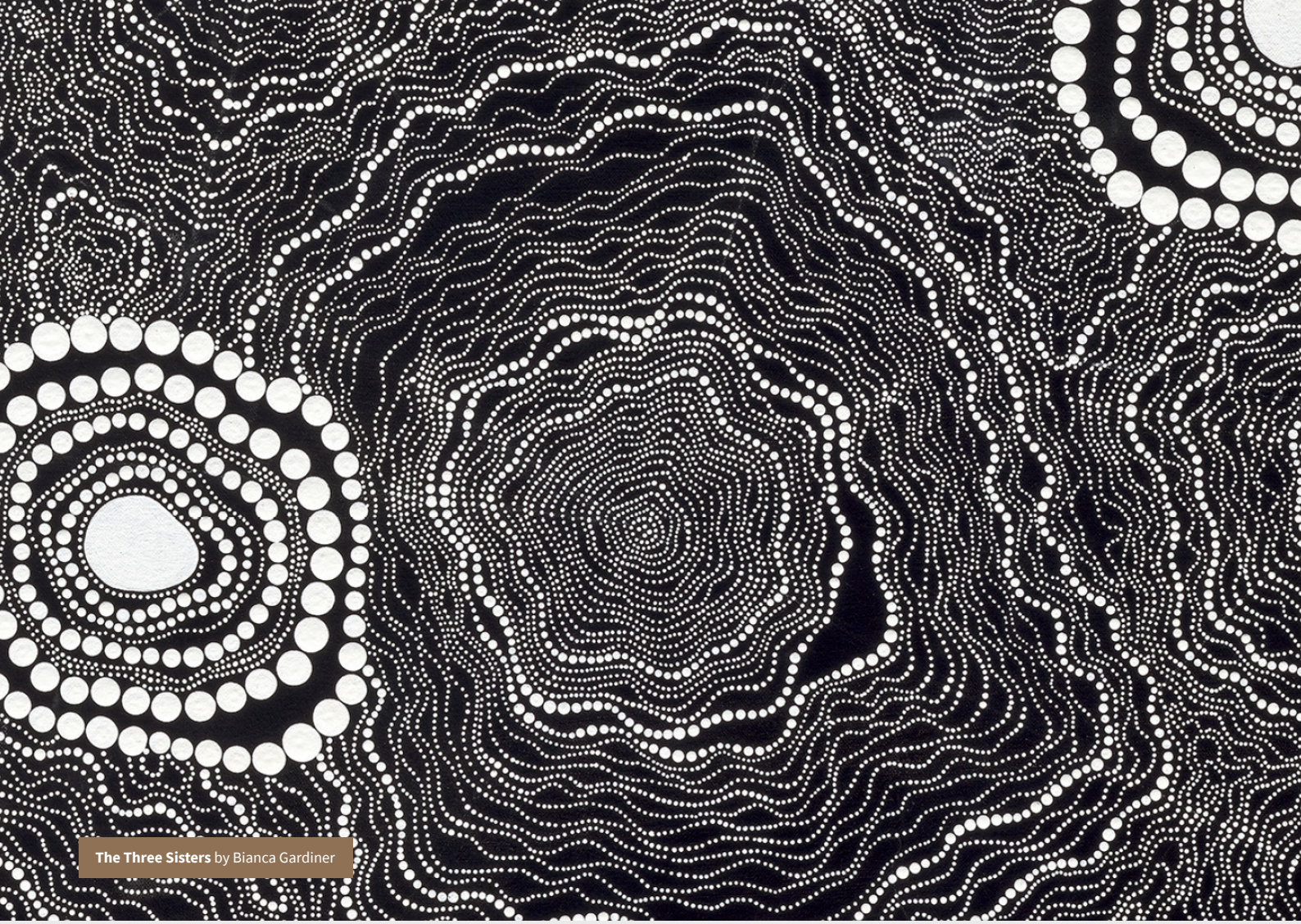


PRIVACY ANNUAL UPDATE

OCTOBER 2023

KING&WOOD MALLESONS
金杜律师事务所

CONTENTS

ANOTHER BIG YEAR FOR PRIVACY - AND PLENTY MORE TO COME!

Each year, as we prepare this publication and reflect on the key developments in Australian privacy law, it seems as though the previous 12 months have been uniquely eventful and the pace of change in this area faster than ever before.

In what seemed like moments before we were about to hit 'send' on this year's update, the Government released its long-awaited response to the Privacy Act Review Report. You can read our detailed summary here. By way of reminder, the Government was responding to a range of sweeping privacy-related reforms proposed by the Attorney-General's Department earlier in the year (see our earlier reporting on that here, as well as our more detailed take on some of the key reform themes here and here). We should now expect draft legislation to implement the first set of proposals accepted by the Government in early 2024, along with further targeted consultation on other proposals that have been accepted 'in principle' but that may require further workshopping between Government and relevant stakeholders. Naturally we will keeping you informed every step of the way.

While much attention has naturally been focused on these pending reforms, the year has also been jam-packed with other developments worthy of note. In this edition of our annual update we look at, amongst other things:

- Changes to the Privacy Act that significantly increase the maximum penalties available for serious or repeated data breaches – an urgent response by the Government in response to a series of recent major data breaches – and expand the geographical reach of the Act.
- Recent examples in which the Privacy Act has been enforced against multinational organisations in relation to conduct outside Australia, illustrating the increasingly global nature of privacy law enforcement.
- Privacy implications of new generative AI technologies (after all, no legal update in 2023 would be complete without a mention of AI!).

We also provide the usual round-up of the most significant privacy decisions and determinations handed down over the last year, along with a special feature from our colleagues in Beijing on new cross-border data transfer rules in China.

We hope you enjoy this 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.

MORE MONEY, MORE PROBLEMS: HIGHER PENALTIES AND EXPANDED ENFORCEMENT POWERS

The maximum penalties available under the Privacy Act have been increased in the wake of a series of high-profile data breaches. Changes have also been proposed to make the Act easier to enforce against foreign organisations, and to boost a range of other enforcement-related powers. This may signal an era of more active and aggressive enforcement of the Privacy Act.

While progress on the overall program of privacy reforms has been frustratingly slow, the Government has moved more swiftly to bulk up certain key enforcement-related features of the Privacy Act. These amendments were passed through Parliament at an accelerated pace in response to the series of high-profile data breaches in the second half of 2022, and took effect in December. You can read our update from the time here, and we have summarised the key changes below.

Increased penalties for serious or repeated breaches

Most significantly, the changes in December massively increased potential penalties for serious or repeated breaches of the Australian Privacy Principles (**APPs**). Such a breach may now attract a civil penalty up to the greater of:

- $50 million;
- three times the value of the benefit obtained from the breach; or
- if the court cannot determine the total value of that benefit, 30% of adjusted turnover in Australia during the 'breach turnover period' (being the longer of 12 months prior to the breach or the period over which the breach occurred).

This brings penalties available under the Privacy Act into line with the Australian Consumer Law, something that had long been a point of bipartisan agreement (we first flagged the likelihood of this alignment in our annual update for 2019 (see here), as a key recommendation made by the ACCC in the final report of the Digital Platforms Inquiry). However, it was not until recent data breaches started dominating the headlines, that the government was actually spurred into action.

Previously, the maximum penalty under the Privacy Act for a serious or repeated breach of the APPs was $2.22 million, so the changes represent a massive increase in the potential exposure for organisations under the Act. This brings Australia's enforcement regime closer in line with the European GDPR (noting that there are still differences, including that maximum penalties under the GDPR are set by reference to global revenue, albeit in a smaller proportion and over a fixed 12 month period). Clearly the changes provide the threat of a much bigger "stick" with which to punish serious breaches of the Act. However, it remains to be seen whether this threat on its own is sufficient to prompt major changes in practice, or whether we will need to wait for fines to actually start being levied before we see organisations really sitting up and taking notice.

