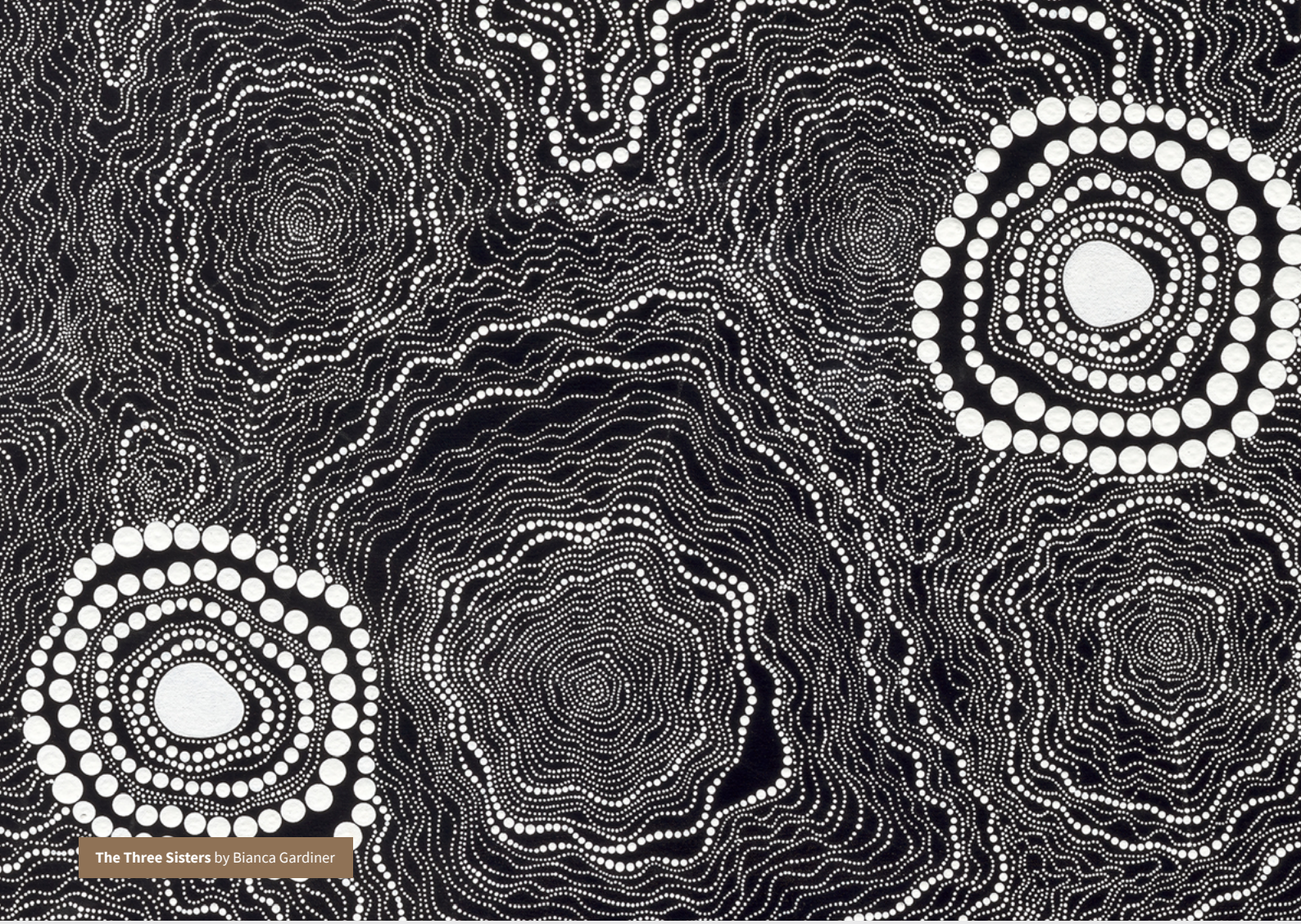


The Three Sisters by Bianca Gardiner

PRIVACY LAW ANNUAL UPDATE

2025

KING&WOOD MALLESONS
金杜律师事务所

INTRODUCTION

Welcome to the 2025 edition of KWM's annual privacy law update.

It's been another busy year in our favourite corner of the legal world. Indeed, from the first tranche of long-awaited Privacy Act reforms, the commencement of a new statutory tort for serious invasions of privacy, new rulings from the Privacy Commissioner on the use of facial recognition technology, consultation on additional protection for children's privacy, the imminent commencement of new social media minimum age laws (along with all of the complex privacy challenges that age verification presents) and the unavoidable shadow of AI across everything … it's hard to think of a more significant year in the world of privacy law. Until next year, of course!

As ever, if you have any questions on anything we cover in this edition, or on the particular implications for your organisation and any actions you should be taking, our team of privacy law experts (read: privacy fanatics) at KWM is always happy to chat. Our contact details are at the end of this document if you would like to reach out.

CONTENTS

ARE WE THERE YET? WHERE TO FROM HERE FOR PRIVACY LAW REFORMS

2025 has been a year of fitful progress down the long and occasionally bumpy road of privacy law reform in Australia.

There have been some notable changes, such as the commencement of the new statutory tort for serious invasions of privacy. The Office of the Australian Information Commissioner (**OAIC**) has also kicked off the process for developing the new children's online privacy code, which must be in place by the end of 2026. Our longer articles below provide more detail on these key developments.

Many organisations are also taking action to comply with additional transparency requirements around use of personal information for automated decision making. Even though these requirements don't take effect until December 2026, many organisations will need this lead time to properly audit the ways in which personal information is being used to power various complex decision making processes and to consider their approach to building automated decision making disclosures into their privacy policies.

However, there is still no obvious pathway to the next tranche of privacy law reform, which may involve more complex and potentially controversial changes to the law given that the low hanging fruit has already been taken. Attorney-General Michelle Rowland indicated in July this year that the Government is still actively working on reforms, with a possible focus on AI, so the journey is far from over. While the next steps remain unclear, there have been some interesting developments that provide pointers as to what we should expect next.

Testing the limits of the current law

As we noted in last year's annual update, in the absence of substantive reforms, the OAIC has been actively producing guidance on how the current law may apply to controversial practices such as online tracking, facial recognition technology, and use of personal information for training generative AI.

In the last 12 months, the Privacy Commissioner has finalised a number of investigations on use of facial recognition technology that reinforce the expectations set out in the OAIC guidance. We expect to see more of the same in relation to the other priority areas for the OAIC in future.

The Commissioner has clearly indicated that they will continue to issue guidance and exercise its enforcement powers to set expectations as to the Commissioner's views on the current application of the Privacy Act - including in the Commissioner's interview with KWM partners Michael Swinson and Bryony Evans at this year's KWM Digital Future Summit. This should serve as a warning to organisations engaged in conduct, including the implementation of new technologies or involving sensitive information (such as health information), that the Commissioner has identified as being 'high risk' from a privacy perspective. While these are not necessarily 'no go' areas, it is important for organisations to tread carefully. We have summarised further insights from our interview with the Commissioner below.

Predictors of future reform

While federal privacy reforms may have stalled, other changes in law provide clues as to what we may expect in future.

- **Online Safety Act:** *The Online Safety Act 2021* (Cth) (**Online Safety Act**) was amended in December 2024 to include new minimum age restrictions for certain social media platforms, which will come into effect in December 2025. Given privacy concerns prompted by potential wide-scale implementation of age verification processes, there are strict restrictions on use of information collected by social media operators to comply with the regime.

  Most notably, section 63F of the Online Safety Act provides that such information may not be used for other purposes without the relevant user's consent, which must be voluntary, informed, current, specific and unambiguous. The user must also be able to easily withdraw their consent.

  These requirements closely reflect long-standing OAIC guidance on consent. However, the hard-wiring of these requirements in the Online Safety Act may well be a preview as to how new consent standards may be framed in any future amendments under the Privacy Act. Certainly, organisations that rely on consent to support their collection and use of personal information more broadly should keep a close eye on how the requirements of section 63F are enforced in the context of the social media minimum age framework.

- **WA Privacy Act:** Another development which may have flown under the radar for many practitioners was the passage of the *Privacy and Responsible Information Sharing Act 2024* (WA) (**WA Privacy Act**). While it only applies in Western Australia, the WA Privacy Act again provides an interesting preview as to how some issues may be addressed in the context of broader federal privacy reforms. For example:

  - The definition of 'personal information' in the WA Privacy Act expressly includes 'a unique identifier, online identifier or pseudonym', as well as 'technical or behavioural information in relation to an individual's activities, preferences or identity'. This suggests an intention to capture IP addresses and similar identifiers that are not currently clearly caught under definitions used in the federal Privacy Act.

  - Even more significantly, the Information Privacy Principles established under the WA Privacy Act contain restrictions on collection, use and disclosure of personal information unless 'fair and reasonable in the circumstances'. This is an interesting development, as a similar overarching 'fair and reasonable' requirement has been proposed as part of the federal Privacy Act reform process, and has been strongly supported by the Privacy Commissioner and many other privacy advocates. The WA Privacy Act provides an example of how the obligation may be drafted in practice.

