

The Three Sisters by Bianca Gardiner

PRIVACY ANNUAL UPDATE

2024

KING&WOOD
MALLESONS
金杜律师事务所

INTRODUCTION

Each year, we write this publication to recap the key developments in Australian privacy law over the past year. What a momentous year this was! with a long-running law reform process finally resulting in the [Privacy and Other Legislation Amendment Bill 2024 \(Cth\)](#) (the **Bill**) landing in Parliament in September (and after some minor tinkering in the Senate passing in a rush of legislative activity on the final sitting day of the year).

While the Bill was widely considered to be anticlimactic, implementing only a limited first ‘tranche’ of reforms, it nevertheless represents a major landmark. The more impactful aspects of the Bill include the establishment of a new statutory tort for serious invasions of privacy (something that Australian lawmakers have flirted with for many decades) and a significant expansion of the Australian Information Commissioner’s enforcement powers.

We have written extensively on the Bill and its potential implications. You can access highlighted articles via the links in the panel below and learn more by visiting the [KWM Data and Privacy page](#). So, although there is no doubt the Bill was the major talking point in privacy law this year, we will avoid taking up additional space discussing it in our Annual Review. Instead, our focus will be on the other privacy law developments that you may have missed amidst all the excitement.

There is certainly no shortage of ground to cover, with many of the more nuanced and sometimes contentious areas within the current law having received some fresh and much-needed scrutiny over the past year. And with a newly enforcement-focussed regulator, and a multiplicity of privacy-related claims hitting the courts, the rate of change is unlikely to slacken any time soon.

These are important developments, and we hope you will find value in reading our take on their implications for Australian businesses. No doubt there will be further exciting developments in 2025, as we look forward to the next tranche of Privacy Act reforms.

As always, please reach out at any time to a member of the KWM Privacy Team if you would like to discuss the potential impact on your business. To stay in touch with privacy and other tech-related regulatory developments, please remember to visit and bookmark the [KWM Tech Regulation Tracker](#).

The following KWM articles dive into more detail on the recent changes to the privacy reform Bill.



[**Privacy Act Reforms – A Long Running Saga, Yet Still to be Continued...**](#)



[**Breaking down the Privacy Amendment Bill**](#)



[**Data Wars Part III: Statutory tort, incoming!**](#)



[**Data Wars Part IV: Enforcement reforms in the Privacy Amendment Bill**](#)

C O N T E N T S

04

**WRAPPING UP THE LATEST
PRIVACY LAW CASES**

13

**MORE DATA BREACHES
- SO WHAT?**

16

**ACMA EXPECTATIONS
ON SPAM**

20

**DARK (AND WIDESPREAD)
PATTERNS**

22

**OAIC GUIDANCE ON USE OF
EMERGING TECHNOLOGIES**

28

ENFORCEMENT TRENDS

33

CONTACTS

WRAPPING UP THE LATEST PRIVACY LAW CASES

FLEETING STORAGE OF PERSONAL INFORMATION AMOUNTS TO COLLECTION

[Commissioner Initiated Investigation into Bunnings Group Ltd \(Privacy\) \[2024\] AICmr 230.](#)

What was this case about?

This decision considers the application of the Australian Privacy Principles (APPs) to the use of facial recognition technology (FRT) in retail settings. Between November 2018 and November 2021, Bunnings Group Limited (Bunnings) used FRT in 63 stores across Victoria and New South Wales. The FRT system captured images of customers' faces via CCTV footage, which were then converted into vector sets that were checked against a database of individuals deemed to pose a risk to customers or staff, or of criminal conduct. The verification process occurred in real time, largely within the random access memory (RAM) of the relevant system server, with the facial images of non-matched customers being deleted within an average of 4.17 milliseconds of creation.

The investigation focused on whether Bunnings complied with.

- **APP 3.3** – regarding collection of sensitive information,
- **APP 5.1** – regarding notification on collection of personal information, and
- **APP 1.2 and APP 1.3** – regarding open and transparent management of personal information.

The decision is one of the first published decisions of the recently appointed Privacy Commissioner, Carly Kind, and is notable for its considered treatment of a technology the subject of interest from privacy activists and retail businesses alike.

What was the Commissioner's decision?

The Commissioner found that the use of the FRT system to obtain still images of customers' faces and to create associated vector sets amounted to a 'collection' of personal information under the APPs. This was despite the facial images and vector sets of non-matched individuals being deleted on average within 4.17 milliseconds of creation, with the Commissioner finding that even momentary storage in random access memory in Bunnings' servers was sufficient to amount to collection 'for inclusion in a record'.

The Commissioner also found that the CCTV footage, facial images and vector sets were 'sensitive information' on the basis that the footage and facial images constituted 'biometric information that is to be used for the purpose of automatic biometric verification or biometric identification' and the vector sets were 'biometric templates'.¹

¹ See paragraphs (d) and (e) of the definition of 'sensitive information' in s6(1) of the Privacy Act.



In response to the Commissioner’s assertion that Bunnings had collected sensitive information, Bunnings sought to rely on certain of the permitted general situations in s 16A of the Privacy Act (which modify the application of certain APPs where relevant conditions are met). Specifically, Bunnings argued that permitted general situations 1 (relating to public health or safety) and 2 (relating to unlawful activity or serious misconduct relating to an entity’s functions or activities) applied.