Expanded extraterritorial reach

The changes in December also radically expanded the extraterritorial reach of the Privacy Act by removing the last limb of the existing 'Australian link' test. We discuss the impact of this amendment and the wider context later in this update, but the key point to note is that the Privacy Act now applies to acts done outside Australia by any foreign organisation as long as the organisation carries on business in Australia. There is no longer a need to establish that the acts relate to information that was collected or held in Australia. The implications of this are significant, as it may extend the reach of the Privacy Act to conduct that takes place outside Australia in relation to individuals who have no connection with this country (although due to existing anti-overlap provisions there would be no contravention of the Privacy Act if a foreign entity could establish that their conduct was required by an applicable law of a foreign country). This broad expansion may not have been the intended outcome. However, it is clear that the changes were intended to remove barriers to enforcement, and so it may signal the start of a new phase of more aggressive investigation of breaches and associated enforcement action by the OAIC in relation to multinational organisations.

Other enhanced enforcement powers

Finally, the changes in December also granted the OAIC a range of enhanced statutory enforcement powers, including:

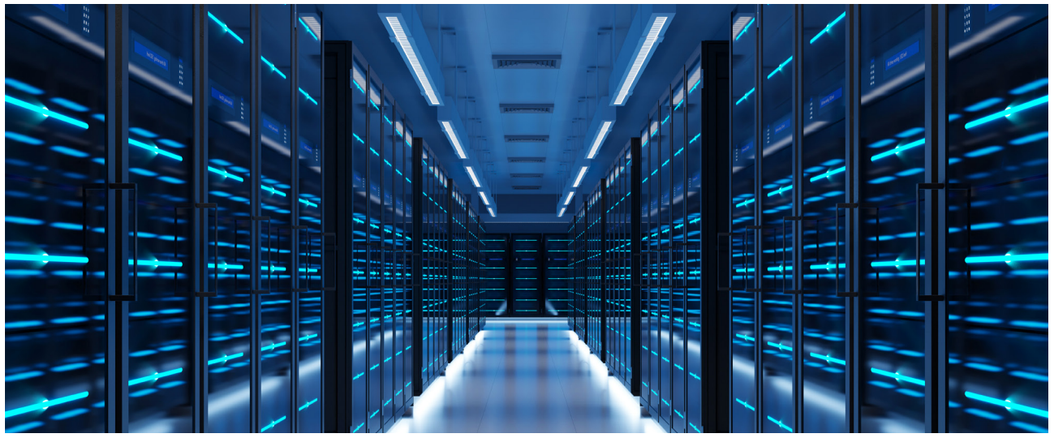
- enhanced information gathering powers in relation to actual or suspected data breaches and compliance with data breach reporting requirements;
- powers to publish information obtained under the Privacy Act (including potentially confidential commercial information) if satisfied it is in the public interest to do so;
- when making a privacy determination, powers to require that an organisation engage an independent adviser to review its privacy compliance practices and/or to publish a statement about a privacy breach and associated remediation action; and
- powers to issue infringement notices to persons who refuse to answer questions or produce documents when required.

As a result of these changes, it is at least somewhat more likely that information shared with the OAIC during an investigation or relating to a data breach will be made public (especially where there is a major incident). Importantly, unlike the increased penalties (which will only apply to future breaches), a number of these changes have retrospective effect and so apply to existing investigations and information previously shared with the OAIC.

What does this mean for my organisation's risk profile?

While many column inches have been taken up with law firms and journalists writing on these changes, our key takeaways can be summarised in four points:

- Despite the significant *theoretical* maximum penalties that the OAIC may seek under the Act, it is important to remember that it is ultimately the court that decides a civil penalty, not the regulator. In doing so, the court will apply usual sentencing principles, including to ensure that the penalty is proportionate to the breach. The maximum available penalty would be reserved for only the very worst conduct and, therefore, only represents a theoretical upper boundary rather than an expected outcome.
- Civil penalty proceedings will be reserved for the most significant cases where there has been significant consumer harm. In order to obtain a penalty order, the OAIC will still need to establish that any breach of the APPs was either 'serious' or 'repeated'. It is notable that the OAIC has historically not sought to bring civil penalty proceedings. Indeed, there is only one instance in which the OAIC has done so (against Meta in relation to the Cambridge Analytica breach), and that proceeding is still working its way through the courts. While the increase in maximum penalties is significant, this change alone is unlikely to result in a flood of new proceedings and we expect this remedy will still be reserved for only the most serious breaches.
- Further enforcement-related changes, including the introduction of a wider range of enforcement options for the OAIC, have been accepted by the Government and will likely be legislated in 2024. This will include a new 'mid-tier' civil penalty provision for breaches that do not meet the threshold of being 'serious' as well as a 'low-level' civil penalty provision for specific administrative breaches, with associated infringement notice powers with set penalties. If this comes to pass, we anticipate that in most cases the OAIC will prefer these alternatives - it would, for example, be much less resource-intensive for the OAIC to issue an infringement notice that is unlikely to be contested (and potentially may be accompanied by an enforceable undertaking to address risk of ongoing breaches), than to pursue civil penalty proceedings which may be robustly defended. This would be consistent with current practice in other analogous areas, such as under the *Spam Act 2003* (Cth), where the vast majority of enforcement actions result in a negotiated outcome via an infringement notice and accompanying enforceable undertaking, rather than court proceedings.
- The changes introduced last December do not actually change any underlying privacy compliance obligations on entities. As such, they do not of themselves impose any new or greater compliance burden on companies that manage personal information (except perhaps for those overseas organisations that may now be caught by the wider extraterritorial test). The changes to come as part of the broader Privacy Act reforms in 2024 and beyond will have a far more substantive impact from an operational perspective, and will likely require all organisations that deal with personal information to rethink their information management processes and procedures.



LOOKING ABROAD: THE INCREASINGLY GLOBAL NATURE OF PRIVACY LAW ENFORCEMENT

The extraterritorial reach of the Privacy Act has recently been expanded (possibly to an unintentional degree). Any foreign entity that is carrying on business here may now be subject to the Act, even in relation to information that has no other connection with Australia or Australians. At the same time, the OAIC has been actively seeking to enforce the Act against global digital businesses. While the Government has committed to revisit this issue, for the moment it is clear that any online business will need to be wary of the Act, even if they have no physical or other direct presence in Australia.

A key theme across a range of privacy-related developments this year has been the surprisingly complex and changing application of the Australian Privacy Act to entities based outside Australia. While ensuring compliance by digital platforms and other multinational organisations doing business with Australians is clearly a priority for the OAIC, the precise limits on the scope of the Act's reach are still somewhat unclear. We hope that more certainty will be delivered through the ongoing law reform process, including by ensuring greater harmony between Australian privacy laws and those that apply in other jurisdictions. In the meantime, multinational organisations that seek to operate from a single global technology platform face the somewhat unenviable challenge of having to simultaneously comply with a range of different legal regimes.

Legislative changes

It is well-established that the Privacy Act has extraterritorial application. Under section 5B, the Act applies to conduct outside Australia by any entity that has an 'Australian link'.

As noted above, the requirements for whether a foreign entity has an Australian link were changed in December 2022. Following the recent changes, an Australian link will be established so long as the foreign entity is carrying on business in Australia. The former requirement that the conduct relate to personal information that the entity had collected or held in Australia was deleted. This means, that, at least theoretically, the Privacy Act may now apply to conduct outside Australia in relation to information about individuals who have no substantive collection with Australia, so long as the entity in question has some business dealings in Australia.

These changes have not passed without some controversy. Following a number of public submissions, and a hearing in November 2022, the Senate Legal and Constitutional Affairs Legislation Committee noted a range of concerns about the amendments, and that the scope of the Act's extraterritorial reach may have been extended too far. Submissions from the Business Council of Australia and the Law Council of Australia noted that it could bring Australian laws into conflict with requirements in other jurisdictions. Ultimately, the Committee recommended further examination of the appropriateness of the Australian link test through Attorney-General's Department's broader review of the Privacy Act.

The Department duly considered the issue and in the Privacy Act Review Report concluded that *"there would be benefit in further clarifying that foreign organisations will only be regulated to the extent that their handling of personal information has a connection to Australia. This would assist foreign organisations understand their obligations."* However, at the same time, the Report noted that any additional threshold test "*would need to be designed in a way that prevents foreign organisations from using loopholes due to advances in technology, and could not be dependent on the means or method of collection or storage of personal information*."