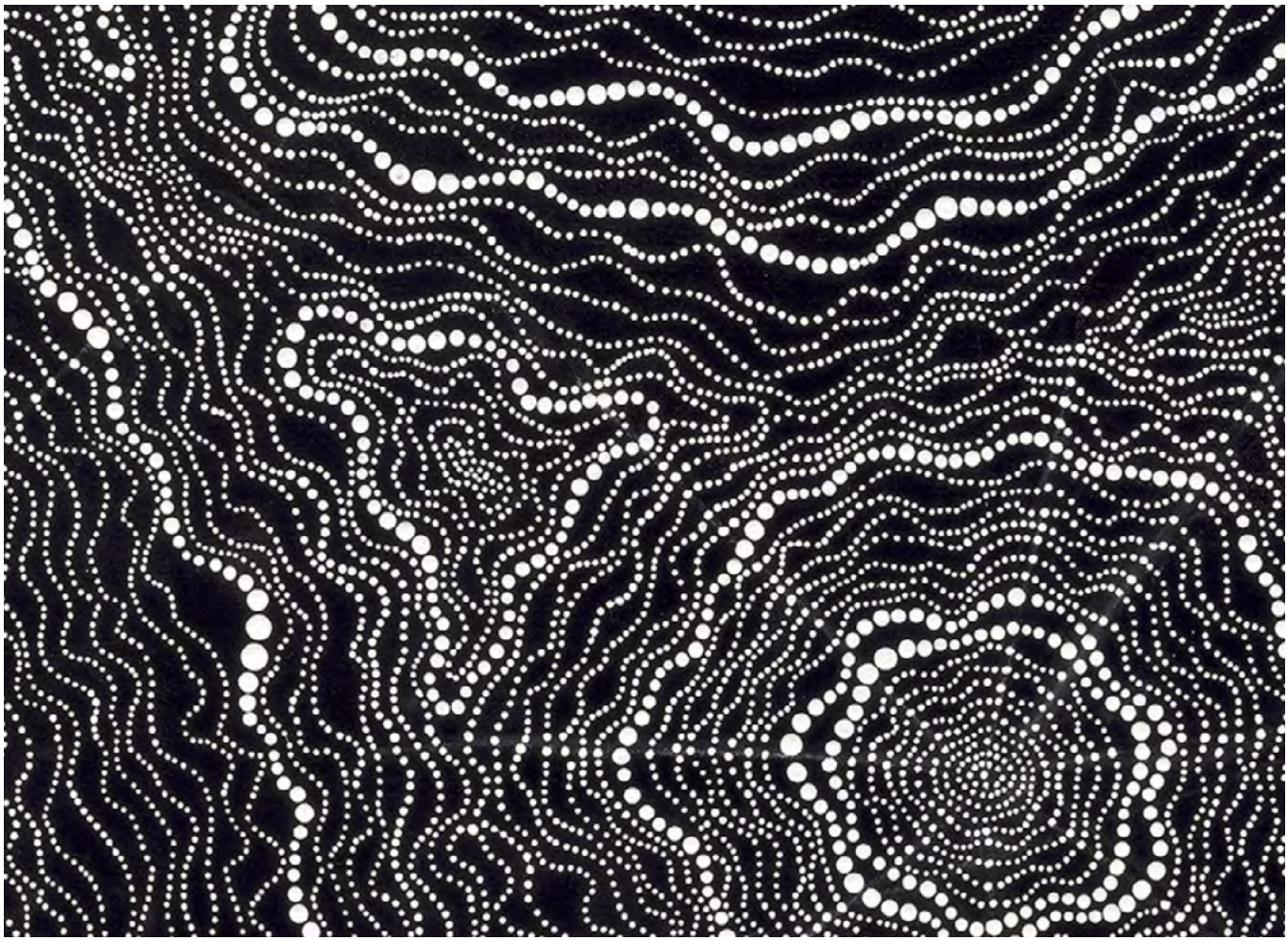
To the extent the Australian Government takes reform proposals such as these forward in 'tranche 2' federal privacy law reforms, we expect they will pay close attention to the precedents set by the Online Safety Act and the WA Privacy Act when it comes to drafting relevant changes.

Implications of reform for productivity

Since being re-elected in May 2025, the Albanese Government has been laser-focussed on issues related to productivity. Interestingly, the Productivity Commission's Interim Report - Harnessing data and digital technology made two draft recommendations in relation to amending the Privacy Act:

- The first interim recommendation is not to introduce a 'right to erasure' due to the high compliance burden this would involve. This suggests that this reform may be less likely to be taken forward by the Government.
- The second interim recommendation is to establish a 'dual track' process under the Privacy Act that provides 'an alternative compliance pathway that enables regulated entities to fulfil their privacy obligations by meeting criteria that are targeted at outcomes, rather than controls-based rules'. In short, the Productivity Commission suggests giving organisations options as to how to comply, and that outcomes may be more important than controls. This is an interesting idea, though it is unclear what it would exactly mean in practice, particularly as many of the current requirements under the Privacy Act are already arguably drafted as outcomes rather than specific controls.

It remains to be seen how influential the Productivity Commission's views will be on the direction of future privacy reform. The Commission's final report is due by the end of 2025 and we suspect that the Government will not commit to any particular pathway until it has had a chance to properly consider the Commission's final recommendations. Nonetheless, the interim report alone demonstrates that there are a range of different possibilities, and it is not necessarily a given that the reforms will reflect the proposals presented by the Attorney-General's Department back in February 2023 in the Privacy Act Review Report.



REGULATORY PERSPECTIVES: PRIVACY IN FLUX

In a conversation with KWM partners Michael Swinson and Bryony Evans at this year's KWM Digital Future Summit, Australian Privacy Commissioner Carly Kind shared perspectives on the privacy landscape and provided interesting insights as to how the Commissioner proposes to deploy regulatory powers to deal with systemic privacy risks, power imbalances, and the rapid rise of AI and emerging technologies.

With the next wave of Privacy Act reforms on the horizon, the Commissioner's comments suggested an intention to double down on robust enforcement, practical guidance, and collaboration with other regulators to ensure privacy remains a cornerstone of trust and innovation.

We have summarised the main themes from the discussion below.

Regulatory priorities

The Commissioner indicated an intention to focus the OAIC's resources on dealing with:

- systemic, egregious or persistent privacy violations that impact vulnerable groups
- power asymmetries resulting from opaque data handling practices that are difficult for individuals to monitor and challenge and
- privacy risks associated with AI and other emerging technologies, including biometric, facial recognition and location tracking technologies.

As part of this approach, the Commissioner suggested that she would prioritise investigations and other action on cases where enforcement is likely to influence market conduct and provide broad benefits to the community.

Clear regulatory guidance

In this context, the Commissioner stressed the importance of setting clear and prescriptive expectations for regulated entities. This includes providing comprehensive, practical guidance that serves as a roadmap for best practice. A recent example is the OAIC's guidance on AI development and use of commercial AI tools, which offers much-needed clarity on how existing privacy laws apply to AI technologies. Ultimately, the value of regulatory guidance, and the OAIC's interpretation of the law, will be further enhanced as these positions are tested and refined through enforcement actions.

Notifiable data breaches: a non-discretionary area of compliance

The Commissioner reinforced the importance of organisations reporting data breaches as required under the mandatory reporting regime established under the Privacy Act.

However, the Commissioner reinforced that experiencing a data breach is not itself a contravention of the Act. In addition, she indicated that the Commissioner typically reserves further action for cases involving systemic issues, repeated incidents, exposure of sensitive information, or egregious non-compliance.

Children's privacy and online safety take centre stage (side by side)

The development of the Children's Online Privacy Code will be an important priority for the Commissioner in the coming year. She indicated that recent consultations revealed not only a wide awareness about data collection practices, but also a keen sense of privacy among Australian children. The OAIC is now in a process of developing a draft Code based on insights gleaned through the consultation process, with the draft expected to be published in early 2026.

In the meantime, the Commissioner will be responsible for overseeing privacy safeguards built into the social media minimum age restrictions that will come into effect in December 2025. While industry has raised concerns about the privacy implications of large-scale age verification, the Commissioner emphasised that age verification measures can be delivered in a privacy-protective manner, provided appropriate privacy safeguards are embedded from the outset. The Commissioner made clear the expectation that a broader commitment to ensuring that online safety should not come at the expense of children's privacy rights.

Privacy and productivity – a false dichotomy

In response to the Productivity Commission's inquiry into Harnessing data and digital technology, the Commissioner pushed back against the idea that privacy poses a threat to innovation. On the contrary, the Commissioner stated her view that robust privacy protections are essential for building public trust and confidence in digital products, acting as a catalyst - not a brake – on economic growth.

In the context of AI adoption, the Commissioner pointed to recent guidance from the OAIC as to how AI models can be trained while remaining compliant with the Privacy Act. She noted that the flexible, principle-based framework of the Privacy Act provides scope for innovation and productivity objectives to be thoughtfully balanced with privacy obligations.

Collaboration between regulators at home and overseas

The Commissioner highlighted the OAIC's ongoing collaboration with other regulators, including the eSafety Commissioner, the Australian Competition and Consumer Commission, and the Australian Communications and Media Authority through the Digital Platform Regulators Forum (DP-REG). The goal of this unified approach is to deliver more consistent and effective regulation, particularly in areas of shared responsibility such as social media, digital identity, and the Consumer Data Right.

On the international front, the OAIC is actively engaged with counterparts in New Zealand, Europe and beyond, sharing insights and working to harmonise approaches on emerging issues like facial recognition and AI.

Competitive AI market for greater privacy choices

Last but not least, the Commissioner expressed her aspirations for a privacy-friendly digital environment powered by AI. The Commissioner emphasised that this vision is achievable - provided there is strong transparency, clear information about data use, and meaningful user choice.

Looking ahead, the Commissioner indicated that the OAIC supports the development of a broader ecosystem of AI models and tools, including sovereign Australian solutions, to ensure that users have genuine options that reflect local values and contexts. The Commissioner expressed a view that fostering a vibrant and competitive market for AI will ultimately empower individuals to select technologies that best align with their privacy expectations and needs.

Click here to access all sessions from the KWM 2025 Digital Future Summit.

STATUTORY TORT FOR SERIOUS INVASIONS OF PRIVACY

In August 2025, tennis-star-turned-politician Sam Groth and his wife commenced legal proceedings against the Herald Sun. They allege that the paper seriously invaded Brittany Groth's privacy by publishing a story suggesting that their relationship began when she was underage. This proceeding presents the first use case of the new statutory tort for serious invasions of privacy.

The new statutory tort, which was introduced in November 2024 and came into effect on 10 June 2025, represents a landmark development in Australian privacy law. Claimants may now bring a direct action for a serious invasion of privacy where there has not been any financial loss, relying on emotional harm or loss of dignity alone. The tort has been designed to offer a flexible framework to address current and emerging privacy risks and to empower individuals to seek compensation for a broader range of invasions of privacy (including those which would not be caught as an interference with privacy under the Privacy Act, for example where the invasions of privacy are undertaken by an entity which is not an APP entity).

The cause of action

The statutory tort is contained in Schedule 2 of the Privacy Act. It covers two types of invasions of privacy:

- *Intrusion upon seclusion* – physical or electronic incursions into an individual's private affairs (for example, hidden cameras in change rooms or unauthorised geolocation tracking) and
- *Misuse of private information* – collecting, disclosing or altering personal data (for example, this could range from unauthorised collection of medical records to reposting intimate content).

In either case, to succeed in establishing the cause of action, a plaintiff must establish four cumulative elements:

1. **Reasonable expectation of privacy**

   The cause of action is only available where a person in the position of the plaintiff would have reasonably expected privacy in all the circumstances. The Privacy Act sets out a range of factors relevant to whether a reasonable expectation exists, including the means used to invade the plaintiff's privacy, the attributes of the plaintiff, the nature of the information, how it was obtained, and whether it was already in the public domain.

2. **Intentional or reckless conduct**

   The plaintiff must establish either that the defendant's objective intention was to invade the plaintiff's privacy by intrusion upon seclusion or misuse of information, or that the defendant was aware of a substantial risk and proceeded anyway. This element confines the scope of the tort by excluding mere negligence, as opposed to intentional or reckless conduct.

3. **Seriousness**

   The plaintiff must establish a degree of seriousness. The Privacy Act suggests the court may consider the degree of offence, distress or harm to dignity caused, or whether the invasion of privacy was intentional and motivated by malice.