These exceptions apply where an entity reasonably believes that particular conduct involving handling of personal information is reasonably necessary for a defined purpose (ie to lessen or prevent a safety risk or to take appropriate action in relation to unlawful activity). The exceptions are only expressed to apply to ‘personal information’ and so on their face do not apply to sensitive information that is not also personal information. Nonetheless, the Commissioner appears to have proceeded on the basis that the exceptions were relevant in this case, presumably on the basis that the sensitive information used by the FRT system was also, in the Commissioner’s view, personal information, though this point not addressed in detail in the decision.

In any event, the Commissioner found that the FRT system was not a suitable or proportionate response to the risks identified by Bunnings, taking into account the availability of alternatives and other relevant considerations. In particular, the Commissioner found that the widespread collection of sensitive information through the FRT system was not a proportionate response to address actual or suspected unlawful activity by a relatively small number of individuals in limited circumstances. On the basis that permitted general situations 1 and 2 did not apply, and in the absence of consent, the Commissioner found that Bunnings had breached APP 3.3.

In addition to breach of APP 3.3, the Commissioner also found that Bunnings breached.

- **APP 5.1** – on the basis that Bunnings’ in-store notices and privacy policy did not adequately inform customers as to the use of an FRT system to collect sensitive information, the purpose of such collection, or the consequences for individuals if the information was not collected.
- **APP 1.2** – on the basis that Bunnings had taken insufficient steps to assess and address privacy issues relating to the use of the FRT system, including by not performing a Privacy Impact Assessment or Privacy Threshold Analysis prior to implementing the FRT system.
- **APP 1.3** – on the basis that failure to disclose use of FRT in its privacy policy amounted to insufficient disclosure of the kinds of personal information it collected and the means by which it collected such information information.

What are the implications?

Bunnings has indicated that it intends to seek review of the Commissioner's decision in the Administrative Review Tribunal. We expect that issues likely to be relevant to the review include:

- whether the momentary storage in RAM did in fact amount to 'collection';
- whether, in respect of non-matched customers, the CCTV footage, facial images and vector sets generally constituted 'personal information' and/or 'sensitive information';
- the proper approach to assessing whether an APP entity reasonably believes that a collection, use or disclosure is necessary to achieve the outcomes set out in permitted general situations 1 and 2; and
- whether individuals, as invitees to Bunnings' premises, consented to CCTV surveillance and the use of FRT by entering stores that displayed notices at the entry.

While the outcome of the review will be relevant to the ongoing impact of the Commissioner's findings, the decision nevertheless provides important clarity on the Commissioner's positions on key issues relevant to implementation of FRT and other surveillance. In particular, that:

- the Commissioner takes a technical reading of 'collection', finding that any storage of personal information (even if only ephemeral in RAM) will amount to 'collection' of personal information, irrespective of whether the entity intends to retain such information;
- the permitted general situations are to be understood narrowly, and in seeking to rely on such situations, APP entities will need to carefully consider the suitability and proportionality of the relevant practices, as well as whether any less privacy invasive alternatives are viable; and
- use of FRT systems requires thorough consideration of privacy impacts prior to and during implementation, as well as explicit disclosure to customers.

In the wake of this determination, the Commissioner published guidance on the application of the APPs to FRT generally, which we analyse in further detail below. While the law may remain unsettled pending the outcome of the review process, organisations considering use of FRT should carefully consider this guidance in order to mitigate the risk of drawing unwanted attention from the Commissioner.



DISCLOSURE' REQUIRES INFORMATION TO BE READ NOT JUST RECEIVED

Insurance and Care NSW v FMM [2024] NSWCATAP

What was this case about?

This case, brought under the *Privacy and Personal Information Protection Act 1998* (NSW) (the **NSW Privacy Act**), provides some much-needed guidance on what it means to 'disclose' information from a privacy perspective. The key issue was whether Insurance and Care NSW (the **agency**) had disclosed an individual's personal and health information to an insurance broker by mistakenly sending the broker an email with an attachment containing that information. The insurance broker had opened the email but deleted it before opening the attachment.

What amounts to a 'disclosure'?

The NSW Civil and Administrative Tribunal (the **Tribunal**) agreed with the agency's position that the information was never made known to the insurance broker because the attachment was never opened, and so there was no 'disclosure' of information for the purposes of the NSW Privacy Act.

In making its decision, the Tribunal referred to interpretations of the concept of 'disclosure' under other legislation, most notably the NSW Court of Appeal's decision in *Nasr v State of New South Wales* [2007] NSWCA 101 (which concerned an alleged disclosure under the *Criminal Records Act 1991* (NSW)), and accepted the base proposition that the essence of a disclosure is to 'make known' to a person information that they did not previously know.

Importantly, the Tribunal drew a distinction between having access to information, and knowing that information:

'placing information in a person's possession or under the person's control ... does not make that information known to the person ... Having access to information is different from knowing the information.'

While the information in the attachment was made available to the broker, and there was a possibility that the information would be made to known to them, the information was never actually made known to the broker because the attachment was never opened by the broker and so there was no disclosure.

The Tribunal said that the concept of disclosure under the NSW Privacy Act relates to the interaction between a discloser and recipient, rather than solely on to the unilateral actions of the discloser. In particular, the Tribunal said that 'the person to whom the disclosure is made must receive the information before the information can be said to have been disclosed.' The Tribunal said that this was consistent with the objects of the NSW Privacy Act, in the sense that even if a person could have accessed personal information about an individual, the privacy of the individual in question will not be compromised unless the person actually does access the information.