Clearly there remains a concern that foreign digital platform operators could slip through the Act's grasp. Ultimately, the Report concluded that further consultation on the issue should occur, and the Government has agreed to that further consultation in its response to the Report, so this remains a live issue and an area to watch- particularly for foreign enterprises that may have some Australian customers but are currently operating on the assumption that they are not bound by the Act as they have no physical presence here.

Practical enforcement

In practice, the OAIC has in recent years well and truly faced into the challenges enforcing the Privacy Act against global platform operators. In 2021, the OAIC made a determination against Uber, finding that the global technology platform was subject to the Privacy Act given that it entered into contractual arrangements with both Australian riders and drivers, despite having no physical presence. Read more about the Uber decision in our annual update from 2021 (see here). Similarly, a determination made by the OAIC against Clearview AI, along with the subsequent appeal to the Administrative Appeals Tribunal, was in large part focussed on determining whether the scraping of information from Australian websites was sufficient to bring Clearview AI within the purview of the Australian Privacy Act (more on this in our case note below).

Perhaps most significantly, issues regarding the establishment of an Australian link, and the extraterritorial reach of the Privacy Act, have been live issues in the OAIC's ongoing civil penalty proceedings against Meta in relation to the Cambridge Analytica incident (to date the only time the OAIC has sought a civil penalty under the Act). In *Facebook Inc v Australian Information Commissioner* [2022] FCAFC 9, the Full Federal Court held that activities in Australia may constitute carrying on business even if they lack a "commercial" quality and that an entity may be carrying on business in Australia though "repetitive but non-commercial activity" which occurs in one jurisdiction but is ancillary to a business conducted in another jurisdiction. This is a very expansive approach – arguably broader than the approach taken in previous cases – and could result in many more digital platform businesses falling within the reach of the Privacy Act and other Australian laws that use similar jurisdictional tests. An application for special leave to appeal to the High Court of Australia on this question was originally granted in September 2022 but then was later revoked in March 2023. As a result, we'll need to wait a little longer for further insight from the High Court on how the Privacy Act might apply to overseas entities in the modern digitally connected environment. KWM is acting on this matter.

In the meantime, it is also notable that the OAIC has been actively building connections with other regulators both within Australia and around the world. This has manifested in joint investigations with the UK Information Commissioner's office (in relation to Clearview AI) and more recently with the NZ Office of the privacy Commissioner (in relation to the Latitude data breach). The OAIC has actively engaged in international working groups, and signed formal MOUs with regulators in Ireland, the UK and Singapore. Most recently, the OAIC joined 11 other international data protection and privacy regulators in a joint statement (see here) encouraging action on 'data scraping' on social media and other public websites. This clearly reflects the OAIC's view that effective enforcement of privacy laws requires international cooperation, given the global nature of many online businesses. In the future, we expect to see more of this kind of coordinated international action in addition to direct enforcement against businesses in Australia.

THE WAY FORWARD

As noted above, there will be further consultation on whether further adjustments are required to the "Australian link" test under the Privacy Act.

In the Privacy Act Review Report, the Attorney-General's Department suggested that there should be a requirement that the conduct in question be "connected to Australia" though the precise circumstances in which such a connection could be established are unclear. If this phrase is given its ordinary meaning, it could involve consideration of whether information is collected or held in Australia (as was the case before the recent changes) or whether the information relates to Australian citizens, or to individuals who are based in Australia (something that a service provider may not always be able to easily discern or control, given the borderless nature of the internet).

An illustrative contrast is the position in the NZ Privacy Act 2020, which applies to any action taken "*in the course of carrying on business in New Zealand in respect of personal information collected or held*" by an overseas entity.

Rather than establish the link by reference to the location of the individuals, or where the personal information was held or collected, the relevant jurisdictional link is established by whether the relevant action was "in the course of" the business being carried on in NZ. It is possible, although entirely speculative, that a Court could read a similar qualification into the current carrying on business test in Australia. Regardless, it shows the range of possible approaches that could be considered to strike the right balance.

Ultimately, we will hopefully see a growing trend towards global harmonisation as domestic privacy laws around the world are reviewed are updated. In that way, while jurisdictional challenges may never be eliminated, organisations will be able to operate with greater confidence, knowing that a compliance approach designed in one jurisdiction is more likely to also be adequate for ensuring compliance in other similar jurisdictions.

CLEARVIEW AI INC AND AUSTRALIAN INFORMATION COMMISSIONER [2023] AATA 1069 (8 MAY 2023)

The AAT has determined that Clearview AI was bound by, and breached, the Australian Privacy Act in relation to the provision of facial recognition software to law enforcement agencies.

The requisite Australian link was established by Clearview AI scraping images from servers in Australia, which amounted to Clearview AI carrying on business in Australia. The AAT found that Clearview AI breached the Privacy Act by not obtaining consent from individuals depicted in the scraped images. However, the AAT declined to find other breaches that had been alleged and made some comments that may cause some concern from the OAIC's perspective, including expressing doubts that a photo of a person's face without any further context to identify the person is personal information, that scraping information from a public website isn't necessarily 'unfair', and that when collecting information about a large number of individuals via a third party source it may be reasonable to proceed without notifying the individuals in question.

Background

Clearview AI provides facial recognition software to law enforcement agencies to assist in the identification and location of victims and suspects in criminal investigations.

Clearview AI's software operates through the use of 'web-crawlers' to collect information that has been published on the internet and transmits that information to Clearview's servers. The information collected consists of images of individuals (and related metadata) uploaded to websites that do not require a password or any security or firewall to be passed. These images are saved to an 'Image Library' and to a 'Vector Database' in a machine-readable form. The Vector Database can then be compared against similar vectors generated from a 'probe' image uploaded by a customer of Clearview AI in order to identify any matches against the Image Library – this in turn will help to identify the person who is depicted in the probe image.

Clearview AI's services have proven controversial and sparked concerns from a number of civil society groups about increasing levels of surveillance. In January 2020, a New York Times article detailed the capabilities of the Clearview AI system, and some months later the OAIC launched an investigation into Clearview AI's activities in Australia. Clearview AI had previously conducted marketing activities in Australia, including by offering Australian law enforcement agencies free trials of Clearview AI's services while at the same time providing Australian residents with an opt-out facility that allowed them being included in Clearview AI searches. In March 2020, Clearview AI ceased offering and marketing free trials in Australia. Clearview deprecated the opt-out facility for Australian users in 2021.

Relevantly, Clearview AI's servers, on which both the web-crawlers operate and the information collected is stored and processed, are outside of Australia. Clearview AI is based in the US, does not operate an office in Australia and has not generated revenue in Australia.

Determination by the OAIC

On 14 October 2021, the Commissioner determined that, during the period under consideration, Clearview AI had an Australian link and was, therefore, bound by the Privacy Act. The Commissioner also determined that Clearview AI had breached various Australian Privacy Principles, including:

- when Clearview AI collected the images of Australians from the internet;
- when Clearview AI converted those images into a machine readable form;
- when Clearview AI received and stored probe images provided by law enforcement agencies;
- when Clearview AI converted the probe images into machine-readable form; and
- when Clearview AI stored machine-readable form images of Australians seeking to opt out of the Clearview AI system.

Clearview AI appealed this decision to the Administrative Appeals Tribunal on the basis that it is not bound by the Privacy Act as it does not have an Australian link. The AAT considered the test for carrying on business in Australia in relation to both prior and post the 2022 amendments that simplified the threshold for establishing an Australian link. You can read more about the Commissioner's determination in our annual update from last year (see here).

AAT findings on 'Australian link'

The AAT referred to both the Full Court's decision in F*acebook Inc v Australian Information Commissioner* [2022] FCAFC 9 (as discussed) and the previous leading case of *Valve Corporation v Australian Competition and Consumer Commissioner* (2017) 258 FCR 190 (which considered similar issues under the Australian Consumer Law) in considering whether Clearview AI's conduct amounted to carrying on business in Australia. In particular, the AAT noted that a "more expansive analysis" is required when a business is concerned with the monetising of information. In such an instance, although the mere obtaining of information may not appear to be commercial in nature, it is critical to the conduct of the business.