4. **Public interest**

   Finally, the court will assess whether the public interest in the plaintiff's privacy is outweighed by any countervailing public interest, such as freedom of expression, freedom of the media, or the prevention and detection of crime.

Defences

The Privacy Act sets out several defences, including where:

- the invasion of privacy was required or authorised under law or by a court
- the plaintiff expressly or impliedly consented to the invasion of privacy or
- the defendant reasonably believed that the invasion of privacy was necessary to prevent or lessen a serious threat to the life, health or safety of a person.

There are also three related defences for absolute privilege, publication of public documents, and fair reporting of proceedings or public concern. In addition, there are exemptions for journalism, law enforcement bodies, intelligence agencies and for persons under the age of 18.

Remedies

The court may award damages or grant remedies as the court thinks most appropriate in the circumstances. Damages must not exceed the greater of **$478,550'** or the maximum amount of damages for non-economic loss that may be awarded in defamation proceedings under an Australian law.

The tort in action

The first opportunity for judicial consideration of the tort is likely to arise in the Groth claim against the Herald Sun.

The claim relates to three articles published by the Herald Sun in July 2025 which allege that the couple commenced their relationship while Brittany Groth was 17 and being coached by her now-husband. The Groths claim that the portrayal of Brittany Groth as a victim of sexual assault and publication of intimate details about her teenage years amounts to a serious invasion of her privacy.

The Federal Court heard the first case management hearing in the proceeding in late October 2025. How the Court assesses the concept of seriousness and weighs the Groth's privacy against the public interest in the reporting is likely to shape the future application of the tort.

There will also likely be interesting issues to address as to the application of the exemption for journalism, including as to the nature of the 'journalistic material' that may be within scope of the exemption. Early indications are that this will be a key point of contention in the Groth case, with different views as to whether the history of their relationship was a newsworthy topic or merely the subject of scandalous gossip.

While the progress of this case will perhaps be of most interest to the news media, other businesses should also take this as an opportunity to review their personal information collection processes and disclosures to confirm that they are not exposing themselves to similar claims under the new tort. Care should be taken when collecting sensitive information, such as biometric data, including by ensuring that consumer consents are explicit and well-informed. Businesses should also be cognisant that the statutory tort is not subject to some exemptions that apply under the Privacy Act more broadly, including in relation to the handling of employee records. This means that businesses should ensure that any review extends to the full scope of their data handling practices, including in relation to employees.

LATEST PRIVACY LAW CASES

5.1 Commissioner determinations

Over the past year the Privacy Commissioner has issued a number of determinations that usefully illustrate how the existing Privacy Act applies in practice. We have set out detailed summaries below. However, it is also worth highlighting some of the overarching lessons that can be drawn from these determinations:

- **Organisations cannot outsource responsibility for privacy compliance.** Organisations remain liable for breaches of privacy by their employees and contractors. However, there are limits to this vicarious liability, and organisations may not be responsible for employees who commit privacy breaches while acting beyond the scope of their duties and in violation of applicable work policies and procedures.
- **Data access obligations work hand-in-hand with record retention and destruction requirements.** While organisations cannot be compelled to provide access to information they no longer hold, they are expected to preserve information where it has ongoing relevance in accordance with clearly documented policies. The tension between expectations around retention and destruction can be difficult for organisations to manage effectively.
- **A higher standard of privacy compliance is expected when dealing with vulnerable individuals.** In addition, organisations may be held to a stricter compliance standard based on their relative size and sophistication and the volume of personal information that they manage, as well as the sensitivity of that information.

(a) 'ATU' and 'ATX' (Privacy) [2025] AICmr 23 (30 January 2025)

What was this determination about?

This determination concerned a privacy complaint made by 'ATU' against 'ATX', the operator of a residential building business. The complainant, ATU, was a customer who had paid a deposit to ATX for the construction of a new home. After a contractual dispute arose, ATU sought access to the draft building agreement, which ATU believed contained their personal information. ATU made several requests for this document (both written and oral) and later lodged a complaint with the OAIC when those requests were not met.

The main question for the OAIC was whether ATX had breached its obligations under APP 12, which gives individuals the right to access their personal information held by an organisation. The OAIC noted that this is a common source of complaints, and that while the complaint was not upheld in this instance the determination was published for its 'educative value'.

Organisations must 'hold' the information at the time of the access request

APP 12 requires that an organisation must give access to personal information it 'holds', subject to certain exceptions. In this case, ATX argued that it did not hold the draft building agreement at the time of ATU's access request because the physical file containing the document had been destroyed shortly before the request was made, and no electronic copy existed.

The destruction of the file was said to be in line with the company's usual practice for files relating to projects that did not proceed, although ATX could not provide a formal written policy addressing such practices. ATX submitted that its practice of destroying clients' personal information is concurrent with its obligations under APP 11.2 to take reasonable steps to destroy personal information it no longer needs for any purpose.

Ultimately, the complaint was dismissed on the basis that there was insufficient evidence to find ATX held personal information in question. Further, ATX had provided adequate written notice of refusal as required under APP 12.9. However, the Commissioner expressed concern about ATX's record retention and destruction practices, especially given the ongoing dispute and the significance of the documents involved. The Commissioner recommended that ATX review its relevant policies to ensure it could properly respond to access requests in the future and avoid similar issues.

What are the implications?

This determination seems to be good news for organisations facing challenges with APP 12 requests. The determination appears to overlay an implied 'reasonableness' requirement in response to an APP 12 request, which is notable as this is one of the few APPs that is not subject to an express reasonableness qualification.

This determination also clarifies the Commissioner's view on the interplay between the right to access personal information and the practical realities of organisational record-keeping. In particular, the Commissioner stated that '[a]lthough the right to access one's personal information is a critical pillar of the right to privacy, it should not place an unreasonable burden on the respondent to act outside of reasonable administrative and logistical practices.' Organisations can strengthen their position by maintaining clear and robust record retention and destruction policies to define when and under what circumstances the information in their possession will be retained or destroyed.

(b) 'ATQ' and CEO of Services Australia (Privacy) [2025] AICmr 19 (23 January 2025)

What was this determination about?

This determination addressed a privacy complaint brought by 'ATQ' against the CEO of Services Australia. The complaint arose from repeated entwinement of the complainant's personal records with those of other customers, primarily due to processing errors by Services Australia staff between April 2015 and September 2021 in handling Medicare and vaccination records. ATQ alleged breaches of APP 6.1 (unauthorised disclosure of personal information), APP 10.2 (failure to ensure the accuracy and currency of personal information), and APP 11.1 (failure to take reasonable steps to protect personal information from unauthorised disclosure).

Systemic failures in protecting personal information

The Privacy Commissioner found that all three alleged breaches were made out. The breaches were serious and repeated, with Services Australia failing to take reasonable steps to protect ATQ's personal information, ensure its accuracy, and prevent its unauthorised disclosure. The following factors were of particular relevance to the breaches of APP 10.2 and 11.1:

- *Sophistication of the entity:* Despite its sophistication and significant annual budget (over $6 billion for the 2022–2023 financial year), Services Australia's systems and processes were found to be inadequate. The Commissioner noted that the measures Services Australia had in place, such as flagging systems and operational guidelines, failed to prevent repeated breaches over an extended period. Having regard to the size and resources of Services Australia, the Commissioner's view was that it would not have been unreasonably burdensome to implement additional security measures.
- *Sensitivity of the personal information:* Services Australia collects and handles sensitive information relating to customers' health and welfare, financial situation, disabilities, citizenship status and family circumstances for millions of Australians. In the Commissioner's view, the sensitivity and volume of this data demanded robust protections.

- *Significant adverse consequences:* The Commissioner highlighted the possible adverse consequences of Services Australia's systems being inadequate given the nature of the personal information that it collects and handles, including potential identity theft, fraud and inability to access specific services. ATQ experienced real-world harm, such as difficulties in obtaining digital vaccination certificates required for employment and international travel, and exclusion from health screening programmes.

What are the implications?

This determination highlights the higher standards which are likely to be applied to organisations that hold sensitive information or which are more sophisticated organisations with more significant budgets. More sophisticated organisations will be expected to take into account their complexity and size in resourcing and budgeting decisions relating to compliance with privacy laws.

The Commissioner emphasised that Service Australia's failure to implement reasonable steps to prevent repeated breaches over an extended period demonstrated systemic inadequacies. Such breaches can expose organisations to significant liability, including potential civil penalties where the Commissioner considers them to be sufficiently serious to warrant further action in court.

(c) 'ATE' and 'ATF' (Privacy) [2025] AICmr 10 (13 January 2025)

What was this determination about?

This determination considered whether a telecommunications company (the respondent) was liable under the Privacy Act for the unauthorised disclosure of a customer's personal information by a senior employee. The complainant, who was incarcerated, had been attempting to recover a mobile number from the respondent. During this process, a senior employee of the respondent disclosed the complainant's personal information, including his full name and details of his correspondence with the company, to a journalist. This resulted in a media article about the complainant's criminal history and his efforts to recover the number. The complainant alleged that this disclosure interfered with his privacy and sought compensation and an apology.

Direct and vicarious liability under the Privacy Act

A central issue was whether the respondent could be held directly or vicariously liable for the actions of its senior employee. The Commissioner found that the senior employee's actions were not authorised, were contrary to the respondent's internal policies, and were not connected to his ordinary employment duties. The employee was not responsible for media engagement and had acted entirely on his own initiative, motivated by personal reasons rather than any commercial or employment-related purpose. The Commissioner concluded that the employee was on a 'frolic of his own' and that the respondent was neither directly nor vicariously liable for his conduct under relevant provisions of the Privacy Act. As a consequence, the complaint was dismissed, and the remedies sought by the complainant were not granted.

What are the implications?

This determination reinforces the principle that employers may be held liable for privacy breaches by their employees. However, it also illustrates that there will be limits to this vicarious liability, and organisations will not automatically be liable for unauthorised acts of employees that fall outside the scope of their employment, even where those employees hold senior positions. The determination also demonstrates the value of having clear internal policies and rules on data handling – as these may set the boundaries of what employees have been authorised to do, so if they cross those boundaries then it is clear they are acting on their own rather than for the company.

(d) Commissioner Initiated Investigation into Property Lovers Pty Ltd (Privacy) [2024] AICmr 249 (22 November 2024) and Commissioner Initiated Investigation into Master Wealth Control Pty Ltd t/a DG Institute (Privacy) [2024] AICmr 243 (18 November 2024)

What were these determinations about?

These two determinations concerned the privacy practices of Master Wealth Control Pty Ltd (trading as DG Institute) and Property Lovers Pty Ltd, both of which operated property investment education businesses in Australia and are related bodies corporate. The core issues in both cases concerned the collection, use, and disclosure of personal information relating to individuals in 'distressed' property situations, such as bankruptcy, divorce, or deceased estates. Both companies compiled and distributed 'leads lists' containing personal information of these individuals to paying participants of their respective businesses. The information was sourced from third-party websites and databases, including court listings, published death and funeral notices and property data services, and was used to enable program participants to target vulnerable property owners for potential below-market-value acquisitions.