Where information is placed in the control of another person, there may be a separate question as to whether there has been a failure to keep the information secure and protected against unauthorised disclosure, but there will not actually be a disclosure until the person accesses the information in question.

What are the implications?

The interpretation of the concept of 'disclosure' adopted in this decision may lead to some interesting evidentiary challenges in future privacy cases. In particular, if a regulator or other claimant wishes to establish that there has been an unauthorised disclosure of information, they will need to prove not only that the information was placed in the control of a recipient (i.e. that an email was sent) but also that the recipient then actually accessed and reviewed the information (i.e. that the email was opened and read). In some cases, this will be a relatively straight-forward matter (and some technological tools, such as 'read receipts' may assist). However, in other cases, this may prove to be more challenging, including where the precise identity of a recipient may not be known (such as where an email is mistakenly sent to an unknown address).

It is important to note that the Tribunal's decision was made under the NSW Privacy Act, and that a different position could apply under either the Federal Privacy Act, or other State or Territory privacy legislation. In its guidance on the Federal Privacy Act, the OAIC's position is that an entity will be taken to have disclosed personal information where 'it makes it accessible or visible to others outside the entity and releases the subsequent handling of the personal information from its effective control.'

This is obviously a broader approach than what was taken by the Tribunal, and it will be interesting to see whether it may be challenged in future. Similarly, while the OAIC's guidance is that a disclosure can occur even where the information in question was already known to the recipient, the Tribunal suggested, consistently with established authority from the NSW Court of Appeal, that would not be the case under the NSW Privacy Act (though that was not an issue that had to be decided on the facts of the case).

If the Tribunal's narrower approach is extended to the Federal Privacy Act, then further evidentiary complications may arise, with the recipient's state of knowledge at the time of the alleged disclosure possibly needing to be established in order to establish that an unauthorised disclosure has taken place.

The Privacy Act Review Report 2022 (published in 2023)² recommended that a definition of 'disclose' in the Federal Privacy Act be introduced to reflect the OAIC's preferred position and the government's response indicated that the government agreed in principle with this recommendation.³



² [Privacy Act Review Report 2023](#), Proposal 23.6

³ [Government Response - Privacy Act Review Report \(2023\)](#), at p15. As with other 'agreed-in-principle' proposals, this issue was not addressed in the Privacy and Other Legislation Amendment Bill 2024 (Cth), introduced by the government into Parliament in September 2024.

SCRAPING PUBLIC SOURCES FOR COMMERCIAL PURPOSES MAY NOT BE ‘FAIR’

‘AHM’ and JFA (Aust) Pty Ltd t/a Court Data Australia [2024] AICmr 29

What was this case about?

This determination by the Information Commissioner addressed some interesting issues regarding the collection of personal information from public sources, which is becoming an increasingly important topic with the ever-increasing use of generative AI technologies that have been trained with publicly accessible data.

Specifically, this determination concerned a searchable database of court cases developed by Court Data Australia, a database management company, using information drawn or ‘scraped’ from daily court listings. Court Data Australia made the database available as part of a commercial service so that users could search on an individual or business name to identify whether the individual or business in question had been involved in court proceedings. The Commissioner was prompted to investigate this by an individual complainant aggrieved at the inclusion of their information in Court Data Australia’s database.

Is scraping information from public sources ‘fair’?

A key issue was whether the Court Data Australia had collected the information for its database in a ‘fair’ manner. The Commissioner noted the determination by the Administrative Appeals Tribunal in *Clearview AI Inc and Australian Information Commissioner* [2023] AATA 1069 (the **Clearview AI case**). In that case, it was held that photographs scraped from social media and other public websites had not been collected in an unlawful or unfair manner. However, the Commissioner drew a factual distinction between the two cases, noting that in the Court Data Australia case, information had been scraped from court listings that were published for a relatively short period (on the date of the listing) and that the publication did not occur at the instigation of the individual concerned. The Commissioner said that affected individuals were not informed of this activity and, in the circumstances, would not have reasonably expected that their information would be scraped and included in a separate searchable database for a longer period. The Commissioner also noted that the information was also collected for a commercial purpose, which was contrary to the original terms on which the daily court listings data was made available. On that basis, the Commissioner said that the collection was not fair.

What other privacy issues should web scrapers be wary of?

This determination illustrates that information made available publicly on the internet is not necessarily ‘fair game’ from a privacy perspective. It underscores the OAIC’s view that personal information that is publicly accessible is still subject to data protection and privacy laws, a point underscored by the OAIC along with data protection regulators from a number of other jurisdictions (including the UK, Canada and NZ) in an August 2023 [joint statement on data scraping and the protection of privacy](#).

Businesses that want to scrape information from public sources to use for commercial purposes – whether for training AI models or for compiling reference databases – need to carefully consider how they will comply with privacy laws when doing so. In this regard, the Commissioner also considered a number of other compliance issues associated with the operation of the Court Data Australia database:

- **Notice of collection – clear and comprehensive privacy documentation is required**

The Commissioner considered whether Court Data Australia had provided adequate notice under APP 5 about the information collection that was occurring. In the Clearview AI case, the AAT found that there was no practical way for Clearview AI to notify individuals about information being scraped from public websites. While accepting that Court Data Australia could not contact relevant individuals directly, the Commissioner distinguished this case from the Clearview AI case by noting that there were some steps that could have been taken to notify individuals that their information may be collected from court listings, including by Court Data Australia posting a clear privacy policy on its website. The Commissioner found that the policy that Court Data Australia had published was deficient in that it did not disclose how information would be collected from daily court lists. If the policy had been adequate, the decision on the adequacy of notice under APP 5 may have been different.

