprints', which were compared with other faceprints to exclude survey responses that may not be genuine. The facial images were also used to ascertain a broad understanding of the demographic profile of customers who completed the survey.

The Commissioner found that 7-Eleven breached the Privacy Act by collecting sensitive personal information in circumstances where the collection was not reasonably necessary for its functions and activities, and without valid consent. The Commissioner also determined that 7-Eleven did not take reasonable steps to notify customers about the collection of their information and the purposes for which their information was being collected.

Were the facial images and faceprints "personal information"?

7-Eleven contended that the facial images and faceprints were not personal information for the purposes of the Privacy Act because, among other things:

- they were not used to identify, monitor or track any individual; and
- none of the information collected by the facial recognition tool was associated or matched with any personal information or customer data.

7-Eleven also pointed out that the facial images were heavily blurred, and that the "raw" images showing visible faces were only accessible to a very limited group.

The Commissioner considered whether or not individuals were "reasonably identifiable" from the facial images and faceprints. This is an objective test that has practical regard to the context in which the issue arises. The Commissioner concluded that a *"facial image alone will generally be sufficient to establish a link back to a particular individual, as these types of images display identifying features unique to that individual".* This was so even where the images were not used to actually track or monitor any of the individuals.

The Commissioner also found that the system used by 7-Eleven *"enabled an individual depicted in a faceprint to be distinguished from other individuals whose faceprints were held on the Server"*. On that basis, the individuals depicted in the faceprints were "reasonably identifiable" and, therefore, the faceprints were themselves personal information. This was perhaps a surprising finding, as 7-Eleven had no way of actually ascertaining the identity of the individuals concerned from the faceprints. It seems that the Commissioner's view is that "individuated" information that can be used to distinguish an individual within a defined group without necessarily revealing the individual's identity can be caught by the existing definition of "personal information" under the Privacy Act. This may have significant implications for other types of individuated information, such as cookies and tracking IDs that are used to customise online experiences without revealing individual identities.

Was the information collected by 7-Eleven?

The Commissioner's found that 7-Eleven collected the images generated on the tablets because:

- the tablets were set up in 7-Eleven's stores at 7-Eleven's request;
- the images were generated in the course of collecting feedback about 7-Eleven's stores;
- 7-Eleven had a contractual right to use the tablets; and
- the agreement with the service provider referred to the images as being 7-Eleven's data.

Similarly, the Commissioner's view was that 7-Eleven collected the faceprints generated on the service provider's servers because:

- they were generated for 7-Eleven's benefit;
- the faceprints themselves were also described in the agreement as being 7-Eleven's data; and
- the agreement technically granted 7-Eleven rights to access and use the faceprints, even though in practice 7-Eleven did not make use of those access rights.

Again, this may be considered a somewhat surprising finding, given that the facial information existed only very briefly on the in-store tablets and 7-Eleven had very little practical control over the service provider's systems. The consequence of the position taken by the Commissioner is that customers may in effect become vicariously liable for personal information generated by their service providers, even if in practical terms they never take possession of or have access to that information. This could have clear implications for outsourcing arrangements as customers may become legally responsible for conduct over which they have little or no practical control. It reinforces the position that the Commissioner has consistently taken that it is not possible to outsource responsibility for privacy compliance.

Was it "reasonably necessary" for 7-Eleven to collect this information?

Under APP 3, the general position is that a private sector entity such as 7-Eleven must not collect personal information unless it is reasonably necessary for one of its functions or activities. The Commissioner indicated that in making this assessment *"consideration should be given to whether any interference with personal privacy is proportionate to a legitimate aim sought"*. This includes consideration of whether the function or activity could be undertaken without collecting that personal information, or by collecting a lesser amount of personal information.

The use of biometric information, such as facial images and faceprints, is generally regarded as a privacy-invasive activity. A corollary of this is that biometric information should be used in a sparing and considered manner. The Commissioner was satisfied that implementing systems to understand and improve customers' in-store experience was a legitimate function of 7-Eleven. However, the Commissioner also found that the large-scale collection of customers' biometric information was not reasonably necessary for that purpose. This was in part because of the higher risk to individuals if this type of information is compromised (since biometric information generally cannot be changed) and because there were less privacy intrusive ways that the customer feedback surveys could have been conducted. Of particular note, the fact that 7-Eleven did not conduct a privacy impact assessment was considered to be a relevant factor for the Commissioner in determining that the activity was not reasonably necessary.

Did 7-Eleven provide adequate notice and obtain consent?

The Commissioner reaffirmed that entities should generally not rely on implied consent when collecting sensitive information. Guidance from the Commissioner indicates that, where an entity intends to collect sensitive information from its customers, a request for consent should:

- clearly identify the kind of information to be collected, the recipient entities, and the purpose of the collection;
- be sought expressly and separately from a privacy policy at a current point in time; and
- be fully informed and freely given.