Data scraping in these circumstances found unlawful

The Privacy Commissioner found that both Master Wealth Control Pty Ltd and Property Lovers Pty Ltd had engaged in multiple breaches of the APPs, specifically:

- **Unfair collection of personal information (APP 3.5):**

  Both companies collected personal information from third-party sources in a manner that was not fair. The individuals concerned had no knowledge or reasonable expectation that their information would be collected for commercial purposes, particularly in circumstances where they were likely to be vulnerable (such as if they were party to court proceedings because of bankruptcy or a deceased estate).

  The collection of this information was also contrary to the terms and conditions of the third-party sources, which generally prohibited commercial use or redistribution of the data. Although the respondent removed the names of some prospective property owners from their lists, they provided instructions and guidance on how to re-identify individuals.

  According to the Commissioner, these cases could be distinguished from the decision in Clearview AI Inc and Australian Information Commissioner [2023] AATA 1069, which concerned the scraping of information that individuals had voluntarily contributed to various public websites, because the publication of individuals' personal information on the court websites and subscription-based services is the product of Australia's open justice system and is beyond the individuals' control.

- **Failure to notify individuals (APP 5.1):**

  Neither company took reasonable steps to notify individuals that their personal information was being collected, nor did they otherwise ensure that individuals were aware of the relevant matters under APP 5.1. The Commissioner found that, given the nature and potential adverse consequences of the collection and use, it was reasonable and practicable for the companies to have notified affected individuals once sufficient information had been compiled to identify them.

- **Failure to ensure data quality (APP 10.2):**

  Both companies failed to take reasonable steps to ensure that the personal information they used and disclosed was accurate, up-to-date, complete, and relevant. The companies relied on 'educated guesses' and did not verify the information before distributing it to program participants, increasing the risk of misidentification and harm.

- **Deficient privacy policies (APP 1.3 and 1.4):**

  The privacy policies of both companies were found to be inadequate. They did not clearly specify the types of personal information collected, the methods of collection, the purposes for which the information was used and disclosed, or how individuals could access or correct their information or make complaints.

What are the implications?

These cases highlight that privacy laws still apply to information that is in the public domain.

In other words, information is not 'fair game' simply because it is accessible online or through public records. This is especially the case for information relating to vulnerable individuals who do not have direct control over how their information has been placed in the public domain.

The determinations also reinforce the strict manner in which the Commissioner will apply transparency requirements under the Privacy Act, with the expectation being that companies will make every effort to ensure that relevant individuals are aware of their information collection and handling practices, even where they have had no prior direct contact with those individuals. This may present a significant practical barrier for organisations wishing to use information from third party sources.

(e) Commissioner Initiated Investigation into Regional Australia Bank Limited (Privacy) [2025] AICmr 89 (14 May 2025)

What was this determination about?

In this determination, the first made by the Privacy Commissioner in relation to the Consumer Data Right (**CDR**) regime, the Commissioner found that Regional Australia Bank (**RAB**), in its capacity as a CDR data holder, breached Privacy Safeguards 1 and 11 by virtue of the conduct of its third-party service provider, Biza Pty Ltd (**Biza**).

The case arose after a data incident in which the CDR data of up to 197 consumers was commingled, resulting in RAB disclosing inaccurate data to third parties. The breach was traced to Biza, RAB's contracted CDR solution provider, which failed to implement a critical software patch in RAB's CDR environment.

Contractual provisions to shift liability for non-compliance insufficient

The central issue was whether RAB, as a data holder under the CDR framework, had taken reasonable steps to ensure the accuracy and security of CDR data, and whether it could be held responsible for the actions of its service provider, Biza.

The Commissioner found that, under section 84(2) of the Competition and Consumer Act 2010 (Cth), Biza was acting as RAB's agent in relation to CDR compliance, and therefore RAB was liable for Biza's conduct even though RAB had sought to shift liability to Biza through contractual provisions.

The investigation revealed that Biza had identified a software fault in February 2023 and patched it for other clients, but failed to do so for RAB's environment, which was still in pre-production. When RAB's system went live, the unpatched software led to the commingling of CDR data. The issue was only discovered after a consumer complaint and was resolved when Biza implemented a broader software update in June 2023.

The Commissioner determined RAB breached Privacy Safeguards 1 and 11 by virtue of Biza's conduct.

What are the implications?

This determination highlights the high standards imposed on data holders under the CDR regime. The Commissioner emphasised that data holders remain responsible for the acts of their agents in relation to CDR data, regardless of contractual attempts to shift liability.

In other words, it is not possible to simply outsource responsibility for compliance. The same applies under other privacy laws. It is not enough for organisations to rely upon contractual assurances. Before engaging third party service providers to assist them in the management of their data assets, organisations should undertake appropriate due diligence to validate the processes that the third party service provider has in place to comply with applicable privacy and data security obligations. Any pre-contract due diligence should be supported by ongoing monitoring to ensure that contractual compliance obligations are being honoured in practice.

(f) Commissioner Initiated Investigation into Kmart Australia Limited [2025] AICmr 155 (18 September 2025)

What was this determination about?

This determination concerned the use of facial recognition technology (**FRT**) by Kmart Australia to detect and prevent refund fraud. The determination describes that the FRT system:

- was deployed as part of a pilot program aimed at detecting and preventing refund fraud by capturing facial images of all store entrants and comparing them against stored databases; and
- operated by capturing multiple facial images at store entry and again at the returns counter. These images were used to generate biometric metadata, which was then compared against two databases: a 'History Database' of all entrants to a particular store and an 'Enrolment Database' of individuals suspected of refund fraud or related misconduct across multiple stores.

The system was designed to alert staff if a match was detected, enabling further scrutiny or refusal of refund requests.

The Commissioner's investigation related to whether the use of the FRT system complied with the APPs, with particular focus on the collection of sensitive information, notification requirements, and disclosures made in privacy policies relating to the use of facial recognition technology.

What was the Commissioner's decision?

In summary, the Commissioner determined that there had been a breach of:

- APP 3.3, by the collection of sensitive information without consent and without a valid exception;
- APP 5.1, by the failure to take reasonable steps to notify individuals of the collection and its purposes; and
- APP 1.3 and APP 1.4, by the failure to maintain a clearly expressed and up-to-date privacy policy that accurately described its collection of sensitive information in the FRT system.

Orders were made for the cessation of the practices that were found to interfere with privacy, publication of an apology and detailed statement on websites and in stores, retention and then destruction of all FRT-collected data according to specified timelines, and for the improvement of applicable privacy policies. These outcomes appear to reflect the fact that the FRT system in question was only used for a limited trial, which ceased quickly.

APP 3: Collection of sensitive information without consent

The Commissioner found that the FRT system process involved the collection of sensitive information (specifically, biometric information used for automated identification) about all store entrants, not just those suspected of wrongdoing. Consent was not sought or obtained from individuals for this collection.

Submissions were made that the collection of sensitive information without consent was permitted, as the relevant 'permitted general situation' exception under section 16A of the Privacy Act allows for the collection of sensitive information without consent where an entity reasonably believes the collection is necessary for an organisation to take appropriate action in relation to suspected unlawful activity or serious misconduct in connection with its functions or activities.

The Commissioner accepted that refund fraud constituted unlawful activity and that there had been a reason to suspect such activity was occurring. However, the Commissioner concluded that there could not have been a reasonable belief that collecting the sensitive information ***of every store entrant*** was necessary or proportionate to address the issue, having regard to other less privacy-intrusive alternatives which the Commissioner considered were available (such as changes to refund policies, procedures, and other security measures).

The Commissioner's primary focus was on whether there could have been a reasonable belief at the relevant time (i.e., before the pilot program commenced) that collecting the sensitive information of every store entrant was 'necessary' to take 'appropriate action' against refund fraud.

Some of the factual details are redacted in the public determination, but in essence the Commissioner found that the requirements of the exception were not met, for several reasons:

- **Necessity requires more than helpfulness or convenience.** The Commissioner emphasised that 'necessary' means more than merely helpful, desirable, or convenient. It must be shown that the collection is required, not just preferred, to achieve the intended action. This aspect of the Commissioner's reasoning is also consistent with the (albeit limited) case law on necessity in the context of the Privacy Act,[1] which indicates necessity is a relatively strict standard.
- **Suitability.** While FRT could help detect some refund fraud, its effectiveness was limited to a subset of cases and the overall impact was small compared to the scale of the issue. The Commissioner found the system was only 'partially suitable' for addressing the relevant known refund fraud techniques.
- **Proportionality.** The determination emphasises that the system collected sensitive information from all customers, not just those suspected of fraud, which in the Commissioner's view had a privacy impact that far outweighed the limited benefits in fraud prevention for a relatively small number of fraudulent incidents detected – and so was disproportionate to the risk. This aspect of the reasoning considered the scale of commercial impact, balanced against the potential privacy harms from FRT surveillance generally, as well as specific risks from the pilot program implementation.
- **Less intrusive alternatives.** The Commissioner identified several options, such as: requiring proof of purchase for refunds, undertaking additional staff training to identify suspicious behaviour, implementing changes to store layout or returns processes, and use of other security technologies (e.g., RFID tags). In the Commissioner's view, these alternatives could have addressed refund fraud without collecting biometric data from all customers.

1. See further, *Seven Network (Operations) Limited v Media Entertainment and Arts Alliance* [2004] FCA 637 (21 May 2004) at [46], discussing the former National Privacy Principle 1.

- **Lack of evidence of a Privacy Impact Assessment.** The Commissioner found no evidence was provided that a privacy impact assessment had been conducted before implementing FRT to demonstrate that less privacy intrusive options had been considered. This is a common feature across recent FRT determinations and it is clear that, while not a mandatory requirement, the Commissioner will take a dim view if a PIA is not conducted for any implementation of FRT.

APP 5 and APP 1: Notification and Privacy Policy disclosures

The Commissioner also found that there had been a failure to take reasonable steps to notify individuals about the collection of their sensitive information, as required by APP 5.1. The limited signage referencing CCTV and facial recognition was found to not adequately inform customers of the nature and purpose of the collection, nor did they direct individuals to the applicable privacy policy.

In addition, the Commissioner found that the applicable privacy policy did not sufficiently describe the kinds of personal information collected via FRT or the means by which it was collected, even though two out of three of the relevant versions of the policy expressly disclosed the collection of 'images from facial recognition software'. In particular, the Commissioner concluded that the policy did not adequately disclose that the use of the FRT system involved the generation and collection of 'metadata' and 'biometric information' (as well as the collection of facial images from which that information was extracted) and so failed to disclose the kinds of personal information collected and held as required by APP 1.4.