This underscores the importance of organisations having clear and comprehensive privacy documentation that accurately covers all of their information collection and use activities.

- ***Quality of information – the collecting entity has the onus of implementing an independent level of quality control***

The Commissioner found that, in the context of the service it was providing, and the potential adverse consequences for individuals if incorrect information was provided, Court Data Australia failed to take reasonable steps under APP 10 to ensure that the information it collected was accurate and up to date. While the information was drawn from official public sources over which Court Data Australia had no control, the Commissioner identified two additional steps that could have been taken to ensure the information collected was accurate and up-to-date. The first step was to provide a better process to facilitate requests from individuals to remove or change information in the database. The second, and arguably more important step was to include additional information on the website to clearly articulate the limits of the information provided and to cease inviting users to draw adverse inferences from entries found in the database (noting that a case listing does not of itself provide any indication of the underlying merits of the case). While drawing attention to these limitations may have made Court Data Australia's service less commercially appealing to customers, in the Commissioner's view, it was still a reasonable and appropriate step to take.

This finding illustrates the problems that may arise from simply accepting information at face value, even if taken from a public source, and that there will still be an onus on the collecting entity to implement an independent level of quality control.

- ***Generally available publications – exemptions applied narrowly***

As a side issue, the Commissioner considered whether Court Data Australia's database was a 'generally available publication' for the purposes of the Privacy Act, in which case certain privacy compliance obligations may not have applied to information in the database. The database was available to the public, albeit with some features subject to payment of a fee, but that of its own did not mean that it was automatically a generally available publication.

In particular, the Commissioner determined that it was relevant to consider the relative prominence of the database (noting that while it had a relatively large number of customers, it did not appear on the first page of Google search results for relevant search terms) and that given the volume of information included in the database, the likelihood of an individual record being accessed on the database was relatively low. In addition, the process, which required individuals to register for the use of the database created a barrier to accessing the information. On that basis, the Commissioner found that the database was not a generally available publication. In addition, the Commissioner noted that the same data was held in a backup version of the database, which was not made available to the public, and could clearly not be considered to be a generally available publication.

This relatively narrow approach reflects the limitations in the exceptions recognised under the Privacy Act for generally available publications – based on this outcome, it would be imprudent to assume too readily that information made available on a public-facing website will be treated as falling within the scope of generally available information.

EMPLOYEE RECORDS EXEMPTION REQUIRES A DIRECT CONNECTION TO THE EMPLOYMENT RELATIONSHIP WITH THAT EMPLOYEE

ALI and ALJ (Privacy) [2024] AICmr 131

What was this case about?

This determination considered the scope of the employee records exemption and whether it would apply to enable sharing of an employee's information within a wider workforce.

The respondent in this case operated a wholesale distribution business that employed approximately 3,000 staff. One of the respondent's employees had a medical episode in the work car park as a result of a pre-existing medical condition that they had not disclosed to their employer or colleagues. The episode was witnessed by a group of other employees who assisted in providing first aid before paramedics arrived. The next day, one of the respondent's managing directors wrote an email to approximately 110 other staff indicating that the employee had experienced a medical episode, had been taken by ambulance to hospital and was recovering well. The employee was upset by the email, claiming that it disclosed the fact of her medical episode to other workers who would not have otherwise been aware of it.

Limits of the employee records exemption

A key question was whether the sending of the email was covered by the employee records exemption under the Privacy Act. While the existence of the exemption is widely known, in our experience, organisations are often surprised to learn about the limits that apply – it is certainly not the case that it is a 'free for all' right to dealing with information about employees.

In particular, the exemption only applies where there is an act or practice that is directly related to both (a) a current or former employment relationship between the employer and the individual and (b) an employee record held by the employer. In the present case, the employer fell at the first hurdle. The employer argued that the email was directly related to its employment relationship with the relevant employee because it addressed an incident that happened at work that the employer had an obligation to address for work health and safety reasons.

However, the Commissioner did not agree with this rationale, and said that 'it appears that sending the email directly related to the employment relationship between the respondent and other employees to whom it owed a duty of care'. In other words, the fact that the email related to an incident involving an employee at work did not automatically mean that the sending of an email was directly related to the employment relationship with that employee. Rather, it was more directly concerned with the relationship that the employer had with other members of the workforce.

What are the implications?

This determination aligns with other decisions that have applied a narrow reading of the employee records exemption. For example, in *Jeremy Lee v Superior Wood Pty Ltd* [2019] FWCFB 2946 the Fair Work Commission determined that the exemption did not apply to the initial collection of an employee record, but only to the subsequent handling of that record.

As part of the ongoing reform process, the current Government has agreed in-principle that further consultation should be undertaken on how to provide enhanced privacy protections for employee records, which would inevitably involve some further narrowing or even removal of the current employee records exemption. Given the potential disruptive effects these reforms may have on businesses accustomed to relying on the exemption, this is one of the more contentious reform proposals and so it was perhaps unsurprising that it was not included in the first tranche of reforms. It remains to be seen whether changes to the agenda will be implemented in any future tranche.