In this case, the Commissioner found that 7-Eleven did not take reasonable steps to notify individuals about the facts and circumstances of collection, or the purpose of collecting their facial images and faceprints. While a notice was displayed at the store entrance about use of facial recognition cameras, there was no specific information provided on or in the vicinity of the tablet device, or while the customer completed the feedback survey. While there was some general information about collection and use of biometric information in 7-Eleven's privacy policy, which was freely available on its website, this was not clearly linked to the operation of the in-store feedback system. In these circumstances, even though customers gave their feedback voluntarily, there was no basis upon which customers had consented to the collection and use of their sensitive biometric information.

KEY TAKEAWAYS

Use of any kind of widespread facial recognition technology in consumer settings will likely attract regulatory scrutiny – notably, the Commissioner recently commenced an investigation into the use of facial recognition technology by Bunnings and Kmart following a report by the consumer group CHOICE.

Facial images and technical abstractions of facial images such as 'faceprints' may be viewed as personal information even where extensive efforts are made to mask or decouple facial images from other identifying information – in other words, where it is in a sufficient level of detail, a record of a person's face is inherently personal information.

Even if not currently mandatory, conducting a data privacy impact assessment is an important step in identifying and mitigating potential compliance risks, and is something that the Commissioner expects organisations to do as a matter of course before deploying any new technology that may be considered high risk from a privacy perspective.

Commissioner initiated investigation into Clearview AI, Inc. (Privacy) [2021] AICmr 54 (14 October 2021)

Controversial facial-recognition service provider Clearview AI, Inc (**Clearview AI**) has been the subject of close attention over the past year by national privacy regulators around the world. Following a joint investigation with the UK's Information Commissioner, the Australian Information Commissioner found that Clearview AI's facial recognition service failed to comply with numerous aspects of the Privacy Act and made orders that essentially will prevent Clearview AI from providing its services in Australia.

Background

Clearview AI provided a facial recognition tool to registered users, limited in Australia to law enforcement agencies, including the Australian Federal Police (which was incidentally the subject of a separate investigation and determination by the Commissioner in relation to the use of the Clearview AI tool). The tool was described by Clearview as 'like Google search for faces' and operated by scraping public images from the internet, creating facial 'vectors' with machine learning, and then matching uploaded images against the scraped image vectors. If the tool identified sufficiently similar image vectors, it would return the matched scraped images as a thumbnail and include a link to the source. Essentially, the tool could help agencies identify an unknown person from their photo.

What did the Commissioner find?

The Commissioner found that both the scraped images and the uploaded images collected by Clearview AI were biometric information and biometric templates. Therefore, the images were sensitive information for the purposes of the Privacy Act and should not have been collected without consent. The terms 'biometric information' and 'biometric templates' are not defined in the Privacy Act. However, the Commissioner provided some useful guidance about how these terms will be applied by the Commissioner in enforcing the Privacy Act:

- 'biometric information' may include physiological characteristics (such as a fingerprint, iris, face or hand geometry) or behavioural attributes (such as a person's gait, signature or keystroke pattern), both of which are usually persistent and unique to an individual; and
- a 'biometric template' is a digital or mathematical representation of an individual's biometric information that can be used by machine learning algorithms to match against other equivalent representations, for verification or identification purposes.

Despite the information provided in various Clearview AI policies, the Commissioner was not satisfied that individuals consented to the collection of their information, or that sufficient notice was provided to the individuals whose images were collected and used by Clearview AI. The Commissioner was predictably critical of Clearview AI's argument that consent could be implied simply from publishing a policy and then allowing individuals to opt-out. In addition, consent to collection could not be implied simply from the fact an image had been uploaded on a 'public' social media page. The Commissioner stated that *"the act of uploading an image to a social media site does not unambiguously indicate agreement to collection of that image by an unknown third party for commercial purposes"* and could *"certainly"* not be inferred where the individual's image was uploaded by another person. There was also no suggestion that Clearview had considered whether the individuals from which it was collecting sensitive information, including children, had the relevant capacity to consent.

In fact, the Commissioner found that *"the vast majority of individuals would not have been aware or had any reasonable expectation"* that their information would be collected by Clearview AI. As such, not only did the Commissioner find that there was no consent to collection, Clearview AI had collected images by covert means and for purposes that could result in significant harms, including risk of misidentification by law enforcement agencies. In those circumstances, the Commissioner considered that the "indiscriminate" method of collection used by Clearview AI was unreasonably intrusive and unfair, and could not be justified by reference to any public interest benefit.

Just how accurate is facial recognition anyway?

Notably, the Commissioner found that Clearview AI had also breached the requirement to ensure that personal information is *"accurate, up-to-date, complete and relevant"* having regard to a particular use or disclosure. In making this finding, the Commissioner pointed to concerns raised in academic research regarding the risk of false positives, bias and inaccuracy in facial recognition technology.