What are the implications?

While the details of the determination itself are specific to the particular context in which the FRT system was used in this case, it provides valuable insight into how the Commissioner will apply relevant privacy laws to this type of technology.

The determination certainly does not indicate an intention to apply a blanket ban on use of FRT. The Commissioner's blog post that accompanied the determination – itself indicative of a new approach by the OAIC to providing guidance along with enforcement – indicates that use of FRT may be permissible, provided it is proportionate and transparent, although 'it is a high bar that must be cleared'. Extensive groundwork will need to be carried out to support any use of this type of technology, even as part of a pilot program, with careful consideration being given to other less privacy intrusive alternatives. At a minimum, a detailed PIA should be conducted to support any initiative of this nature.

5.2 *Waller v Barrett* – Victorian court recognises common law privacy tort

What was this case about?

In *Waller (A Pseudonym) v Barrett(A Pseudonym)* [2024] VCC 962, the County Court of Victoria was required to determine, among other issues, whether a parent's public statements about their child could give rise to a cause of action in tort for invasion of privacy under Australian common law.

The defendant (the father) had made statements to journalists and an author about the plaintiff (his estranged daughter), including a claim that she had apologised to him, which was not true. The plaintiff argued that this was a serious intrusion into her private life and dignity.

Recognition of the tort of invasion of privacy, at least in Victoria

Before turning to the tort, the Court first considered the breach of confidence claims. In relation to one of the pieces of information, there could be no breach of confidence as the information was not true (i.e. it did not pass the first threshold of being 'information'). As such, the Court considered whether the plaintiff could seek redress under the tort.

The Court held that a distinct action for invasion of privacy now forms part of the common law of Australia. This was not the creation of a new tort, but rather the recognition of a 'bifurcation' within the action for breach of confidence: one branch protecting commercial secrets, the other protecting personal privacy and human dignity.

The Court declined to provide an exhaustive definition of the elements, but held that relief should be available, at a minimum, where there is the making public of private matters in circumstances that a reasonable person, standing in the shoes of the claimant, would regard as highly offensive. The Court also declined to identify any potential defences, or express a view whether the action for invasion of privacy is better viewed as an equitable or tortious cause of action.

The Court found the defendant liable for breach of confidence and invasion of privacy.

What are the implications?

This decision confirms that individuals in Australia (at least in Victoria) can now bring a common law action for invasion of privacy, particularly where private matters are exposed to the public without consent and in a manner that would be highly offensive.

The implications are heightened by the recent introduction under the federal Privacy Act of a statutory tort for serious invasions of privacy (which commenced on 10 June 2025), which provides an additional, formal avenue for individuals to seek redress for privacy harms.

Unlike the common law tort of invasion of privacy, where the elements and defences are not exhaustively defined, the statutory tort for serious invasions of privacy sets out specific elements that must be established and provides express defences and exemptions. However, statutory caps on damages apply under the statutory tort, and so despite the greater uncertainty plaintiffs may still be attracted to the common law action, or at least may wish to run both actions in parallel, in order to stand the best chance of obtaining a favourable outcome. This may result in additional complexity and lengthy litigation, particularly while the elements of the common law tort are further teased out.

While there has been a relatively limited history of privacy-related litigation in Australia to date, the emergence of these new statutory and common law actions in rapid succession makes it likely that this trend will soon change..

5.3 *NSW v Wojciechowska* - High Court consideration of NSW privacy legislation

What was this case about?

In *NSW v Wojciechowska* [2025] HCA 27, the High Court considered an Australian constitutional law question in the context of a dispute involving compliance by the NSW Police with NSW privacy legislation (the *Privacy and Personal Information Protection Act 1998* (NSW) (**NSW PPIPA**).

Ms Wojciechowska owned a property in NSW and complained to the police about the removal of some trees on her property. In 2018 the police attended her property. Ms Wojciechowska was dissatisfied with the result.

In late 2018 Ms Wojciechowska relocated from her property in NSW to Tasmania. From her new location in Tasmania, Ms Wojciechowska pursued a complaint under section 16 of the PPIPA against the NSW Police, alleging that information they held about her was inaccurate. After the NSW Police decided not to take action in response to that complaint, she applied to the NSW Civil and Administrative Tribunal (**NCAT**) for administrative review of that decision. In late 2020, Ms Wojciechowska had decided that NCAT was not the proper jurisdiction to pursue her complaint against the police, and she requested that NCAT decline to exercise jurisdiction. She argued that if NCAT heard the case, it would be exercising the judicial power of the Commonwealth (by deciding a case involving an interstate resident) and that the NSW Parliament lacked the power to invest a tribunal to resolve a case of that kind.

Unsurprisingly, NCAT found that it did have jurisdiction to determine the case. Ms Wojciechowska, a self-represented litigant, expanded the dispute by commencing tort proceedings in the District Court of NSW and, in May 2022, commenced proceedings in the Supreme Court of NSW seeking to challenge NCAT's jurisdiction. Those proceedings in the Supreme Court were removed to the NSW Court of Appeal and the NSW Court of Appeal found in favour of Ms Wojciechowska. In March 2024 the High Court of Australia granted the NSW Government special leave to appeal. Judgment was delivered in August 2025.

NCAT's role in reviewing privacy cases is administrative

The assessment of whether a kind of tribunal decision (part of the executive branch of government, and not a court) is of an administrative or judicial character is a notoriously tricky issue. However, after a close analysis of NCAT's role under the PPIPA and the NSW Administrative Decisions Review Act, the High Court unanimously held that NCAT's role was administrative and that NSW Parliament could empower NCAT to order that a public sector agency pay compensation for loss or damage suffered as a result of conduct in contravention of an information protection principle.

The NSW Court of Appeal had decided that the regime in issue could not be distinguished from that considered by the High Court in *Brandy v Human Rights and Equal Opportunity Commission* [1995] HCA 10; 183 CLR 245 (***Brandy***), where the Court held that a regime involved the impermissible exercise of judicial power by a member of the executive branch of government. The material elements of the regime in *Brandy* were:

- an obligation on the Human Rights Commission (part of the executive branch) to lodge with the Federal Court a determination that an entity had engaged in unlawful discrimination when the Commission had reached that conclusion;
- an obligation on the registrar of the court to register the determination and
- on registration, the determination had effect as an order of the Federal Court.

The regime in issue in this case involved the possibility of the Tribunal ordering a public sector agency to pay damages when it found that a public sector agency had contravened the PPIPA and an individual had suffered loss or damage as a result, and an obligation on the registrar of NCAT to certify the amount to be paid. If that certificate was subsequently filed in the registry of a court having jurisdiction to give judgment for a debt of the amount in question, the certificate operated as a judgment. Presumably, the individual who suffered loss or damage would be the person who would file the certificate in a court registry if the public sector defendant failed to pay. The High Court saw this as sufficiently different to distinguish Brandy. In particular, weight was put on the fact that it was not NCAT as the decision maker that was obliged to register the certificate in court – the Tribunal's role was complete when the certificate was issued, so it was not the Tribunal's conduct that converted its order into one that was binding, authoritative and enforceable as a judgment of a court.

What are the implications?

NCAT can continue to decide the 'correct and preferable' outcome in cases involving alleged breaches of the NSW PPIPA, including that NSW government agencies pay compensation to individual data subjects. The same reasoning will apply to NCAT decisions under the *NSW Health Records and Information Privacy Act* (which applies to private sector health services providers in addition to public sector health agencies). The decision will not affect the powers of the Information Commissioner or Privacy Commissioner under the federal Privacy Act or the method of enforcing the Commissioner's determinations.

The decision is not relevant to enforcement under the federal Privacy Act, which is Australia's main privacy law. After *Brandy*, federal human rights legislation, including the Privacy Act, was amended to address the 'judicial power' issue. Section 55A of the Privacy Act deals with the enforcement of a determination made by the Commissioner, which is relevant if an entity refuses to comply with an adverse determination. That section provides for a 'de novo' hearing by a federal court into whether an entity has contravened the Privacy Act and the orders to be made as a result, with the Commissioner's determination and any document considered by the Commissioner being admissible as evidence before the court. This is designed to make it clear that it is the role of the court (and not the Commissioner as a member of the executive branch of government) to decide, on a binding basis, whether there has been a contravention of the Act and the consequences of that contravention.

If an entity has received an adverse determination by the Commissioner, the entity may also apply for review on the merits to the Administrative Review Tribunal, or challenge the Commissioner's determination in judicial review proceedings (e.g. on the basis of error or law or failure to afford procedural fairness etc). The case is also not relevant to civil penalty proceedings commenced by the Commissioner in a federal court – in those rare cases it is clear that it is the role of the court (and not the Commissioner) to determine whether there has been a contravention and the appropriate civil penalty. In civil penalty cases, even where the Commissioner and the defendant entity have reached an agreement on the nature of the contraventions and the corresponding penalty, the court does not act as a 'rubber stamp' and must be satisfied that the evidence justifies the orders proposed by the parties. Famously in the 'Wagyu and Shiraz' case,[2] the Federal Court refused to accept that a contravention had been established even though the defendant bank was prepared to consent to a declaration being made that the bank had breached the law and to pay a penalty in order to avoid further litigation.

5.4 *Australian Information Commissioner v Australian Clinical Labs Limited (No 2)* – First civil penalty under the Privacy Act

Overview

On 8 October 2025, the Federal Court delivered judgment in *Australian Information Commissioner v Australian Clinical Labs Limited (No 2)* [2025] FCA 1224, imposing the first civil penalty issued under the Privacy Act, handing down a $5.8 million penalty to Australian Clinical Labs (**ACL**) in relation to a 2022 data breach incident.

The decision provides the first judicial guidance on three core obligations under the Privacy Act:

- taking 'reasonable steps' to protect personal information (APP 11.1)
- conducting a 'reasonable and expeditious assessment' when an eligible data breach is suspected (s 26WH) and
- notifying the Commissioner 'as soon as practicable' once such a breach is believed to have occurred (s 26WK).

2. *Australian Securities and Investments Commission v Westpac Banking Corporation (Liability Trial)* [2019] FCA 1244, upheld on appeal in *Australian Securities and Investments Commission v Westpac Banking Corporation* (2020) 277 FCR 343.

However, the decision followed a settlement between the Commissioner and ACL reached at mediation convened in around June 2025 by the Honourable Peter Jacobson KC, and was made after the parties filed a statement of agreed facts and admissions on 17 September 2025 and joint submissions on 1 October 2025. In support of an agreed penalty, and based on an agreed factual background, the parties jointly submitted to the Court how these three core obligations should be interpreted, and how many contraventions of the Privacy Act arose from the agreed facts and submissions. Without a contradictor, the Court essentially adopted the parties' agreed position. In circumstances where these key aspects of the case were not subject any contest on the merits, the decision may have limited precedential value.