UNCERTAINTY REMAINS OVER WHETHER PERSONAL INFORMATION ON A WORK DEVICE CONSTITUTES AN EMPLOYEE RECORD

[Madzikanda v Australian Information Commissioner \[2023\] FCA 1445](#)

What was this case about?

This decision of the Federal Court concerned whether information stored on a work computer would qualify as an employee record under the Privacy Act. It serves as a useful counterpoint to other decisions, such as the one mentioned above, which apply a narrow reading of the employee records exemption.

This case concerned a decision made by a delegate of the Information Commissioner not to continue investigating a privacy complaint made by an employee regarding their employer accessing personal information stored on a work computer they had returned when leaving the business. This included personal emails that had been saved onto the computer and passwords that had been saved on the computer for personal email and other online services.

Status of information on work devices

The Commissioner's delegate found that all information on the work device constituted an employee record on the basis that it had been entered on the device by the employee knowing that the employer's policy was that all data on work devices would be subject to monitoring. In concluding so, the delegate said:

'I consider that you were aware that the work computer was not your private property, and that any data saved to the computer may have formed part of your employee records, as it was subject to routine monitoring and review.

The respondent does not require your consent to access or use the equipment that it issued to you, to perform your employment duties. As the computer was a tool the respondent provided to you to carry out your employment duties, it remains the property of the respondent.

My view in this instance is that as the data you saved on the work computer is required to be monitored in accordance with the respondent's policy, and contravention of such policy would reflect on your performance or conduct as an employee. Therefore, I consider the data to be an employee record.'

Ultimately, the employee's attempt to appeal the delegate's refusal to investigate the matter further was dismissed on other grounds. The Court did not have to decide whether or not the delegate had made an error of law by concluding that personal information saved on the work computer was an employee record. That is perhaps a shame, as it would have been helpful to have a clear judicial statement as to the scope of the employee record exemption, particularly in light of previous decisions, as mentioned above, which have adopted a more measured and restrictive interpretation of the exemption. Certainly, on the face of things, the delegate's initial view that all information stored on a work computer must necessarily be an employee record is somewhat bold, especially when measured against the reality that, notwithstanding relevant work policies, some level of personal use of work devices is reasonably likely to occur.

What are the implications?

While this case does not ultimately shed any further light on how the employee record exemption should be applied in practice, it does illustrate the significant residual uncertainty around the effect of the employee records exemption. We suspect that businesses would welcome any clarity that legislative reform or further judicial consideration may bring.

In the meantime, for more on this topic, you may be interested in reading this article by our employment team on the various employment law issues that may arise when seeking access to an employee's device.

MORE DATA BREACHES – SO WHAT?

Twice a year, the OAIC releases a report on the operation of the mandatory data breach reporting regime that applies under the Federal Privacy Act. The most recent report, covering the period from January to June 2024, was released in September, and adopted a noticeably different tone, with the Privacy Commissioner Carly Kind signalling a shift towards a more practical approach:

'You will observe this report is a little different to previous ones. Our office is evolving our approach in sharing our insights and emerging trends with Australians and the regulated community. There is still statistical information; however, we have focused on providing more succinct guidance and trend observations to help entities comply with obligations.'

OAIC's Notifiable data breaches report, September 2024

In other words, going forward, we should expect these reports to focus not only on the 'what?' but increasingly on the 'so what?'. By distilling specific lessons, the OAIC report allows businesses to avoid the pitfalls that others have encountered when dealing with data breaches.

The latest reporting period saw 527 reported breaches (the highest since the second half of 2020). Helpfully, the report distils the lessons to be learned from these breaches into six key themes and issues:



**MITIGATING CYBER
THREATS**



**EXTENDED SUPPLY
CHAIN RISKS**



**ADDRESSING THE
HUMAN FACTOR**



**MISCONFIGURATION
OF CLOUD-BASED
DATA HOLDINGS**



**RELEVANCE OF A
THREAT ACTOR'S
MOTIVATION IN
ASSESSING A DATA
BREACH**



**DATA BREACHES IN
THE AUSTRALIAN
GOVERNMENT**

1 Mitigating cyber threats

Be proactive and get the basics right!

Noting that 38% of data breaches in the latest reporting period were caused by cyber security incidents, the OAIC's central message is that organisations must take appropriate and proactive steps to keep the information they hold secure. The report underlines the importance of 'basic' measures, such as implementing multi-factor authentication for system access, enforcing strong passwords requirements, implementing layered security controls (to avoid the risk of a single point of failure), ensuring access privileges are appropriate, and implementing robust monitoring processes to detect and respond to unusual or suspicious activities. The OAIC also recommends that organisations have reference to recognised benchmarks and strategies, such as the Australian Signals Directorate's 'Essential Eight' cyber security risk mitigation strategies.

2 Extended supply chain risks

Conduct due diligence and require flow down obligations!