Clearview AI submitted that its results were never intended to be a single-source system for establishing identity, and that its service only provided *"indicative, not definitive"* results. Clearview AI also submitted an 'accuracy report' to the Commissioner as part of the investigation, describing tests that had been conducted on the Clearview AI technology by an independent panel. However, this was not enough to satisfy the Commissioner, who said that:

> *The respondent handles a substantial and rapidly expanding volume of personal information, from which serious decisions may be made by its law enforcement users. In circumstances where a variety of studies have uncovered concerns with the accuracy of different facial recognition technologies, and significant harm may flow from misidentification, the steps needed to ensure accurate disclosures, should be robust, demonstrable, independently verified and audited.*

This statement provides important guidance for any organisation intending to deploy facial recognition technology for 'serious' decision-making and where harm may flow from misidentification. It underscores the expectation that accuracy testing will be robust with reference to the intended use, and demonstrates that even if information is properly collected there remains a separate onus to ensure that the information remains accurate and relevant for its intended use. This will be an important consideration for any AI engine that relies upon personal information.

What's next?

The Commissioner has ordered Clearview AI to delete all data collected in breach of the APPs. While not directly ordered to leave Australia, the outcome will likely be that Clearview AI can no longer viably operate in Australia. However, Clearview AI has applied to have the Commissioner's decision reviewed by the Administrative Appeals Tribunal, arguing amongst other things that the Commissioner lacked jurisdiction to make findings against Clearview AI, given it conducted all information collection and processing activities outside Australia. While not many will wish to follow directly in Clearview AI's footsteps, this challenge will be of great interest to other online service providers that provide their services on a global basis, but without a physical presence in Australia, and may be hoping to avoid the reach of the Privacy Act. It will certainly serve as an interesting counterpoint to the Commissioner's findings about jurisdiction in her recent determination against Uber, which we covered in last year's annual update and the recent decision of the Full Federal Court (albeit on an interlocutory basis) in the ongoing civil penalty proceeding against Meta in relation to the Cambridge Analytica incident as to whether Meta could be considered to be carrying on business in Australia.

Findings similar to those of the Commissioner have been made against Clearview AI by regulators in a range of different jurisdictions. In a number of instances, other regulators have also issued significant fines. The fact that in this case the Commissioner was satisfied with non-monetary declarations may be indicative of the difficulties that the Commissioner currently faces in seeking civil penalty orders under the Privacy Act, including having to establish that the breaches in question are either 'serious' or 'repeated'. One likely outcome of the ongoing reform process is that the Commissioner will be given greater scope to issue penalty notices without having to meet this threshold, which would then open up the option of taking a more aggressive approach on cases such as this one.

KEY TAKEAWAYS

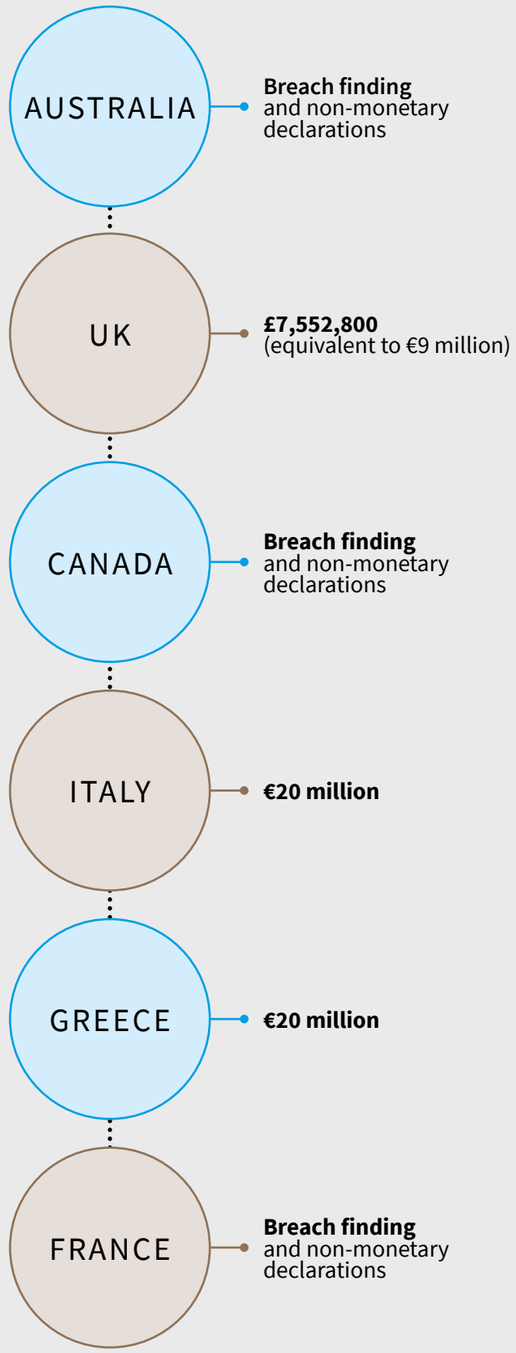
Use of facial recognition and other intrusive technologies remains a key focus for the Commissioner.

Any information about a person's physical characteristics or behavioural attributes may be treated as biometric information, which may then be subject to stricter regulation under the Privacy Act.

Express opt-in consent should always be sought when collecting sensitive information.

Where personal information serves as an input in any automated decision-making process it will be important to ensure that there has been robust testing carried out to confirm the accuracy and relevance of the information and any decision made using that information.