What was this case about?

The Commissioner commenced proceedings against ACL (who is, and was, one of Australia's largest private pathology companies) in relation to a data breach that occurred in February 2022.

In December 2021, ACL acquired the assets of Medlab Pathology Pty Ltd including its IT systems, which contained the sensitive personal and health information of more than 223,000 individuals.

In February 2022, a ransomware group known as Quantum Group launched a cyberattack on the Medlab IT systems. The attack resulted in 86GB of sensitive data being exfiltrated and subsequently published on the dark web.

ACL relied heavily on a third-party cybersecurity provider to investigate the breach. The investigation was limited in scope, and by March 2022, ACL had concluded that no data had been exfiltrated.

Despite receiving a notification from the Australian Cyber Security Centre (**ACSC**) on 25 March 2022 indicating that Medlab may have been the subject of a ransomware incident, ACL maintained that no breach had occurred.

It was not until 16 June 2022, when the ACSC alerted ACL that exfiltrated personal, health and financial information had been published on the dark web, that ACL accepted an eligible data breach had occurred. ACL did not notify the Commissioner of the eligible data breach until 10 July 2022.

The issues before the Court were whether, as jointly submitted by the parties:

1) ACL failed to take 'reasonable steps' to protect personal information under APP 11.1(b)

2) ACL contravened s 26WH(2) of the Privacy Act by failing to carry out a reasonable and expeditious assessment of whether a data breach had occurred and

3) ACL contravened s 26WK(2) of the Privacy Act by failing to notify the Commissioner 'as soon as practicable' that there had been a reportable data breach.

Section 13G of the Privacy Act makes it a civil penalty offence for an entity to engage in an act or practice that constitutes a serious interference with an individual's privacy, and provides for substantial civil penalties.

Findings

Justice Halley adopted the parties' agreed submissions, finding that ACL had contravened s 13G of the Privacy Act in respect of all three of the issues before the Court, and approved the agreed penalties that the parties submitted.

A $5.8 million aggregate penalty was imposed on ACL – summarised in the table below. ACL was also ordered to pay $400,000 towards the Commissioner's legal costs.

RELEVANT SECTION	APP 11.1(B)	S 26WH(2)	S 26WK(2)
Number of contraventions	223,000	1	1
Factors contributing to contravention	• Court identified ACL had 'significant' cybersecurity failings • Poor controls lacking basic cyber protection (MFA, encryption etc.) • Failure to identify critical vulnerabilities • Untrained staff • No clear assignment of responsibilities	• ACL relied on a limited and inadequate third-party assessment (e.g. only monitored 3 of 127 computers attacked) • Accessed logs approximately 4 hours after ransom demand • Conducted a limited investigation into whether hackers were still connected to the Medlab IT network	• Information to be included in notification 'not onerous' • Determined it was practicable for ACL to have notified the Commissioner within two to three days of becoming aware of the breach (ACL took 24 days)
Theoretical maximum penalty	$495,060,000,000	$2,200,000	$2,200,000
Agreed penalty	$4,200,000	$800,000	$800,000
Aggregate penalty	$5,800,000		

Key reasoning

The judgment provides the first judicial interpretation of APP 11.1(b), and confirms that 'reasonable steps' under APP 11.1 are assessed objectively and contextually. However, key aspects of the judgment should be treated with caution in circumstances where it was the subject of a settlement and there was no contest or contradictor on key issues.

The assessment of the circumstances could be expected to include:

- the sensitivity of the personal information
- the potential harm to individuals if the information was accessed or disclosed
- the size and sophistication of the APP entity
- the cybersecurity environment in which the APP entity operates and
- any previous threats or cyberattacks made against the APP entity.

The Court drew on analogous 'reasonable steps' jurisprudence to emphasise that the obligation is holistic, cannot be discharged by mere delegation to third-party providers, and does not require the 'optimal' or all possible steps to have been taken, rather, the totality of steps must be reasonable in the circumstances.

Applied to the agreed facts, it was found that ACL had a number of deficiencies in its ability to detect and respond to cyber incidents, including that it had failed to identify vulnerabilities in the Medlab IT Systems prior to acquiring the assets, had limited security monitoring, weak authentication measures and inadequate cyber incident playbooks and training.

The Court found, as jointly submitted by the parties, that the APP 11.1(b) contravention in respect of each affected individual whose data was impacted constituted a separate serious interference with privacy within the meaning of the former section 13G of the Privacy Act (being a civil penalty provision) – meaning that ACL committed 223,000 contraventions with a maximum theoretical penalty exceeding $495 billion. If the parties had not reached an agreed settlement outcome, this is an aspect of the reasoning that we expect would have been tested more thoroughly, and a different conclusion may have been reached. It is questionable whether the proper construction of the (former) section 13G of the Privacy Act provides for a separate contravention with a separate maximum pecuniary penalty based on the number of individuals whose information is impacted. There are other ways in which the civil penalty provisions under the Privacy Act could be interpreted for the purposes of assessing the number of contraventions, focussing on the number of 'acts or practices' in question rather than the number of affected individuals. Notably, since the ACL data breach, the relevant provisions have been amended with 'the number of individuals affected by the interference with privacy' now expressly listed as a factor that will be taken into account when assessing the seriousness of a breach. This language seems to contemplate that a single interference with privacy may affect multiple individuals – it is not necessarily the case that there would be a separate interference in relation to each individual.

It is also worth noting that the civil penalties available under the Privacy Act were materially increased relatively recently because of concerns that they would not otherwise provide a sufficient deterrent, including for larger multinational organisations. We can see how that may be the case if a breach affecting multiple individuals is treated as a single contravention. However, it would seem to be less of a concern if there would be separate contraventions, and therefore penalties, for each individual affected by the relevant conduct. It is worth noting that all of the civil penalty proceedings brought by the Commissioner to date have concerned data breaches where thousands of Australians have been affected and where the maximum theoretical penalty calculated on a 'per affected individual' basis would be astronomical. If that was the way that the Parliament had intended for the penalty regime to work, it is hard to understand why there was any concern about the potential size of the financial penalty and its effectiveness as a deterrent, even under the previous penalty regime.

In any event, the Court accepted the parties' agreed penalty figure of $5.8 million as within an appropriate range for all contraventions. Justice Halley considered the gravity and scale of the contraventions, but weighed this against mitigating factors such as ACL's cooperation, absence of intentional wrongdoing, remedial measures, and the fact the breaches arose from a single course of conduct. It is clear from the settlement outcome that following this process may result in a final penalty figure that is nowhere near the theoretical maximum.

The decision also clarifies the threshold for triggering assessment and notification obligations – with the Court determining that:

- the third-party investigation on which ACL relied was inadequate, (monitoring only three of at least 127 affected computers and failing to analyse the attackers' methods or potential data exfiltration) and
- once ACL was notified by the ACSC on 16 June 2022 that personal data had been published online, its obligation to notify the Commissioner 'as soon as practicable' was engaged. It was then practicable for ACL to have provided a compliant statement within two to three days, yet it delayed notification for nearly a month.

This decision is likely to serve as a reference point as the first in what is sure to be a long line of enforcement proceedings for data breach if current trends in cybersecurity continue.

DE-RISKING DE-IDENTIFICATION: GUIDANCE FROM OAIC ON HEALTH DATA

Background

At a time when health AI projects face unprecedented regulatory attention, the OAIC's decision to close its preliminary inquiries into I-MED Radiology Network Limited, Harrison.ai, and Annalise.ai (**the Respondents**) offers a rare public blueprint for getting privacy right. This case demonstrates how robust de-identification, combined with strong governance, can enable cutting-edge diagnostic AI without breaching privacy obligations under the Privacy Act.

In an unusual step, the OAIC has published reasons for concluding an investigation, along with an accompanying explanatory statement, which provide a welcome example of how the health sector can responsibly innovate with AI while meeting privacy obligations.

AI, health data, and privacy scrutiny

Between 2020 and 2022, I-MED (Australia's largest diagnostic imaging network) provided Annalise.ai (a joint venture with Harrison.ai) with patient imaging data to develop and train AI models for diagnostic support.

Media reports in late 2024 raised concerns about whether this data sharing complied with the Privacy Act, particularly in the absence of patient consent. The OAIC's inquiries focused on whether the data had been sufficiently de-identified such that it no longer constituted 'personal information' under the Act.

De-identification is central to privacy compliance in the health sector, particularly when using sensitive information for secondary purposes like AI model training. The Privacy Act applies only to 'personal information', meaning information or opinions about an identified individual, or an individual who is reasonably identifiable. If data is de-identified such that re-identification is no longer reasonably possible (even in combination with other data which may be held by the entity to which the information is disclosed to), it will fall outside the Privacy Act's scope so that the Australian Privacy Principles, including APP 6 on secondary use and disclosure, will no longer apply.

De-identifying health data is inherently challenging due to its complexity and richness. Even without names or addresses, datasets may contain variables (age, gender, diagnoses, imaging) that can, in combination, be used to re-identify individuals, especially when linked with other sources. Rare conditions or unique events heighten this risk.

How the Respondents got it right

The Commissioner highlighted how the Respondents' approach to sharing patient data for AI development illustrates effective privacy risk management while enabling innovation in healthcare.

Start with privacy-by-design

The I-MED example shows the importance of embedding privacy considerations at the inception of a project, rather than bolting them on at the end.

For other health organisations, this means conducting a Privacy Impact Assessment (**PIA**) at the earliest stage of system design. A PIA should map each stage of the data lifecycle — collection, processing, sharing, retention, and deletion — and identify where sensitive health information could present high privacy risks.

This early risk assessment enables legal, technical, and operational teams to design de-identification and security measures into the architecture of the AI system from the start.

Use multi-layered technical de-identification

I-MED's approach underscores that no single method of de-identification is foolproof. Instead, I-MED used a suite of complementary techniques, including: removing direct identifiers such as names and addresses; hashing unique IDs; time-shifting dates to break temporal linkages; aggregating data fields to avoid the isolation of rare or unique cases; and redacting any text that appeared on or near image boundaries.

Each measure targeted a different type of re-identification risk, reducing the likelihood that the dataset could be linked back to an individual.

For health organisations, adopting this kind of layered strategy is critical, especially when datasets are rich, diverse, and capable of being cross-matched with other sources.

Reinforce technical measures with contracts and governance

Technical safeguards must be backed by enforceable obligations on each of the parties handling the data.

In the I-MED project, contractual terms prohibited the AI partner from attempting re-identification or disclosing data to third parties, required secure storage environments, and mandated prompt notification if personal information was inadvertently received.