The report highlights ongoing concerns with security throughout the supply chain, with a number of large-scale breaches, including the well-publicised MediSecure incident that affected over 12 million individuals, being traced back to supply chain compromises. In particular, the report notes that security risks extend beyond the first line of the supply chain – the third parties that a company directly contracts with to provide services - to entities, referred to as 'fourth parties', that are subcontracted to supply services to the first line. This is a particular challenge given that customers will often have no direct contractual or legal relationship with these fourth parties. Risk mitigation strategies recommended by the OAIC include conducting enhanced security due diligence before selecting vendors that will be managing high-risk data, maintaining appropriate oversight of supply chains (including by exercising audit rights), and requiring notice from vendors of any subcontracting arrangements with requirements that they flow-down privacy and information security obligations through their own supply chains.

3 Addressing the human factor

Train your people and assess access credentials!

Human failures continue to be a major cause of data breaches, with 30% of breaches in the last reporting period attributed to some degree of human error. Such errors can never be eliminated, but the associated risks can be mitigated. Importantly, one of the few substantive changes proposed in the Privacy Act Amendment Bill was to clarify that the 'reasonable steps' requirement under APP 11 to keep personal information secure includes both organisational and technical measures.

While most organisations understand the importance of strong technical security – e.g. encrypting data, using strong passwords, installing anti-virus software etc – often organisational security measures are less well-developed. Simple organisational safeguards that can be implemented to reduce the risk of human errors include prioritising staff training (with regular refresher training), keeping a close watch on access credentials (with credentials updated or cancelled whenever a worker changes roles so that, at any given point in time, they only have access to information they actually need to perform their current role), and implementing proactive monitoring to promptly address any unexpected or suspicious network activity.

4 Misconfiguration of cloud-based data holdings

Check your cloud security settings!

Cloud service providers often remind their customers that the maintenance of security is a shared responsibility, not something that the customer can simply delegate to the service provider to manage on their behalf. The OAIC agrees with this. Indeed, the latest data breach report stresses that users of cloud services must take responsibility for the configuration of their cloud services, to confirm that all settings are appropriate for the data that will be stored in the cloud. For example, the OAIC has observed that many data breaches result from misconfigured cloud services, with customers configuring services in a manner that enables public access to data that should have been kept private. Security settings should be checked and confirmed whenever there is a system change, to ensure that no security vulnerabilities are introduced. Even in the absence of material system changes, security settings should be regularly audited to ensure that they remain appropriate for the type of data being stored in the cloud. Major cloud providers provide a wealth of information on this, which customers should proactively consult to ensure they are adopting a robust security posture that is suitable for their activities.



5 Relevance of a threat actor's motivation in assessing a data breach

Don't assume threat actors keep their promises!

As the old saying goes, there is no honour among thieves. Certainly, that is the OAIC's view, with the latest data breach report cautioning against putting blind faith in representations made by threat actors who have undertaken a hacking attack. In particular, the report indicates that when assessing the potential risk of harm arising from a security breach, an entity should not place too much weight on the threat actor's assurances, such as promises that they will neither delete nor publish the compromised data. This has been a consistent reason why both regulators and government officials have discouraged the payment of ransoms – there is simply no guarantee that those responsible for the breach will do what they say they will do and not repeatedly return for more ransom payments. It is perhaps worth noting, as a counterpoint, that when making a risk assessment under section 26WG of the Privacy Act it is relevant to consider whether those responsible for a breach 'have, or are likely to have, the intention of causing harm to any of the individuals to whom the information relates'. As such, the threat actor's motivation clearly is a factor that should be taken into account. However, the OAIC's recent report is a useful reminder to not readily assume that a criminal's statements accurately reflect their true underlying intent.

6 Data breaches in the Australian Government Government agencies should be alert!

The latest report shows that the Australian Government continues to be one of the top 5 sectors impacted by notifiable data breaches (with 12% of all notifications in the relevant reporting period relating to government agencies). The statistics also showed that government agencies were relatively tardy in identifying and notifying these incidents. This is a timely reminder that information security is not only a private sector issue - it is equally, if not more, important for government agencies to follow sound information security practices, not least because, unlike in their dealings with private sector organisations, individuals often will have limited discretion as to what they are required to share with government agencies.

ACMA EXPECTATIONS ON SPAM

The Australian Communications and Media Authority (ACMA), the independent Commonwealth statutory body responsible for regulating communications and media services in Australia, continues to be very active in enforcing strict compliance with the requirements of the Spam Act.

ACMA issued significant penalties over the course of 2024 to a number of major consumer brands, including in one case issuing a record \$7.5m fine.

Two trends arising from these cases

01 The ACMA continues to take a strict approach to interpreting the Spam Act. For example, fines have been issued for messages that were primarily transactional in nature (e.g. to confirm order details or to reset account passwords), due to the inclusion of relatively incidental commercial content (e.g. links to social media pages that included promotional material or links to ‘free shipping’ offers). Fines have also been issued for ‘welcome’ emails that outline benefits available to customers who have just signed up to a new service.

02 Organisations continue to fall victim to a variety of human errors, For example when commercial emails are mischaracterised by marketing team members as being ‘transactional’ or ‘service’ messages. Errors of this nature could be avoided, or at least reduced, by implementing robust compliance processes (for example, improved training and additional layers of review and oversight in order to ensure that nothing ‘slips through the net’).

In July this year, the ACMA released a [‘statement of expectations’](#) on the use of consent for direct marketing purposes. According to the ACMA, the statement is ‘designed to assist businesses to meet both consumer expectations and their minimum legal requirements.’ It is worth noting that the statement does not itself form part of the law, and some aspects may arguably go beyond what the law requires. Nonetheless, it is an essential reference for any entity wishing to remain on the ACMA’s good side and is a useful tool that can be used to reduce the risk of becoming the next recipient of an ACMA infringement notice.