CLEARVIEW AI PENALTIES AROUND THE WORLD TO DATE



Lloyd v Google LLC [2021] UKSC 50

In November 2021, the UK Supreme Court handed down a momentous decision in the *Lloyd v Google* privacy class action. The decision was a significant win for Google and illustrates the challenges that litigation funders may face in turning privacy class actions into a lucrative business.

Background

The facts of the case related to Google's use of advertising cookies on mobile devices in England and Wales, and a 'workaround' developed by Google for Apple's Safari web browser, which was alleged to have negated user consent. Richard Lloyd brought a class action claim on behalf of several million allegedly affected individuals.

At an earlier stage of the proceeding, it was controversially suggested that compensation should be available under the UK Data Protection Act for the mere 'loss of control' of personal data, and that damages could be assessed on a 'lowest common denominator' approach (i.e. based on the hypothetical person least affected by the breach, without having to establish damages for each individual class member). The argument for 'loss of control' damages was based on reasoning from a case on the tort of misuse of private information, with Lloyd arguing that the same approach to damages should also apply to both claims under the Data Protection Act as they also derived from the same right – the right to privacy. However, the Supreme Court disagreed, finding that personal data didn't need to have a 'private' character, and that the terms of the Data Protection Act did not permit damages for harm less than 'distress' and clearly drew a distinction between the contravention and the damage resulting from that contravention. In other words, the legislation assumed that the contravention and the damage resulting from the contravention would not be one and the same. Accordingly, it was not sufficient for Lloyd to establish merely that there had been a contravention, he also needed to establish that each class member had incurred some compensable damage as a result of that contravention.

Global context

The Australian Information Commissioner has authority under the Privacy Act to declare that an individual affected by a privacy breach is entitled to a specified amount of compensation for loss or damages suffered by reason of the breach. As in the case of the UK Data Protection Act, the wording used in the legislation draws a clear distinction between the breach and the loss or damage that may flow as result of the breach. Accordingly, the Supreme Court's reasoning that entitlement to compensation can only flow where some loss or damage has been established may be equally applicable in Australia. This may present significant challenges for representative claims. As we noted in last year's update, the Commissioner's determination in '*WP*' *and Secretary to the Department of Home Affairs* highlighted the complex nuances which can arise when seeking to determine compensation for a large group on the basis of non-economic loss. That was the first determination in Australia which resulted in an award of compensation for non-economic loss on a class basis, and included an expected 12 month period for establishing an evidentiary basis for compensation across the entire group of affected individuals. Unless the law develops in a different direction as a result of the current ongoing reform process, for the time being it seems that difficulties around proving loss and damage will continue to be a challenge for representative privacy complaints.

It is interesting to read the decision alongside the recent decision of the Singapore High Court in *Bellingham, Alex v Reed, Michael* [2021] SGHC 125. That case was the first to be handed down on the scope of the Singapore Personal Data Protection Act (**PDPA**), and the Court was required to consider what constitutes 'loss or damage' for the purpose of the threshold requirement for data subjects to pursue a private claim under the PDPA. The Court held that 'loss or damage' did *not* include 'loss of control' over personal data, nor did it encompass other broader concepts of harm such as distress, or injury to feelings. Instead, the PDPA only refers to those heads of loss or damage available for torts at common law, limiting the available recovery to financial loss, property damage and personal injury (including psychiatric harm). Again, the result is not good news for would-be class action litigants.

KEY TAKEAWAYS

Providing evidence of compensable damage will continue to be a major challenge for future privacy class actions – establishing that there has been a breach will not be enough on its own.

Particular difficulties will arise where compensation is sought for non-economic loss, where the loss suffered by each individual may vary significantly depending on their individual circumstances.

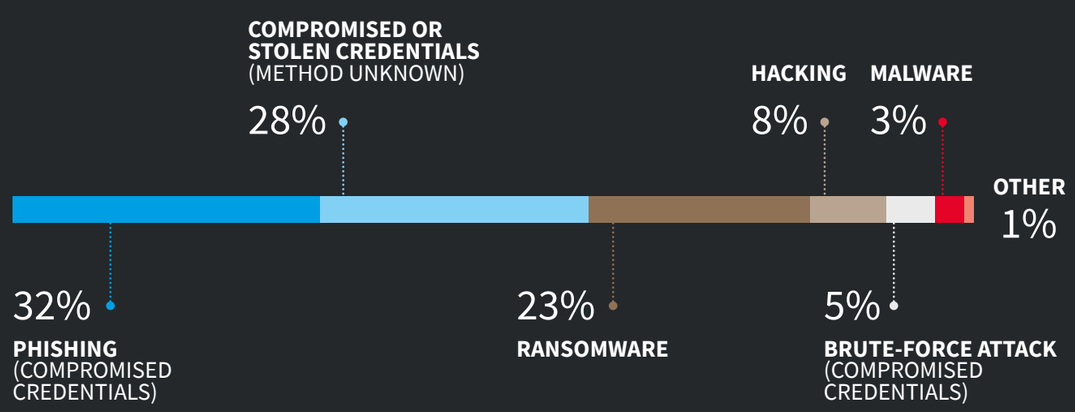
While there is limited case law in Australia to provide precedent, cases from other jurisdictions may provide some insight into how courts may approach these difficult issues.