The AAT emphasised that the test in the Privacy Act is *not* whether there has been a carrying of business "using information about Australians", and rejected the idea that merely acquiring images of Australians, or posted by Australians, amounted to carrying on business "in" Australia. The AAT noted that when retrieving an image from a server located outside of Australia, Clearview AI would not have any way of knowing that the image originated from Australia. However, the AAT found that Clearview AI *was* carrying on business when it acquired images from servers located inside Australia, as this involved acts in Australia that were ancillary to transactions which support Clearview AI's business. While the AAT stated the mere collection of data in Australia is not, of itself, sufficient to establish that an entity is carrying on business, Clearview AI's software was found to be entirely dependent on the collection of images from the internet and, therefore, the collection of data was considered to be essential to its business. The AAT found it irrelevant that the collection of information occurred without human agency.

Notably, the AAT held that the effect of the 2022 amendments (as discussed above) means that where an entity is carrying on business in Australia then all personal information collected by the entity is regulated by the Privacy Act, regardless of its geographical source. That finding – a potential unintended effect of recent tinkering with the Australian link test – reinforces the concerns raised before the Senate Legal and Constitutional Affairs Legislation Committee and justifies the Government's commitment to undertake further consultation on this issue.

AAT findings on APP breaches

As a threshold issue, the AAT found that in the context of the Clearview AI system photos of individuals did constitute personal information, as there was sufficient context in order to enable identification. However, the AAT cautioned that a photo without more context to enable the person in the photo to be identified will not necessarily constitute personal information. While this is a relatively orthodox application of principles, it is nonetheless a point on which reasonable minds may differ, and it also highlights significant practical issues for organisations that deal with a large volume of photographs as, based on the AAT's reasoning, whether or not a particular photograph is personal information to which the Privacy Act applies will always be highly context-specific and will depend on what other information is available to identify persons depicted in the photograph.

In summary, the AAT found that Clearview AI:

- *did* breach APP 3.3 in relation to the collection of sensitive information without consent. The fact the photos were used for biometric identification resulted in it constituting sensitive information, and no evidence was provided of consent;
- *did not* breach APP 3.5 in relation to ensuring that information is collected by a lawful and fair means. The AAT was not satisfied that the collection of information that was freely available on the pubic internet could be unfair or unlawful. The AAT did note, however, that this would be different if there were access limitations on the relevant website. Importantly, in relation to whether the information was obtained lawfully, the AAT noted that social media websites had issued cease and desist letters to Clearview AI. The fact that these letters did not result in any legal action was considered to be indicative of the fact that Clearview AI's conduct was not in breach of the conditions of service of those organisations;
- *did not* breach APP 5.1 in relation to the requirement to take reasonable steps to notify individuals of the collection of personal information. The AAT emphasised that APP 5.1 allows for no notification if that is reasonable in the circumstances, and that it would have been practically impossible for Clearview AI to comply where it collected a large volume of information with no personal connection with the subjects. As a matter of policy, this result may be somewhat unsatisfying as it suggests higher volume data collection may result in lower transparency. However, it is nonetheless an insightful illustration of how the current transparency obligations may apply in practice;
- *did not* breach APP 10.2 in relation to the requirement to take reasonable steps to ensure that information is kept accurate, up-to-date, complete and relevant; and
- *did* breach APP 1.2 in relation to the requirement to take reasonable steps to ensure compliance with the APPs. This breach flowed from the AAT's findings that Clearview AI had breached APP 3.3. While a relatively minor point, the ease with which a breach of APP 1.2 can be supported where there is another breach (as demonstrated here) may mean that we see the OAIC allege breaches of this provision more often in future.

WHAT IS NEXT

The Clearview AI saga is not finished just yet. In the final paragraph of the decision, the AAT notes: "*Whether declarations in light of these findings should be made under section 52 of the Privacy Act is a matter which will be considered at a separate hearing. Until that question is resolved I will not issue a formal review decision in relation to the determination of the Privacy Commissioner.*" Accordingly, 'it is still up in the air as to what orders should be made against Clearview AI, based on the AAT's findings as to the breaches that took place. Many interested observers in the privacy world will be watching closely for what happens next.

AUSTRALIAN COMPETITION AND CONSUMER COMMISSION V GOOGLE LLC (NO 2) [2022] FCA 1476

In late 2022, the Federal Court dismissed an application by the ACCC against tech giant Google, for an alleged contravention of the Australian Consumer Law. The ACCC alleged that Google engaged in misleading and deceptive conduct and made misleading representations, by utilising on-screen notifications to inform its account holders of modifications to its privacy policy and to obtain their consent regarding changes to their account settings and use of personal information. While the case was dismissed, this illustrates the importance of carefully communicating any material privacy changes to existing users, without assuming that all of them will read all of the information made available.

Background

Between June 2016 and December 2018, Google deployed a global project known as "Project Narnia 2.0" seeking to improve the delivery of ads and services provided by Google. Fundamentally, the purpose of Project Narnia was to expand the use of account-based targeted advertising to Google partner websites and apps, by taking into consideration data from a user's activity on Google services, third party websites and third-party apps in association with personal information from the user's Google account.

The ACCC alleged that Google contravened the ACL by issuing a notification about the changes to support Project Narnia 2.0 that was misleading or deceptive in design, and that failed to adequately inform users as to how their personal information would be combined and used to serve more targeted advertisements. The ACCC also contended that Google reduced the rights of its users under Google's privacy policy by making various changes without their explicit consent.

To agree or not to agree – was Google's conduct and representations misleading or deceptive?

In implementing Project Narnia, Google sought the explicit consent of its account holders through an on-screen display notification. If the account holder selected 'I AGREE', then they were taken by Google to have accepted the changes and accompanying account settings.

A key argument advanced by the ACCC was that Google crafted the notification in a deceptive way in order to maximise the number of users who clicked 'I AGREE', rather than to maximise the number of users who properly *understood* the implications of what they were agreeing to. In particular, the ACCC argued that Google presented the proposed changes to its processes and policies as beneficial for account holders without also referring to the fact that the proposed changes were commercially beneficial for Google as well. The Court did not find this argument relevant to the question at hand, on the basis that it was not necessary for Google to notify account holders of any benefit Google might experience. Rather, the question was whether Google failed to inform, or adequately inform, account holders that it was seeking their consent to undertake the information processing activities described in the updated policy.

The ACCC also alleged that Google breached the ACL by representing it would not reduce an account holder's rights under the privacy policy without obtaining their explicit consent. Specifically the policy stated that "*We will not reduce your rights under this privacy policy without your explicit consent*". The ACCC claimed that Google did in fact reduce the rights of account holders by deleting the commitment by Google not to combine certain cookie information with personally identifiable information and making various changes without the account holder's consent.

Ultimately, the Federal Court rejected the ACCC's arguments and dismissed the application. The Court was satisfied that Google account holders, acting reasonably in their own interests, would have understood (by reading and viewing the diagrams included in the notification) the changes Google proposed to make and what they were agreeing to. The Court was also satisfied that Google did not reduce the rights that account holders had under Google's privacy policy, as while the wording of the policy changed the substantive position remained largely the same as Google would still need the customer's consent for the new processing activities. Google actively sought consent by inviting customers to click 'I AGREE'. Only when Google received the explicit consent of its account holders, did give effect to the changes contemplated in the notice.

Importantly, the Court said that the policy updates should not be seen as isolated text, but should be read with the added context of the notification mechanism, and whether account holders accepted the proposed changes. It noted that Google had designed its notifications for a range of different users including those it classified as "Skippers, Skimmers and Readers". The notifications were designed in layers, with the top layer containing all essential information, but with links provided for those who wanted to go into more depth. Critically, in this case the Court found that the first page of the notification was, even when taken alone, not misleading and provided an adequate level of transparency to enable users to understand the nature and scope of the changes.

KEY TAKEAWAYS

- As our regular readers would know, there has been increasing overlap in the Venn diagram of privacy and consumer law in recent years. In our 2020 annual update (see here) we highlighted how organisations dealing with consumer data and personal information may now be faced with regulatory action on multiple fronts, as the jurisdiction of the ACCC and the OAIC on privacy matters continues to blur. While this case was primarily a consumer law case, brought by the ACCC, it has important ramifications for approaches to privacy policies and privacy consents, which will also be relevant under the Privacy Act.
- To ensure compliance with applicable transparency obligations, careful attention must be paid to the user experience when designing privacy-related notifications. In particular, it is critical to consider the information presented to users on the first page or screen of a notification, as there can be no assumption that users will scroll or click on links to access all further details (even though a "layering" approach has been endorsed in the past by the OAIC and other regulators as a way of addressing privacy transparency obligations). Typical user behaviour must be taken into account, including in relation to those who may wish to skip or skim through online process flows, in order to ensure that the message is appropriately comprehensible. This is a particularly challenging proposition where many complex or material changes are being bundled together and cannot easily be reduced to a single page.