These provisions were coupled with a Data De-identification Policy aligned with recognised standards such as the 5-Safes framework and the National Institute of Standards and Technology (**NIST**) guidelines. The project also maintained clear separation between the environments of the data custodian and the AI developer — a governance safeguard that reduced the risk of accidental or unauthorised data mixing.

Monitor, review, and adapt

De-identification is not a set-and-forget process.

I-MED and its AI partner conducted ongoing monitoring, and self-reported the instances where personal information had slipped through the process.

Those instances were promptly addressed through deletion or further de-identification. This illustrates the importance of ongoing review and testing, to ensure that de-identification objectives are being realized in practice.

Additionally, when regulatory concerns were raised by the OAIC, the Respondents engaged openly with the regulator, providing detailed information and sample data — reinforcing transparency and trust.

Additional guidance for the Health Sector

In October 2024, the OAIC released its 'Guidance on privacy and developing and training generative AI models'. It emphasises privacy-by-design and conducting Privacy Impact Assessments (PIAs) before training or deploying AI models using health data.

Although the I-MED/Annalise.ai project pre-dated this guidance, its approach aligns closely with those recommendations. Health organisations developing or commissioning AI tools — whether diagnostic systems, predictive analytics, or chatbots — should integrate PIAs early in project lifecycles, ensuring privacy considerations are built in from the start.

This guidance should also be read alongside the OAIC's 'Guide to Health Privacy', which sets out how health service providers must collect, use, and disclose patient data securely — even beyond AI contexts.

Together, these guidance documents provide a practical roadmap for health organisations to innovate responsibly while meeting privacy obligations.

International experience

While Australia's Privacy Act sets its own standard for when information ceases to be 'personal information', the health sector can draw important lessons from other jurisdictions that have grappled with similar issues. Overseas regulators have had to balance the need to protect privacy with the imperative of maintaining the utility of health data for research and innovation — a tension that is particularly acute in AI development.

US	In the United States, the *Health Insurance Portability and Accountability Act* (**HIPAA**) provides two recognised methods for de-identifying health information under 45 C.F.R. §164.514(b). • The first, known as **the Safe Harbor method**, requires the removal of 18 categories of identifiers, including names, full addresses, and biometric information. • The second, **the Expert Determination method**, involves a qualified expert applying statistical or scientific principles to determine that the risk of re-identification is 'very small.' While the Safe Harbor method provides clarity and certainty, it can strip datasets of valuable clinical information needed for AI model accuracy. The Expert Determination method preserves more utility but introduces subjectivity, and there have been high-profile demonstrations — most notably by Dr Latanya Sweeney, who re-identified Massachusetts hospital discharge records by linking them with publicly available voter data — showing that even 'de-identified' datasets can be vulnerable to re-identification.
EU	In the European Union, the General Data Protection Regulation (**GDPR**) draws a sharp distinction between personal data and anonymous information. Recital 26 sets a high threshold for anonymity: data must be processed in such a way that individuals are not identifiable 'by all means reasonably likely' to be used by any party. Because true anonymisation is difficult to achieve in complex health datasets, many projects rely on pseudonymisation, where direct identifiers are replaced with pseudonyms but the data can still be re-linked. Pseudonymised data remains regulated as personal data under the GDPR, meaning that compliance obligations continue to apply even where some privacy safeguards are in place. For AI developers, this means privacy law continues to apply to most health datasets used in training models.
UK	The United Kingdom's Information Commissioner's Office (ICO) has also published detailed guidance in its *Anonymisation Code of Practice*. One of its most practical tools is the 'motivated intruder' test, which asks whether a person with access to public information, and with no specialist hacking skills, could nevertheless re-identify data. The ICO warns that anonymisation is not a one-off exercise: technological advances, new linkage techniques, and emerging datasets can erode the protections applied to data that was once considered safe. This mirrors the OAIC's own view that de-identification should be treated as a continuous process, informed by context and re-assessed over time.

Taken together, these international experiences underscore a common theme: de-identification is not binary, nor is it permanent. It must be approached as an ongoing, risk-based exercise that combines technical measures with governance frameworks, contractual controls, and regular re-testing.

Key Takeaways

Key Takeaways for Health Sector AI Projects

- De-identification is a process, not a product — treat it as ongoing risk management, not a one-off fix.
- Context matters — assess re-identification risk in light of the nature of the data, the data environment and potential linkages.
- Combine technical and organisational controls — governance is as important as technical rigour.
- Be proactive and transparent — review processes regularly, monitor for disclosures, remediate quickly.
- Align with best practice frameworks — use models such as the 5-Safes and the OAIC Guidance.

What the Health Sector can do now

- Map all current and planned AI projects involving health data, noting where de-identification is relied on.
- Conduct or update PIAs to address both Privacy Act compliance and various OAIC Guidance.
- Embed privacy-by-design into procurement and vendor contracts, with explicit obligations on de-identification and security.
- Train teams on emerging AI privacy risks, including re-identification threats.

DIRECT MARKETING – ENFORCEMENT DEVELOPMENTS UNDER THE SPAM ACT AND INTERACTIVE GAMBLING ACT

In 2024 the OAIC set out its views on the application of Australian Privacy Principle 7 (which concerns direct marketing) to pixel technologies. The Commissioner stated publicly in late 2025 that an investigation relevant to that issue is underway, so we will likely learn more in 2026.

So far the Commissioner has not exercised its new enforcement power to issue an infringement notice alleging contraventions of APP 7.[3]

The infringement notice is the form of enforcement favoured by the Australian Communications and Media Authority (**ACMA**), the regulator with responsibility for enforcing the *Spam Act 2003* (Cth) (**Spam Act**), the *Do Not Call Register Act 2006* (Cth) and the **Interactive Gambling Act** *2001* (Cth) (*Interactive Gambling Act*). APP 7.8 provides that APP 7 does not apply to the extent that any of those laws apply. In practice, this means that the ACMA, rather than the OAIC, has oversight of most forms of electronic direct marketing.

Personalised SMS and WhatsApp messages are just like any other form of commercial electronic message

In 2025 the ACMA announced the outcome of investigations into contraventions of the Spam Act by 2 betting companies, Tabcorp and Betfair. Both of these cases dealt with personalised marketing messages, as opposed to the same form of message sent to many recipients at once as part of a marketing campaign. These betting companies assigned account managers to be the primary point of contact for a cohort of 'VIP' customers. In many cases the customers and the account managers exchanged messages frequently.

The ACMA applied the provisions of the Spam Act strictly and found that the betting companies had contravened the Act. The lessons to be learned from the investigations include:

(a) a message sent by an account manager in response to a query from a customer can still be a 'commercial electronic message' if it contains content that appears to be promotional. For example, in the Betfair investigation report, the ACMA found that the following message sent by SMS was a commercial electronic message that required consent:

> *'Hi [NAME], sorry it's taken me a few days to get back to you about your MatchMe issue. I popped $200 in your account on Tuesday morning! Hope you've been well.'*

On this approach one might wonder whether the ACMA would consider that a bank had sent a 'commercial electronic message' if an account manager sent an email offering a reduced interest rate for a mortgage in response to an email from an existing customer complaining that the interest rate being charged by the bank was uncommercial.

(b) the fact that an account manager and a customer frequently communicate with each other and the customer knows who the account manager is, and the company that the account manager works for, does not relieve the sender from its obligation to include sender identification details in every commercial electronic message.[4]

3. Privacy Act, s13K(1)(v)-(viii)
4. See Investigation Report for Tabcorp, para 35

An infringement notice for just over A$4 million was issued to Tabcorp, and for just over A$870,000 to PointsBet. Both companies also gave enforceable undertakings through which they committed to remediation activities, under the supervision of an independent consultant, over a lengthy period (3 years for Tabcorp and 2 years for Betfair).

Push Notifications under the Interactive Gambling Act and implications for the Spam Act

A scheme known as the National Self-Exclusion Register commenced operation in 2023. It allows Australian consumers to self-exclude from all interactive wagering service providers in a single process.

In 2025 the ACMA announced the outcomes of investigations into the compliance by 2 online betting companies, PointsBet and Buddybet with the requirements of that scheme. Amongst other things, the scheme prohibits the sending of a 'regulated electronic message' to a consumer who has self-excluded.

The ACMA found that both companies had breached the Interactive Gambling Act by sending in-app push notifications to consumers who had self-excluded.

This development is significant because the same definition of an 'electronic address' is used in the Interactive Gambling Act and the Spam Act. Many organisations have previously expected in-app push notifications to fall within the direct marketing provisions in the Privacy Act, which require a simple opt-out mechanism somewhere within the app. If the more prescriptive requirements of the Spam Act apply instead, each such notification that contains promotional content (for example, retail offers, travel deals, loyalty program offers) would need to include sender identification and express opt-out instructions.

ACMA's reasoning in the PointsBet and Buddybet decisions

Both PointsBet and Buddybet published an app that could be installed on a mobile device (with Apple's iOS operating system or Google's Android operating system) to enable users with a betting account to place bets. Each of those apps allowed the publisher to send 'push' notifications to phones or tablets on which the apps were installed. Some of those notifications were promotional in nature.

ACMA decided that these notifications were 'electronic messages' sent using particular kinds of telecommunications services '*to an electronic address in connection with (i) an email account; (ii) an instant messaging account; (iii) a telephone account; or a similar account*'. In each case the app generated a token, unique to the user's device, as an address for receipt of push notifications.

The ACMA determined that the unique device tokens used to deliver the push notifications constituted an 'electronic address', enabling the betting company to send specific messages to specific users. Further, the ACMA found that the user's Apple or Google account used to download the app was a 'similar account' connected with that address. In considering the question of similarity, the ACMA said that the Apple and Google accounts were '*similar to an email, instant messaging or telephone account as, amongst other features, they allow an account holder to be targeted and communicated to*.'

This may come as a surprise to some who would not naturally equate an account used to download apps from the Apple AppStore and the Google Play platform, which may serve multiple purposes, with accounts for email, instant messages and telephone services, which used for dedicated communication channels. We expect that this aspect of the ACMA's reasoning would be closely scrutinised if the issue is ever tested in court.

Interestingly, the ACMA investigated PointsBet at the same time for suspected contraventions of the Spam Act. Their investigation report into the Interactive Gambling Act contraventions found that 1768 push notifications sent by PointsBet had, as one of their purposes, the purpose of advertising or promoting licensed interactive gambling services, which would result in them being 'commercial electronic messages' for the purposes of the Spam Act if the ACMA applied consistent reasoning. But the Spam Act investigation report only referred to messages sent by email and SMS.