Some of the more notable ‘consumer friendly’ practices recommended by the ACMA include:

- **Use a double opt-in process when obtaining consent**

For example, this may involve sending an email confirmation after a person has consented, with an indication of how they can update their preferences in case they change their mind. This avoids the risk of consumers consenting unwittingly or experiencing immediate ‘click regret’.

- **Be cautious when relying on inferred consent**

The ACMA suggests that you should only rely on consent where there is a ‘current or ongoing’ relationship with the individual and the marketing relates directly to that relationship (i.e. it relates directly to goods or services relevant to that relationship). This is consistent with previous advice by the ACMA not to (1) rely upon a single once-off transaction as the basis for an inferred consent or (2) stretch inferred consent to cover marketing for different products ‘such as a bank contacting a current savings account customer to advertise insurance products’.

This reflects a relatively narrow understanding of the way that consumers see their relationship with a service provider – that is, it assumes that consumers will see the relationship as one that is defined by the scope of products they are currently acquiring, rather than by the identity of the service provider or the full scope of products being offered by the service provider. The ACMA’s guidance does not refer to the only decision made by the Federal Court of Australia on the question of whether consent may be inferred when a supplier of goods or services promotes additional products to an established customer.⁴

Our view, consistent with that of the Federal Court, is that there is scope for a different approach to be taken. We think it is somewhat surprising to conclude, for example, that a bank could only send customers marketing information about products that they already acquire from the bank, but not other types of financial services that the bank also offers and that may be commonly acquired by similar customers.

Some of the more notable ‘consumer unfriendly’ practices discouraged by the ACMA include:

- **Using pre-checked tick boxes on consent forms**

This has long been a bugbear of the ACMA and other similar regulators, though unlike in some other countries there is no explicit statutory prohibition on using pre-checked tick boxes as a method of collecting consent.

- **Bundled consents**

The ACMA describes a bundled consent as a situation ‘where a single request for consent is to be used for multiple purposes that does not allow a choice about each purpose’. Again, while bundling has been a bugbear of Australian regulators, including the OAIC, there is no explicit prohibition on bundling of privacy consents. Some level of bundling will likely be justifiable – e.g. it would likely be overkill for a bank to ask a customer for separate consents to send marketing about savings accounts, home loans and credit cards. Nonetheless, it obviously makes sense to consider customer expectations before hard-wiring consents into product T&Cs or using other bundling strategies.

- **Using refer-a-friend arrangements**

Under the Spam Act, consent must be given by the relevant account-holder to whom the marketing communications are directed. Where a consent message originates from a specific account, then the relevant account-holder will be deemed to have authorised the message even if they did not send the message themselves. In other circumstances, the onus of proof will be on the sender to establish that the account-holder has consented. This will be an inherently challenging task when the consent has purportedly been relayed through a third party, as is the case with refer-a-friend schemes. If consents are obtained through an intermediary, it can be prudent to seek some form of indemnity from them to protect against fines or other adverse consequences if it turns out that, in fact, there is no valid consent.

Providing regular compliance training for staff involved in designing and implementing direct marketing campaigns is an important risk mitigation strategy. KWM has developed an online training module, designed for legal and non-legal team members alike, on the basics of the Spam Act. This module can be rolled out to your teams as part of your internal compliance training program. It can also be modified to include specific examples relevant to your organisation, if that would be helpful. Please reach out to a contact at KWM if you are interested in seeing a demo.

⁴ ACMA v Clarity1 [2006] FCA 410 at [96] and [97].

DARK (AND WIDESPREAD) PATTERNS

The Global Privacy Enforcement Network (GPEN), a global network of privacy authorities of which the OAIC is a member, conducts a regular review or ‘sweep’ of online privacy practices around the world. The results of this year’s sweep, released in July 2024, covered more than 1,000 websites and mobile apps and found that use of deceptive design practices remains widespread.

With the potential introduction of a new obligation to be ‘fair and reasonable’ when handling personal information still on the reform agenda in Australia, the results of the GPEN survey are a timely reminder for organisations to revisit their user interface design to streamline customer interactions around privacy where possible.

GPEN sweep - key findings



COMPLEX AND CONFUSING LANGUAGE

89% of websites and apps had privacy policies that were overly long and/or difficult to read



INTERFACE INTERFERENCE

on average, design elements like false hierarchies, preselection and ‘confirm-shaming’ were used to influence privacy choices in **43% of cases**



NAGGING

35% of websites and apps repeatedly asked users to reconsider more than once when they try to delete their account



OBSTRUCTION

obstructive techniques, such as making privacy settings hard to find and creating ‘click fatigue’ for users wishing to update privacy settings, was observed in **39% of cases**