PRIVACY NEWS BITES

1 With an aim to 'build a ring of regulatory defence', four regulatory agencies (the OAIC, the ACCC, the ACMA and the eSafety Commissioner) have formed the 'Digital Platform Regulators Forum' or 'DP-REG' to collaborate on the intersection of their work around digital platforms. For FY23, the DP-REG's strategic priorities are to focus on the impact of algorithms (including algorithmic recommendations and profiling, moderation algorithms, promotion of disinformation, harmful content, and product ranking and displays on digital platforms such as online marketplaces), to increase transparency of digital platforms' activities and how they are protecting users from harm, and to increase collaboration and build capacity within the DP-REG.

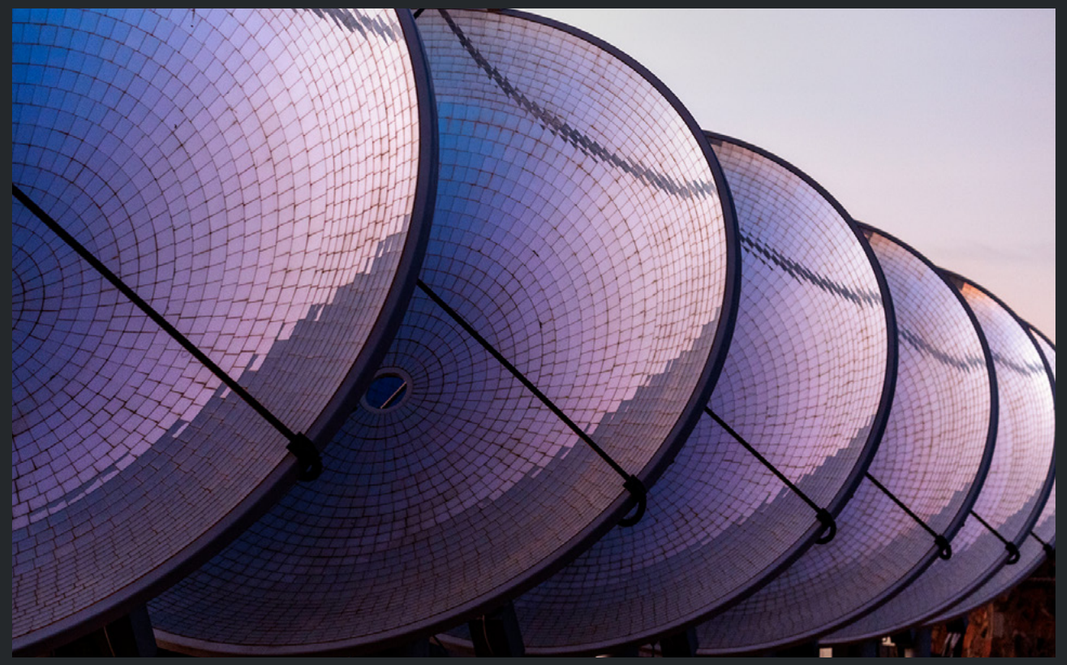
2 In the fourth year of the mandatory data breach notification scheme, the latest Notifiable Data Breaches Report from the OAIC recorded 464 data breach notifications from July to December 2021, a 6% increase compared with the previous 6 months. Interestingly, there was a notable drop in the latest numbers of the percentage attributed to malicious or criminal attacks (55% of the total, down 9%) and a significant rise in the number of breaches due to human error (41% of the total, up 43%). The proportion of cyber security incidents attributed to phishing, compromised credentials, and ransomware continues to vastly outweigh those incidents caused by traditional 'hacking' and other types of attacks.

UNDERLYING CAUSES OF CYBER SECURITY INCIDENTS



3 The ACMA continues to be very active in its enforcement of the Spam Act, with significant fines being issued in recent times to major corporates such as Sportsbet, Woolworths and Optus. Indeed, "enforcing SMS and email unsubscribe rules" is one of the ACMA's compliance priorities for 2022-2023. In particular, the ACMA has indicated that it will be focussing on businesses that are sending SMS and emails when people have unsubscribed. We have also seen recurring issues with organisations mistakenly assuming that they do not need to include unsubscribe links in their messages on the basis that they are purely factual in nature, failing to appreciate that the factual information they contain is intrinsically commercial in nature. Formal investigations by the ACMA are typically preceded by "compliance alerts" sent to highlight specific instances of potential non-compliance that have been the subject of customer complaints. The ACMA is more likely to commence a formal investigation where there are a series of complaints and alerts, indicating a systemic issue or inability / unwillingness to update compliance procedures in response to alerts sent by the ACMA. Accordingly, it is important to take alerts seriously and ensure that any potential non-compliance is promptly addressed to prevent recurrence of issues and further complaints.