HYYL AND PRIVACY COMMISSIONER [2023] AATA 2961 (13 SEPTEMBER 2023)

The AAT has found that the Commissioner can only order compensation for the actual loss or damage suffered by an individual that results from the relevant interference with their privacy. The fact that an individual has had their privacy interfered with is not by itself a recognised, or compensable, form of loss or damage. Therefore, where a group of individuals have had their privacy interfered with, compensation can only be ordered in relation to the individuals who can establish that they personally suffered some form of loss or damage.

Background

On 11 January 2021, the Commissioner made a determination under s 52 of the Privacy Act that the Secretary to the Department of Home Affairs had interfered with the privacy of individuals in immigration detention in breach of the Privacy Act. The breach occurred when the Department published a document on its website with an embedded spreadsheet that contained the personal information of approximately 9,258 individuals in detention. The spreadsheet was accessible for 17 days and detailed the full name, gender, citizenship, date of birth, immigration details and detention details of the affected individuals.

The determination required that the Department pay compensation for loss or damage incurred by affected individuals who had provided submissions and/or evidence of loss or damage. Compensation was to be assessed on a case-by-case basis. The Commissioner directed the Department to send a notice to relevant individuals that informed them of the breach and set out the process by which they could establish eligibility for compensation. The notice required that the relevant individuals provide the Department with submissions and/or evidence of loss or damage within a stipulated timeframe. In total, 2,579 individuals registered their interest, and 1,297 individuals ultimately provided submissions and/or evidence of loss or damage. You can read more about the Commissioner's determination in our 2021 update (see here).

One of the affected individuals, HYYL, appealed the Commissioner's determination on behalf of all the affected individuals, including as to the appropriateness of the compensation scheme established under the determination.

Loss or damage must be established to order compensation under s 52

There was no dispute that the Commissioner has the power to determine that a scheme be established to assess the amount of compensation payable to affected individuals. However, the AAT found that the Commissioner can only order compensation where an individual has established that they have personally suffered actual loss or damage that is causally connected to the breach. In doing so, the AAT found that:

- the Commissioner is not empowered to order that a base sum be paid for "common" loss or damage suffered by affected individuals; and
- there is no Australian authority which supports the contention that "right to privacy is a substantive right" and that any impairment of that right constitutes a form of loss or damage.

Applicable principles for determining compensation

The AAT agreed with previous AAT decisions that the following general principles are relevant to the calculation of compensation under the Privacy Act:

- where a complaint has been substantiated and loss or damage has been suffered, the Privacy Act contemplates that some form of redress should be ordered;
- compensable forms of loss or damage include injury to feelings, distress and humiliation; however, it does not include feelings of anger, outrage or injustice alone as they cannot be characterised as an injury or as damage;
- awards should be restrained but not minimal;
- tortious principles of damages can assist in measuring compensation, but statutory construction of the Privacy Act is the paramount consideration;
- aggravated damages may be awarded, if appropriate; and
- compensation is to be assessed in light of the complainant's subjective reaction to the breach, not against the objective reaction of the community or a reasonable person in similar circumstances.

Relevance of factual circumstances and external factors in assessing compensation

In considering the particular circumstances of this case, for the purposes of assessing the appropriateness of the compensation scheme established by the Commissioner, the AAT also said that:

- although the seriousness of the breach must be considered, the following factors weighed in favour of restraint in the award of compensation:
  - that the information disclosed was only basic identification information and did not include the details of any individual protection claim;
  - that the accessibility of the information was limited as it was embedded in a published document and was only viewable if specific steps were taken;
  - that the data breach was inadvertent and the result of human error;
  - that the information was only accessible for a limited period; and
  - that steps were taken to remove the information shortly after being notified of the breach;
- the compensation scheme should be broadly consistent with previous awards under the Privacy Act;
- compensation awards by other Australian agencies or overseas governments cannot be used as a guide for an award under the Privacy Act as any award must consider the unique factual context of the privacy breach; and
- compensation under s 52 is strictly compensatory and cannot be made with reference to increasing public awareness of privacy issues.

Defining categories of non-economic loss for purposes of calculating compensation

Having found that it was not appropriate to award a base level of compensation for all affected individuals, the AAT broadly agreed with the approach taken by the Commissioner of defining different categories of individuals that had suffered non-economic loss (six in total), with an indicative range of compensation for each category, with each individual then able to provide evidence as to the category they fall into and the amount of compensation to which they should be entitled. In doing so, the AAT said that:

- a compensation range provides flexibility to adapt the quantum to the individual Class Member's circumstances – in other words, there is a strong preference for individualised assessment, rather than fixed amounts for individuals whose circumstances fall within a defined category;
- more detailed descriptions of each category will provide greater guidance and promote transparency about the Commissioner's approach to ordering compensation; and
- more detailed explanations assist in ensuring that the categories can be more easily understood.

Comments on the decision's significance

This is an important decision, as it concerns the first time the Commissioner awarded compensation for non-economic loss in a representative action. While AAT decisions are not binding on the Courts, the Commissioner will need to have regard to the AAT's comments in future determinations to avoid further review applications.

In particular, the AAT's decision illustrates the complexity of awarding compensation in relation to major privacy breaches that affect a large group of individuals. In many cases, due to their own unique circumstances, different individuals will be impacted by the breach in very different ways. The need to assess loss or damage on an individual basis, including through consideration of subjective reactions, and to draw potentially fine distinctions between the level of emotional injury that may have been suffered, will inevitably prove costly and time consuming.

The AAT's determination requires the Department of Finance to appoint an independent law firm to act as the scheme assessor (at the Commonwealth government's expense), rather than the law firm that pursued the appeal on behalf of the representative (who acted pro-bono) or the law firm that represented the Department. A similar approach is unlikely to be feasible in the context of settlement of a class action in court proceedings in a case that does not involve the Commonwealth government – the prevailing practice in non-privacy class actions is for the cost of the assessment to be deducted from the overall settlement sum or award of damages and the court scrutinises the expense of administering the settlement distribution scheme.

In any event, what is clear is that the process of obtaining relief in relation to a major breach such as this one is likely to be long and tortuous. In this particular instance, the breach occurred in 2014 and almost a decade later the administrative process of assessing loss and damage and paying compensation is still underway. That is unlikely to be a satisfactory outcome for any of the parties involved.

YOU CAN'T SPELL 'PRIVACY' WITHOUT A AND I

Law-makers and regulators around the world are grappling with the best way to mitigate privacy-related risks associated with generative AI technologies. There are concerns about transparency, the lawfulness of collecting training data, information security, individual opt-out controls, and more. We have identified a range of developments from the past year which illustrate the issues in play.

Artificial intelligence has been the hottest of hot topics this year, with commentators falling over one another to make predictions about the massive impact that AI will have on every aspect of our future lives. Without attempting to cover the field, we have highlighted below a few key developments from the past year that demonstrate the significant privacy-related implications of this burgeoning technology.

AI a focus in Privacy Act reforms

The Government has committed to progress a number of AI-related reform proposals set out in the Attorney-General Department's Privacy Act Review Report.

In particular, the Government has agreed that privacy policies should set out the types of personal information that will be used in 'substantially automated decisions which have a legal, or similarly significant effect on an individual's rights'. For example, this may include situations where personal information is used to make access-related decisions on lending, housing, insurance or employment. However, given that today AI technology often still operates in tandem with human decision-makers, further clarity will be required as to what constitutes a 'substantially' automated decision.