We will need to wait to see whether the ACMA decides in one of its Spam Act investigations whether in-app push notifications are a form of 'commercial electronic message' and whether the target of that investigation has the appetite to challenge the ACMA's interpretation. In our experience, a Spam Act investigation by the ACMA often reveals a range of contraventions such that the likelihood of a harsher civil penalty being imposed by a court is sufficiently high to deter companies from seeking judicial review of the ACMA's more adventurous interpretations of the Spam Act. This is because:

(a) the ACMA only has power to issue an infringement notice in respect of conduct that occurred within the 12 month period prior to the notice[5], and some systematic issues can go unremedied for more than a year, whereas there is no such restriction in court proceedings; and

(b) the maximum civil penalties that can be imposed by a court are twice those that can be imposed under an infringement notice.[6]

Given these dynamics, it is possible that future ACMA investigations may find that in-app push notifications are 'commercial electronic messages' (amongst a number of other clear contraventions) and that finding may go unchallenged.

5. Spam Act, Schedule 5, section 3(2).
6. Compare Spam Act s25(3) and Schedule 5, section 5(1)

PROTECTING CHILDREN'S PRIVACY

Development of an Australian Children's Online Privacy Code

Following the passing of the *Privacy and Other Legislation Amendment* Act 2024 in September 2024, the Privacy Commissioner has been tasked with developing a Children's Online Privacy Code (**Code**).

The Code is intended to put children at the centre of privacy protections in Australia, with an explicit intention to leverage insights from international counterparts such as the UK's Age Appropriate Design Code.

The Code, which must be registered by 10 December 2026, will specify how online services accessed by children must comply with the APPs. It may also impose additional requirements provided these are not inconsistent with existing principles.

An APP entity will be bound by the Code if:

- the entity is provider of a social media service, a relevant electronic service or designated internet service (terms defined under the Online Safety Act with a broad scope that capture most if not all online services);
- the service is likely to be accessed by children (a criteria that may be difficult to apply in practice, particularly for services broadly used by a wide range of users, including both adults and children, that are not specifically targeted at children); and
- the entity is not providing a health service.

The Commissioner may also specify additional APP entities, or a class of entities, that must comply with the Code.

The Commissioner is obliged to consult widely on the development of the Code. Two rounds of consultation have already been completed. The first involved children, parents and relevant organisations focused on children's welfare, while the second involved civil society, academia and industry stakeholders. The Commissioner is now working on a draft of the Code, with the aim of releasing the draft for public review and consultation in early 2026. The public consultation must be open for at least 60 days.

The OAIC must also consult with the eSafety Commissioner and the National Children's Commissioner before registering the Code.

A closer look at the UK's Age Appropriate Design Code

The Privacy Commissioner has indicated that, to the extent possible, in developing the Code it will seek to align with international frameworks, including, the UK's Age Appropriate Design Code (**UK Code**). An analysis of the UK Code should therefore provide an insight as to what the Code could entail.

The UK Code was developed to provide guidance on standards of age-appropriate design for online products and services, such as apps, programs, websites, games, and connected toys or devices, which are likely to be accessed by children. The UK Code was required to be produced under the Data Protection Act 2018 but is not itself binding. It sits alongside the UK General Data Protection Regulation (**GDPR**) which governs the collection and handling of personal data of both adults and children.

The standards in the UK Code provide that:

- The best interests of the child should be a primary consideration in the design and development of a service;
- Data protection impact assessments should be undertaken to assess and mitigate risks to children who are likely to access the service;
- A risk-based approach should be taken to recognising the age of individual users and ensure the standards are applied effectively with appropriate certainty;
- Privacy information and terms should be presented in concise, clear, age-appropriate language, with additional explanations at the point of data use;
- Children's personal data should not be used in ways that could harm their wellbeing or contravene industry or regulatory standards;
- Published terms, policies, and community standards should be consistently upheld;
- Privacy settings should be set to 'high privacy' by default unless a compelling, child-focused reason justifies otherwise;
- Only the minimum personal data necessary for the child's active use should be collected and retained, and children should be offered choices over which features to activate;
- Children's data should only be shared if there is a compelling reason, always considering the child's best interests;
- Geolocation should be off by default, with clear indications when it is active, and location visibility should reset to off after each session;
- Children should receive age-appropriate information about parental controls and clear signs when monitoring is active;
- Profiling should be off by default unless justified by a compelling reason, and safeguards should be implemented to protect children from harmful profiling effects;
- Nudge techniques should not be used to encourage children to share unnecessary data or reduce their privacy protections;
- Connected toys and devices should include effective tools to ensure compliance with the Code's requirements; and
- Prominent, accessible online tools should be offered for children to exercise their data rights and report concerns.

A failure to comply with the UK Code may result in enforcement action by the UK Information Commissioner for a breach of the UK GDPR. In this sense, the Code being developed in Australia will be different to the UK Code, as it will be binding in and of itself. If a relevant entity fails to comply with the Code, it may face enforcement action by the Privacy Commissioner, even if there is no breach of any other underlying compliance obligations under the Privacy Act.

Other developments in children's privacy

In June 2025, the UK Parliament passed the *Data (Use and Access) Act 2025* (**DUA Act**). The DUA Act amends, but does not replace, other data protection legislation in the UK, including the UK GDPR. The objective of the DUA Act is to promote innovation and economic growth, while still protecting privacy interests.

While many aspects of the DUA Act are designed to make things easier for businesses, there are also additional requirements of note. In particular, in the context of children's privacy, the DUA Act requires providers of services likely to be accessed by children to have 'particular regard to children's higher protection matters' when designing and developing their systems. 'Higher protection matters' are defined to include age-appropriate presentation of privacy information, prominent default privacy settings, and minimisation of geolocation.

This amendment effectively embeds the key principles of the UK Code into underlying data protection laws. While the development does not create any further compliance burden for service providers already satisfying the requirements of the UK Code, it indicates a continuing sharp focus on protecting children's personal data.

Multinational businesses that have designed their services to comply with the UK Code and the requirements of the DUA Act should be well placed to comply with the Code being developed in Australia. Nonetheless, it will remain important to keep a close eye on the Code to identify potential quirks and points of difference against international standards. We expect that any material differences that may impose different design considerations beyond those already in place in the UK and elsewhere, will be strongly opposed by entities that offer services with a global audience in mind. As always, such entities will strongly advocate for harmonisation with global standards, in order not to unnecessarily increase the cost of doing business in Australia.

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

PETA STEVENSON

PARTNER
SYDNEY

TEL +61 2 9296 2492
MOB +61 438 289 743
EMAIL peta.stevenson@au.kwm.com

KIRSTEN BOWE

PARTNER
BRISBANE

TEL +61 7 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

JAMES RUSSELL

PARTNER
MELBOURNE

TEL +61 3 9643 4204
MOB +61 449 844 755
EMAIL james.russell@au.kwm.com

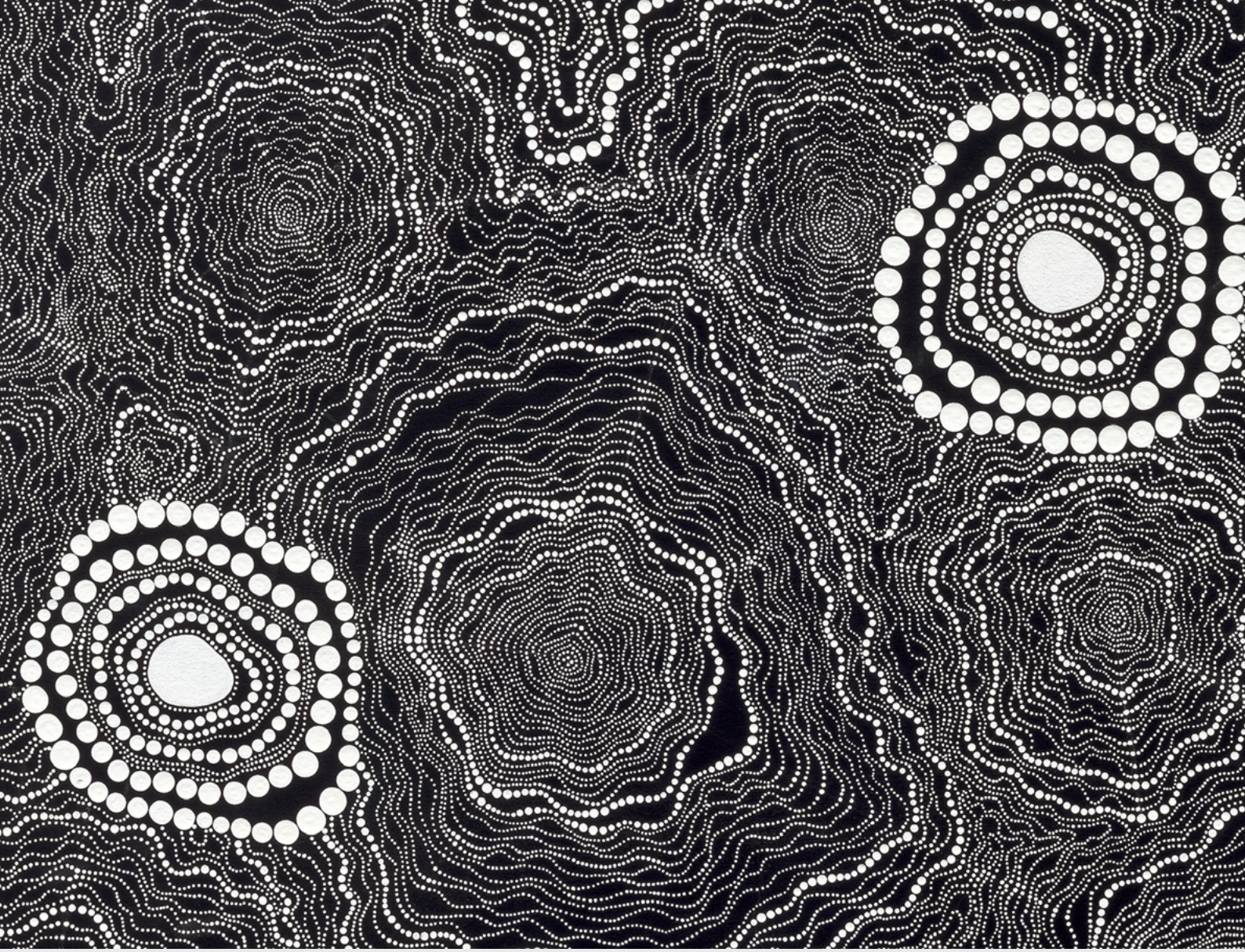
BEN KIELY

PARTNER
MELBOURNE

TEL +61 3 9643 4241
MOB +65 457 735 183
EMAIL ben.kiely@au.kwm.com

Additional contributions & acknowledgements

Cal Samson, Luke Hawthorne, Sophie Crowe, Claris Foo, Inna Kuzminykh and Alana Stone.



ABOUT KING & WOOD MALLESONS

A firm born in Asia, underpinned by world class capability. With over 3,700 lawyers in 26 global locations, we draw from our Eastern and Western perspectives to deliver incisive counsel.

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