4 An updated version of the Privacy (*Credit Reporting*) Code 2014 came into effect from July 2022. The updated code reflects the new ability for reporting of financial hardship information, which the OAIC described as a 'significant reform' to the Privacy Act. Financial hardship arrangements will now be reported on an individual's credit report, alongside their repayment history information.



INTERNATIONAL DATA TRANSFERS – A GLOBAL HEADACHE

One of the areas that has attracted most attention (particularly from multinational organisations) in the current round of privacy law reforms in Australia is how best to regulate the transfer of personal information out of Australia. Restrictions on the flow of data across borders can present a major headache for organisations that wish to centralise their global operations. As well as imposing costs on business, these restrictions can also cause confusion for individual consumers and leave them uncertain as to how their data will be protected when dealing with international organisations.

The Privacy Act Review Discussion Paper proposes a number of possible changes to Australian law that would help to streamline the current framework for transferring information outside Australia, including by introducing a mechanism to create a whitelist of countries that are considered to provide an equivalent level of privacy protection to Australia and developing standard contractual clauses to support disclosures to entities in other jurisdictions. The Discussion Paper also contemplates the introduction of enhanced transparency requirements around international transfers, including by imposing stricter requirements to identify the types of information that may be transferred and the locations where information may be transferred.

However, it would be a mistake to think that Australia is the only jurisdiction grappling with these issues. Uncertainty regarding rights to transfer personal information across borders is a global issue, as the insights below from our colleagues in the KWM global network attest.

The view from China (Peter Bullock, KWM Hong Kong)

International businesses operating in China have broadly two concerns surrounding exports of data from Mainland China:

1. Can such transfers be undertaken as part of servicing the normal business model (e.g. selling European goods from Europe into China)?

2. Can management and other corporate data be freely sent from China back to head office?

Until recently, both questions could be answered with a cautious 'yes'. The first set of transfers would be viable unless and until the offshore website was blocked by the Great Firewall. The second set of transfers should not trigger queries so long as mandatorily disclosable information remained available to China regulators in-country.

However, a triumvirate of recent Mainland China laws (Personal Information Protection Law, Cybersecurity Law and Data Security Law) have significantly complicated matters. Their combined effect is to require anyone seeking to collect and export data (personal or otherwise) to carefully evaluate what is to be exported, and in many cases to obtain prior state permission for the export.

The potentially most disruptive requirements involve a Mandatory Security Assessment by the Cyberspace Administration of China (**CAC**), the de facto data privacy and cybersecurity regulator. Such mandatory assessments are triggered when personal data exports from China and required by

- the operators of critical information infrastructure;
- a data processor (essentially anyone with a data network) wishing to export "important data". "Important data" is broadly defined in relation to the damage caused in the event of its misuse;
- a data processor that processes personal data of more than 1 million data subjects; or
- a data processor that has transferred personal data of more than 100,000 data subjects or sensitive personal data of more than 10,000 data subjects out of Mainland China since 1 January of the previous year.

The regulations relating to Mandatory Security Assessment are highly granular. Even when assessment is not required, data controllers face the prospect of requiring a personal information protection certificate from the CAC or meeting other conditions of the CAC or other regulators before being permitted to export data.

These regulations have been causing consternation for most businesses requiring transfer of data across Chinese borders. This is not least felt in Hong Kong where, ironically, there are currently no formal regulations constraining the export of personal data. The relevant provisions of the Personal Data (Privacy) Ordinance (**PDPO**) (section 33) have never been brought into force since the PDPO's enactment in 1995. Businesses in Hong Kong are facing the same difficulties in complying with the new PRC laws as everyone else, but given that Mainland China is Hong Kong's primary market, considerable thought is being given as to how to promote cross border data transfers, not least owing to Hong Kong's imperative to develop seamless trade with its immediate neighbours in Guangdong (and Macau) pursuant to the Greater Bay initiative.

The view from the EU (Sana Duncan and Daniel Jones, KWM London)

There have been a number of significant shifts in the European data protection landscape over recent years. The EU's General Data Protection Regulation (EU) 2016/679 (**GDPR**) has been considered the gold standard of data protection globally since it came into force in 2018, placing a number of obligations on organisations both inside and outside the EU that are processing personal data of EU-based individuals. These obligations have only increased in scope over the last few years.

One constant is that, under the GDPR, transfers of personal data outside of the EU are prohibited unless one of the following circumstances applies:

- the country to which the personal data is being exported has an "adequacy" decision from the European Commission (this means that the Commission has designated a third country as having "adequate" data protection safeguards in place); or
- where a third country does not have adequacy status, the appropriate safeguards as prescribed by the GDPR are in place.

What are the "appropriate safeguards"?

Article 46 of the GDPR sets out the appropriate safeguards available to organisations when conducting data transfers with organisations based outside of the EU. Data transfers, in this context, mean sending personal data out of the EU (e.g. by email) and/or accessing EU personal data outside of the EU (e.g. a non-EU company accessing shared systems with an EU group company).

By far the most common mechanism for transferring personal data outside of the EEA is via the European Commission's Standard Contractual Clauses (**SCCs**). The SCCs are a standard set of clauses that have been published by the EU Commission to govern data transfers from the EEA data exporting party to the non-EEA data recipient.