The Government has also agreed that individuals should have a right to request 'meaningful information' about how these types of automated decisions are made. This aligns with the results of the OAIC's recent Australian Community Attitudes to Privacy Survey 2023 (see here), in which:

96%

of respondents wanted condition in place before organisations use AI to make decisions that might affect them

69%

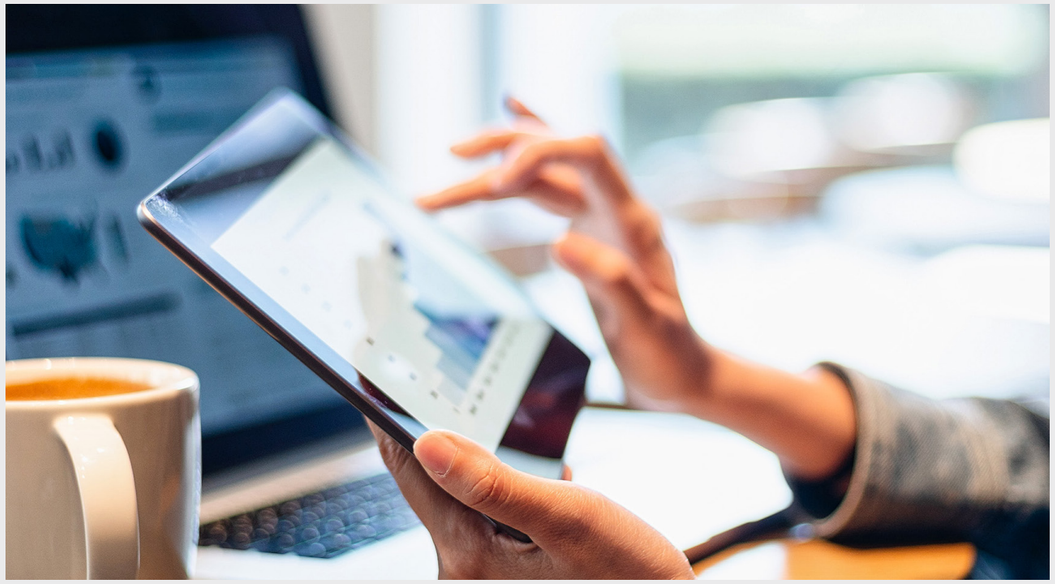
wanting organisations using AI to be bound by strict privacy rules and

68%

wanting a right to request information about how AI decisions are made

While industry will take some comfort from the fact that the Government has also indicated that this should not require businesses to disclose commercially sensitive information, there will need to be careful consideration about what information can be provided to provide an acceptable level of transparency when the exact operation of some self-teaching neural networks used to power AI systems may not be 'knowable' even by their human designers. There is also a risk that explanations will become over-simplified and lose their essential meaning in the effort to make them comprehensible for the average consumer.

Nonetheless, it is encouraging to see privacy reforms progressing in tandem with consideration by Government of the regulation of AI technologies more broadly. For example, issues around privacy were a key them of the recent Supporting Responsible AI in Australia led by the Department of Industry, Science and Resources (see here) and the need for AI systems to 'respect and uphold privacy rights' has baked into the (non-binding) AI Ethics Principles developed by the Department to ensure AI is safe, secure and reliable (see here). Maintaining overall regulatory cohesion will be important to ensure that there is a stable regulatory environment within which AI operators can continue to innovate.



Privacy in AI training materials

Generative AI models must be 'trained' on vast amounts of input data, whether that be words or images. A key concern for many privacy advocates is whether AI models may be trained on data that is personal information and, if so, whether such data has been obtained lawfully and fairly in a way that ensures the individuals in question retain an appropriate level of control over their information.

Concerns in this regard have been highlighted in the several proposed privacy-related class actions that Google and OpenAI (the organisation behind ChatGPT) are facing in relation to data scraped from the web for AI training purposes (see here). In each of the cases, complainants suggested that unauthorised scraping of information from public websites had interfered with various privacy rights in the United States.

We have already seen similar concerns raised in Australia, most notably in relation to Clearview AI's facial recognition software, as discussed above, and through the OAIC joining with 11 other international data protection and privacy regulators to make a statement addressing the issue of data scraping from social media platforms and other publicly accessible sites (see here). The joint statement notes that in most jurisdictions, privacy obligations will generally apply to personal information irrespective of whether it is publicly accessible (though it's worth noting that exceptions may apply in Australia for information contained in 'generally available publication'). The regulation of information placed in the 'public domain' raises some complex policy issues, which Governments and regulators will need to properly engage with sooner rather than later.

ChatGPT banned (and then unbanned) in Italy

Italy's data protection authority (the **Garante**) made headlines blocking ChatGPT in March this year. In doing so, the Garante said there was no basis to justify the mass collection and storage of personal data for the purpose of training algorithms. Interestingly, the Garante also raised concerns about the use of ChatGPT by children, including the risk that they could be exposed to 'unsuitable' responses, which is perhaps not strictly a privacy-related concern.

In any event, the Garante lifted the ban after just a couple of months, with OpenAI agreeing to take a number of steps to address the Garante's concerns, including offering a tool to verify the age of Italian users upon sign-up, to provide greater visibility of its privacy policy, and to provide EU users with new ways to object to the inclusion of their information in training data.

This brief but dramatic episode illustrates the genuine concerns that some regulators hold about this type of technology, and the importance of companies adopting a privacy-by-design approach to any AI-powered products and services, in order to avoid regulatory hiccups.

Privacy risks in the NIST framework

In the US, the National Institute of Standards and Technology (NIST), an agency of the Department of Commerce whose mission is to promote US innovation and industrial competitiveness, has developed a new risk management framework for AI (see here). While focussed on the US, NIST frameworks and standards are highly influential globally, and the new risk management framework will be particularly for the key AI players, as many of them are based in the US alongside other 'big tech' companies.

Although the NIST framework is not solely focused on privacy, it does devote one of its seven sections on AI risks and trustworthiness to privacy. In particular, the framework notes that 'Privacy values such as anonymity, confidentiality, and control generally should guide choices for AI system design, development, and deployment'. The framework also highlights that 'AI systems can also present new risks to privacy by allowing inference to identify individuals or previously private information about individuals'.

While legislators are still grappling with whether or how to pass targeted legislation dealing with AI technologies, standards and rules like those propagated by NIST will serve as a useful benchmark, and will help to manage systemic risks and promote consumer confidence.

The FTC comes for OpenAI

Finally, in what is shaping up to be the most significant legal action to date against the leading provider in the nascent AI industry, the US Federal Trade Commission has opened an investigation into OpenAI, with data protection issues as a key focus. As reported by a range of media outlets in July, the FTC sent OpenAI a 20-page 'civil investigative demand' with dozens of questions on collection, use and retention of data, including for training and quality testing (see here).

In some ways, the investigation is unsurprising given the rapid uptake of ChatGPT – now used by hundreds of millions of people – and the FTC's recent history of pursuing privacy and data-related cases relating to US tech companies. The FTC has commented that misuse of private information in AI training could be a form of fraud or deceptive practice. The FTC has had some success in regulation of consumer privacy issues in the US, so this investigation will be interesting to watch over the coming year, and will serve as an important reference for other AI providers that have undertaken similar information gathering activities.

A LOOK INTO CHINA'S SCC APPROACH AND THE LATEST REGULATORY DEVELOPMENT TO EASE CROSS-BORDER DATA COMPLIANCE BURDENS

The Cyberspace Administration of China has released new draft provisions that aim to streamline the process for transferring personal information out of China, including through the use of Standard Contractual Clauses. It is essential for any multi-national organisation doing business in China to understand relevant cross-border transfer rules, which are complex, in order to ensure either that they have the benefit of an exemption or that the right structures are in place to support any flow of data outside China.

China's Personal Information Protection Law ("**PIPL**") prescribes three mechanisms for exports of personal information from China by personal information processors ("**Handlers**"): (1) passing a government-led Security Assessment, which is mandatorily required for critical information infrastructure operators ("**CIIO**") as well as Handlers that process personal information above a prescribed threshold volume; (2) attaining a personal information protection Certification by government designated institutions; and (3) concluding a data processing agreement containing the Standard Contract Clauses ("**SCC**") with the overseas recipient. Among these three mechanism, the Standard Contract Clauses approach ("**SCC Approach**") is considered to be relatively more convenient for many multinational companies in China as it involves less government interaction. The key points and practical takeaways to note for the SCC Approach are set forth below.