Previously, implementing the SCCs was a fairly standard process, which involved completing the annexes to the SCCs with factual information in relation to the data transfer and signing the SCCs agreement.

However, as a result of the Schrems II decision in 2020, the old SCCs have now been replaced with a new modular format of SCCs in an attempt to take account of modern transfer scenarios with multi-party arrangements and onward supply chains. The correct module must be selected depending on what the recipient party will be doing with the exported personal data.

Further, organisations now have the added responsibility of assessing the risk of the exported personal data being accessed by public authorities in the recipient destination (as was the case in Schrems II, with the European Commission finding that government oversight of data sent to the US invalidated the Privacy Shield – the transfer mechanism agreed between the EU and US). As a result, organisations can no longer rely on the SCCs as being bulletproof simply because they have been rubber-stamped by the Commission, instead, the onus is on organisations themselves to weigh up the risks of transferring personal data outside the EU.

In fact, the new SCCs contain a warranty provision stating that at the time of entering into the SCCs, the parties do not have any reason to believe that the laws and practices applicable to the data importer contradict the essence of the GDPR (i.e., the safeguarding of personal data and ensuring that individuals can exercise their rights over their personal data).

Transfer Impact Assessments

To achieve this, whilst also ensuring the usual technical and organisational safeguards are in place, when an EU-based organisation decides to transfer personal data to an organisation based outside of the EU (and not in an adequate country), it is now additionally necessary to conduct a Transfer Impact Assessment (**TIA**). A TIA should consider:

(a) the local legal framework (i.e., whether the non-EU country has an established and respected legal system, with a high degree of independence and integrity, and which enforces foreign judgments or arbitration awards);

(b) whether public authorities in the non-EU country may seek to access the data without the organisation's knowledge (consideration should be given to the country's legislation and real/reported practices); and

(c) whether public authorities in the non-EU country are able to access the data via telecoms/communication channels (again organisations should consider the country's legislation and real/reported practices).

In the event that a TIA indicates that a particular data transfer is high-risk, organisations will need to implement and document 'supplemental measures' in order to mitigate the risk. Effectively, these are additional security measures (e.g., enhanced encryption techniques).

Clearly, this is a much more involved and labour-intensive process than completing the old SCCs. It is no longer acceptable for data exporter organisations to simply have a good understanding of their own obligations under the data protection laws; they must also now have a firm grasp on the recipient's data protection obligations and the legal and regulatory landscape of the country where the recipient is based.

And the UK...?

Following Brexit, the UK now has its own data transfer regime, which, for now, largely mirrors that of the EU. The EU GDPR has been incorporated into the UK GDPR via the Data Protection Act 2018, although there are some differences that organisations should be aware of.

In February 2022, the UK issued its International Data Transfer Agreement (**IDTA**), which is essentially its version of the new EU SCCs and a new IDTA Addendum (the **UK Addendum**). The UK Addendum can be appended to the new EU SCCs if an organisation has already incorporated the EU SCCs into its data transfer agreements. Together, these two documents are often referred to as the UK SCCs.

This means that where an organisation has already completed the new EU SCCs, if the data transfer includes transfers to the UK, then it will only need to complete the UK Addendum, as opposed to a full version of the IDTA. It cannot, however, be appended to an old version of the EU SCCs.

When conducting data transfers with UK-based organisations, it is necessary to carry out a Transfer Risk Assessment (or 'TRA') which requires fundamentally the same approach as a TIA.

CONTACTS

MICHAEL SWINSON
PARTNER
MELBOURNE
TEL +61 3 9643 4266
MOB +61 488 040 000
EMAIL michael.swinson@au.kwm.com

CHENG LIM
PARTNER
MELBOURNE
TEL +61 3 9643 4193
MOB +61 419 357 172
EMAIL cheng.lim@au.kwm.com

BRYONY EVANS
PARTNER
SYDNEY
TEL +61 2 9296 2565
MOB +61 428 610 023
EMAIL bryony.evans@au.kwm.com

KIRSTEN BOWE
PARTNER
BRISBANE
TEL +61 07 3244 8206
MOB +61 409 460 861
EMAIL kirsten.bowe@au.kwm.com

DARYL COX
SPECIAL COUNSEL
MELBOURNE
TEL +61 3 9643 4170
MOB +65 8321 6377
EMAIL daryl.cox@au.kwm.com

KENDRA FOURACRE
SENIOR ASSOCIATE
MELBOURNE
TEL +61 3 9643 4105
MOB +61 437 959 826
EMAIL kendra.fouracre@au.kwm.com

CAL SAMSON
SENIOR ASSOCIATE
MELBOURNE
TEL +61 3 9643 4166
MOB +61 437 652 995
EMAIL cal.samson@au.kwm.com

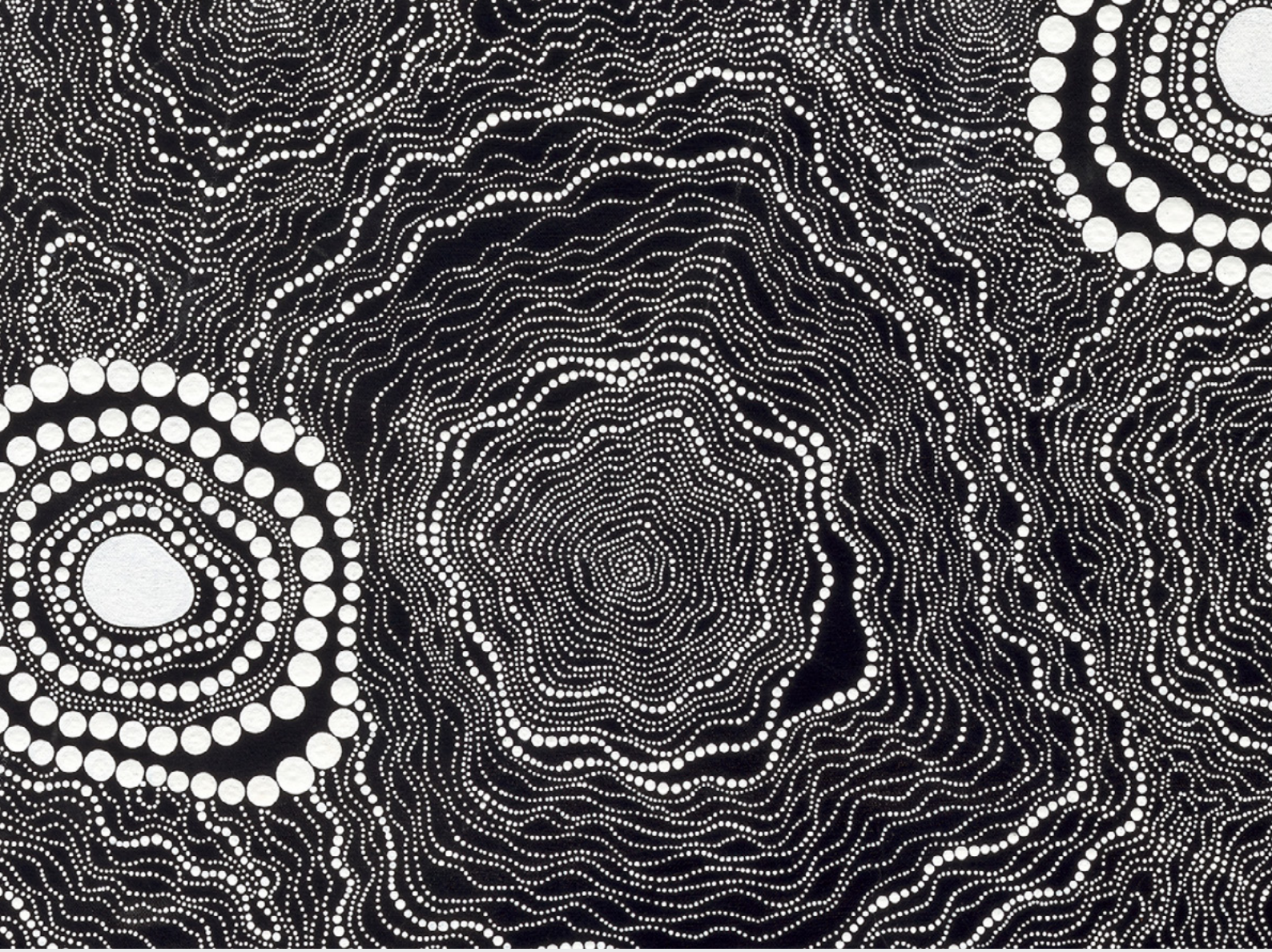
KAI NASH
SOLICITOR
BRISBANE
TEL +61 7 3244 8157
MOB +61 401 250 434
EMAIL kai.nash@au.kwm.com

MADELINE CLOSE
SOLICITOR
MELBOURNE
TEL +61 3 9643 4302
MOB +61 417 059 845
EMAIL madeline.close@au.kwm.com

WHYE YEN TAN
SOLICITOR
MELBOURNE
TEL +61 3 9643 4177
MOB +61 418 556 898
EMAIL whyeyen.tan@au.kwm.com

EDITOR
Cal Samson

CONTRIBUTORS
Michael Swinson, Peter Bullock, Sana Duncan, Daniel Jones, Kai Nash, Kat Jukes



ABOUT KING & WOOD MALLESONS

A firm born in Asia, underpinned by world class capability. With over 2000 lawyers in 30 global locations, we draw from our Western and Eastern perspectives to deliver incisive counsel.

With 30 offices across Asia, Europe, North America and the Middle East we are strategically positioned on the ground in the world's growth markets and financial centres.

We help our clients manage their risk and enable their growth. Our full-service offering combines un-matched top tier local capability complemented with an international platform. We work with our clients to cut through the cultural, regulatory and technical barriers and get deals done in new markets.

JOIN THE CONVERSATION

SUBSCRIBE TO OUR WECHAT COMMUNITY.
SEARCH: KWM_CHINA

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.

www.kwm.com