Legal basis for the SCC Approach

The SCC Approach operates under the following legal instruments:

- The *Measures on the Standard Contract for Outbound Transfer of Personal Information* ("**SCC Measures**") issued by the Cyberspace Administration of China ("**CAC**") on 22 February 2023. The SCC Measures took effect on 1 June 2023 and provide for a six month grace period for compliance, ending on 30 November 2023. The SCC Measures require Handlers to file the SCCs with the CAC bureau at the provincial level along with a personal information protection impact assessment ("**PIPIA**") and relevant formality documents within 10 business days of executing the SCCs.
- The *Guideline on SCC Filing* ("**Guideline**") issued by the CAC on 30 May 2023, which provides detailed filing procedures and templates for the PIPIA and the formality documents.

In addition to the above, on 28 September 2023, the CAC released a *Draft Provisions on Regulating and Promoting Cross-border Data Flows* seeking for public comment ("**Draft Provisions**"). The Draft Provisions whitelisted certain personal information export scenarios as further discussed below that are exempted from complying with the cross-border transfer restrictions. The Draft Provisions are promulgated in the context of the Chinese government's attempt to reverse the nation's foreign investment slump, as the previous regulatory regime is said to impose a much too heavy data compliance burden on international businesses. There is no reason to believe that the CAC will significantly change its position on the draft, which is likely to be finalized before December 2023.

Who is eligible to adopt the SCC Approach?

The SCC Approach is only available for outbound transfers of personal information by non-CIIO Handlers that are below the government-prescribed threshold volume. In particular, a Handler seeking to take the SCC Approach must not: (1) process personal information of more than 1 million individuals; or (2) cumulatively transfer personal information of more than 100,000 individuals or sensitive personal information[1] of more than 10,000 individuals to overseas recipients since 1 January of the previous year (which means that the outbound transfer volume will be calculated for a period of up to two years starting from 1 January of last calendar year on a rolling basis). The above thresholds are calculated on a per-entity basis, taking into account all the outbound data transfer scenarios that an entity may face in its ordinary course of business.

In practice, Handlers often ask whether they can take the SCC approach if their accumulative transfer volume reaches the threshold only during the last few months of a given year. A strict interpretation of the PIPL requires Handlers who meet the threshold volume to transfer personal information abroad only after completion of a Security Assessment. We note that in practice, some local CAC bureaus are comfortable with Handlers only commencing the preparation for the Security Assessment after reaching the threshold, while some are not. As the application of the Security Assessment usually takes months, Handlers should closely monitor and predict their likely outbound transfer volume so that they can apply for the Security Assessment in a timely manner once the volume is expected to exceed the threshold, and in doing so avoid the risk of having to suspend any information transfer.

1 *Sensitive personal information refers to personal information which once disclosed or unlawfully used, may easily lead to damage of a natural person's dignity, personal safety, or property safety, which includes information regarding biological identification, religious belief, specific identities, medical care and health, financial accounts, whereabouts and tracks, and the PI of minors under the age of 14.*

Whitelisted personal information export scenarios that are exempted from adopting a cross-border data transfer mechanism under the Draft Provisions

According to the Draft Provisions, Handlers are exempted from adopting a cross-border data transfer mechanism (including the SCC Approach) under the following personal information export scenarios:

- **Transfer of personal information not collected or generated from PRC:** This may mean that Handlers who do not have a business presence and who do not use servers in China and who only collect personal information of individuals located within China via the Internet on a cross-border basis will be exempted. If not for the Draft Provisions, such Handlers could be subject to the cross-border transfer restrictions under the PIPL by virtue of its extra-territorial application clause.
- **Transfer of personal information necessary to perform contracts entered into by data subjects:** Handlers will be exempted when transfers of personal information are necessary for providing international services to data subjects on a contractual basis, such as cross-border e-commerce services, cross-border payment services, air tickets and hotel reservation services, and visa application services. As such service providers normally have a large customer base and are easily captured by the Security Assessment requirement, this change, if finally introduced, will significantly ease the burden on B2C service providers.
- **Transfer of personal information necessary for HR management:** Transfers of employee data as necessary for implementing human resource management in accordance with legally executed labour contracts are also exempted. If the Draft Provisions were adopted as they are, multi-national companies would be free to transfer HR data of employees in China to their overseas headquarters for HR management purposes without having to go through the SCC filing.
- **Transfer of personal information of less than 10,000 individuals involved:** If the expected outbound transfer of personal information involves less than 10,000 individuals within one year, the transfer mechanisms will not apply. Under this exemption, transfers of personal information of contact persons of business partners, vendors and enterprise customers as well as personal information of individual customers, job applicants, etc could all be exempted from the cross-border transfer mechanisms, as long as the number of data subjects concerned is expected to be less than 10,000 for a given year. Many small and medium enterprises could rely on this exemption to avoid regulatory burden on their cross-border data transfer activities.
- **Transfer of personal information for vital interest under emergency cases:** Outbound transfer of personal information necessary to protect the life, health and property safety of the data subject under emergency circumstances is also exempted.

Entities in the process of preparing the SCC filing should assess whether their outbound transfer activities fall within the whitelisted scenarios under the Draft Provisions. If exempted under the Draft Provisions, entities could suspend this activity and wait for the finalization of the Draft Provisions, as we do not believe the CAC will significantly change its position. For entities who are exempted under the Draft Provisions and who have already submitted the SCC filing and are pending for the CAC's review, we suggest contact the CAC to see whether the filing could be withdrawn.

KEY TAKEAWAYS IN PREPARING THE SCC FILING

Additional terms needed for P2P and P2C transfers

The CAC only provides a single SCC template that applies universally to all of the personal information transfer scenarios between a "Personal Information Handler" (which is defined as the entity that can determine the processing purpose and method on its own, equivalent to "Controller" under GDPR) and an "Overseas Recipient" (which is not defined). Based on the terms in the SCC, it is obvious that the SCC template applies to the transfer scenarios between Controllers and Controllers (C2C) and Controllers and Processors (C2P), to use the terminology of GDPR. Therefore, it should be noted that the SCC template is not suitable for addressing the "Processor to Processor" (P2P) and "Processor to Controller" (P2C) data transfer scenarios. While the SCC Measures do not allow parties to the data processing agreement to modify any of the terms in the SCC, parties are permitted to add additional terms governing their data transfer relationships as an appendix to the SCC as long as those terms do not conflict with the terms in the SCC. Therefore, entities dealing with P2P or P2C transfer scenarios may need to add additional terms governing the particular data transfers in preparing the SCC.

Obligations Imposed on Overseas Recipients

The SCC require the Overseas Recipient to agree to be subject to the supervision and management of the PRC authorities. As a consequence, the Overseas Recipient may need to respond to inquiries from the competent authorities in the PRC, cooperate with relevant investigations, implement orders of the regulators and provide evidence to show compliance, etc.

In addition, the SCC also imposes strict obligations on the Overseas Recipient's onward transfer of personal information to other third parties that are located outside of PRC and holds the Overseas Recipient responsible for any personal information protection matters arising from any such onward transfers. These requirements include: notifying data subjects of the details of how the third party will be processing his/her personal information (such as the processing purpose, method and types of personal information being processed) and the contact information of the third party, as well as obtaining separate consent for such transfer (if the personal information is processed based on the consent of the data subject). In practice, as the Handler will be facing the data subjects, such notification and consent requirements will normally be fulfilled by the Handler.

In light of the above obligations, to the extent that an Overseas Recipient will need assistance from the Handler in order to comply with the SCC, they would be well advised to reach a separate agreement with the Handler on these issues. Similarly, the Overseas Recipient should execute written agreements with the third parties to which it will be transferring the personal information to ensure that such third parties adopt personal information protection measures no less than that required by the PIPL.

Preparation of the PIPIA

Before submitting the SCC filing, the Handler must prepare a PIPIA, which should include the following details regarding the transfer:

- basic information on the Handler ,such as the type of organization and the equity structure, including whether it is a domestic or foreign investment entity;
- the information systems used to collect and export the data, including the use of data centres in the process;
- the personal information to be transferred with a detailed breakdown of purpose, necessity, sensitivity, legality, use of automatic decision making and the location where the data will be stored by the Overseas Recipient;
- the ability of the Handler to protect the data, including technical, management and training for handling, emergency response and compliance;
- the Overseas Recipient's use of the data, ability to protect and details of the information protection in its country/region; and
- an impact assessment for each of the items to be exported, including potential risks.

Timeline of the SCC filing procedure

Companies who choose to adopt the SCC Approach must submit the SCC along with the relevant filing materials to the provincial CAC bureau where it is registered within 10 business days of the execution of the SCC. Upon receipt of the filing submission, the provincial CAC bureau will review the materials and notify the applicant within 15 business days on whether the Handler has passed its review. If a Handler does not pass the review, the Handler can submit supplemental materials or correct the submitted materials within 10 business days upon notification.

Focus of the provincial CAC's review of the SCC filing

Although the SCC filing review of the provincial CAC bureau will not be as strict as the review under the Security Assessment, it is expected that the review of the SCC filing by provincial CAC bureaus will go beyond the formalities of the materials. In practice, the provincial CAC bureau will look at whether (1) the Handler should be subject to the Security Assessment instead of taking the SCC Approach for its data export activities; (2) the tailored terms additionally agreed upon by the Handler and the Overseas Recipient conflict with the terms of the SCC; and (3) the PIPA sets out sufficient details of the outbound transfer.

Update or submit a new filing

Handlers shall submit a new filing (including conducting a new PIPIA and updating or entering into a new SCC) where there is: (1) any change to the purpose, scope, method of the outbound transfer, ***or*** the type, sensitivity or storage location of personal information transferred aboard, ***or*** the Overseas Recipient's processing purpose and method, ***or*** there is an extension of the overseas retention period of the personal information; (2) any change to personal information protection policies and regulations in the country or region where Overseas Recipient is located, which may affect the rights and interests of the data subjects concerned; or (3) other circumstance that may affect the rights and interests of the data subjects concerned.

One SCC filing for one entity?

Multinational companies operating in China usually have multiple affiliates across China that share the same or similar type of business needs to transfer personal information overseas. It would be time-consuming and costly if such affiliates must enter into separate SCCs with each Overseas Recipient and prepare separate SCC filings for each separate SCC. We consider that the best way to approach this problem is to choose a "hub" among the domestic entities as the "Handler" under the SCC and a "hub" among the foreign entities who receive the personal information as the "Overseas Recipient", and have all data transfer activities be carried out between these two "hubs". In this way, only one SCC needs to be executed between the "hubs" and only one filing is needed for that SCC.

If the above approach is impracticable for some companies or when there are multiple Overseas Recipient of personal information involved, the CAC at the central level tends to require signing separate SCCs with each and every Overseas Recipient and prepare separate PIPIAs for such transfers. However, as the SCC filing is subject to the review of the provincial CAC bureaus, the standard may differ depending on each provincial CAC bureau's determination. For example, when there are multiple outbound transfer scenarios between one Handler and one Overseas Recipient, some provincial CAC bureaus require multiple SCCs/PIPIAs/filing while others consider that it can be combined in one SCC/PIPIA/filing. In addition, when there are multiple affiliated Handlers involved, some provincial CAC bureaus allow the affiliated branches to file a combined SCC filing, but still require the execution/preparation of separate SCCs/PIPIAs.

Given the huge difference in the practice of different provincial CAC bureaus, companies are advised to consult with the competent CAC bureau or a legal expert first before preparing the SCC filing so as to save time and cost.

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

PATRICK GUNNING
PARTNER
SYDNEY
TEL +61 2 9296 2170
MOB +65 418 297 018
EMAIL patrick.gunning@au.kwm.com

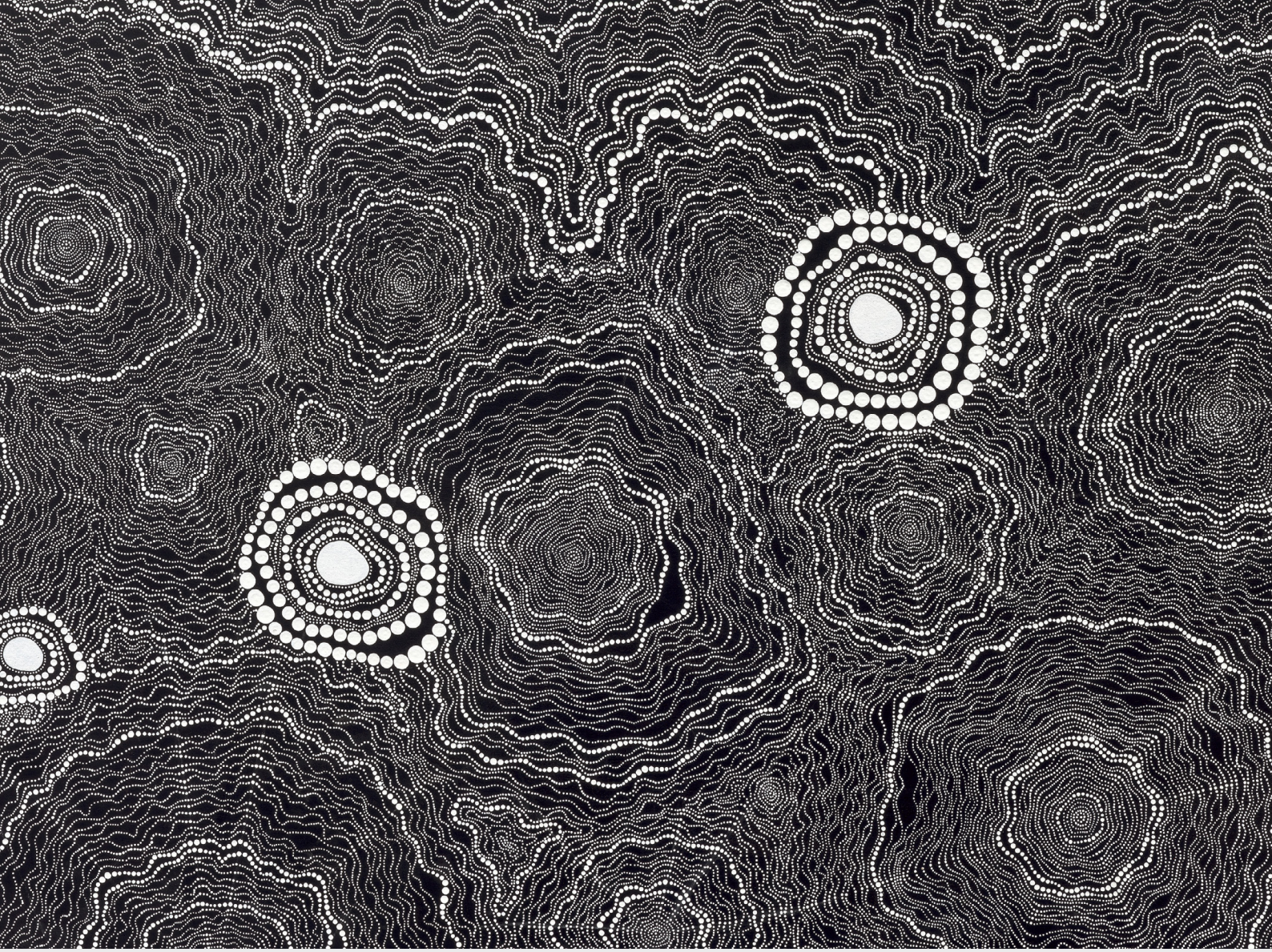
SU CHANG
PARTNER
BEIJING
TEL +86 10 5878 5588
EMAIL suchang@cn.kwm.com

Editor

CAL SAMSON
SENIOR ASSOCIATE
MELBOURNE
TEL +61 3 9643 4166
MOB +65 437 652 995
EMAIL cal.samson@au.kwm.com

Additional contributions & Acknowledgements

Michael Swinson, Luke Hawthorne, Eimear O'Sullivan, Kai Nash, Cal Samson. Su Chang, Jiang Minru



ABOUT KING & WOOD MALLESONS

A firm born in Asia, underpinned by world class capability. With over 3000 lawyers in 31 global locations, we draw from our Western and Eastern perspectives to deliver incisive counsel.

With 31 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