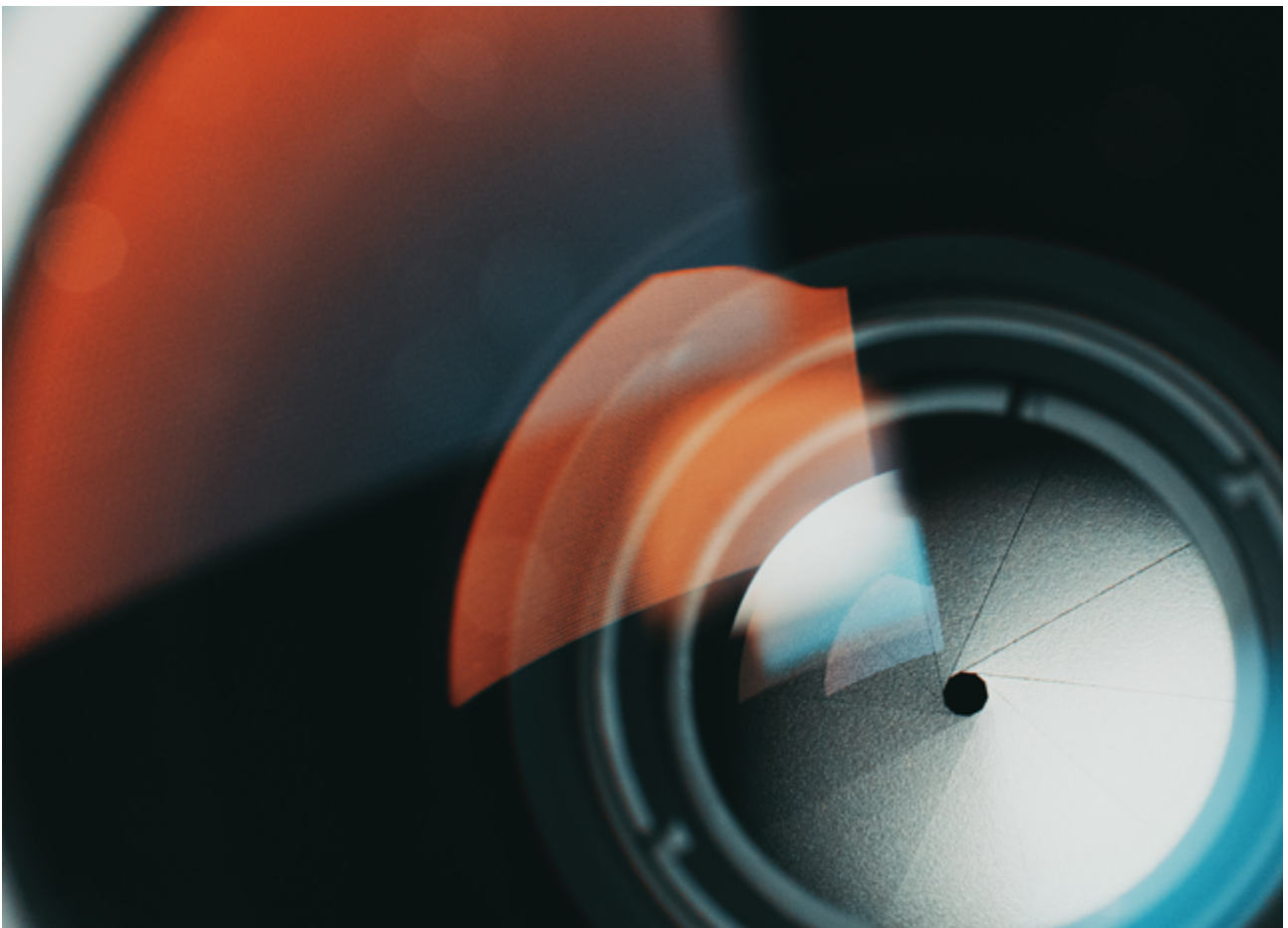
FORCED ACTION

9% of websites and apps forced users to disclose additional personal information when trying to delete their account than when creating the account

OAIC GUIDANCE ON USE OF EMERGING TECHNOLOGIES

The OAIC's [Corporate Plan for 2024-2025](#) indicates that the OAIC proposes to take a 'contemporary' and 'harms-based' approach to regulation and that one of the OAIC's major areas of focus for the coming year will be 'ensuring emerging technologies, including AI, align with community expectations and regulatory requirements'.

Consistent with this aim, the OAIC has recently released new guidance documents about how Australia's existing privacy laws apply to several emerging technologies that the OAIC has previously identified as presenting potential privacy risks: generative AI, tracking pixels and facial recognition. We have summarised the key takeaways from these guidance documents in the following diagrams:



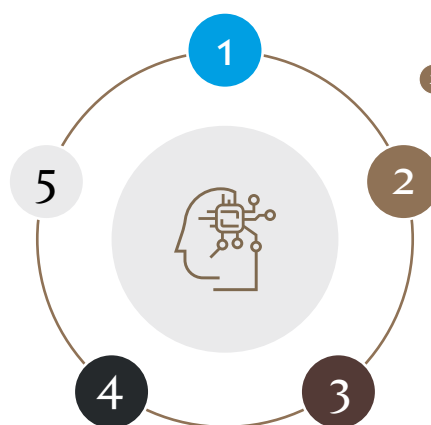
OAIC GUIDANCE ON USE OF AI PRODUCTS

1 Be mindful of privacy obligations when inputting personal information into an AI system

Organisations should conduct due diligence on commercial AI products to ensure they are suitable for the intended uses. Relevant considerations will include whether the product has been tested, how human oversight can be embedded into processes, potential privacy and security risks, and who will have access to personal information input or generated when using the product.

5 Do not enter personal information into public AI tools

The OAIC recommends that organisations do not enter personal information, and particularly sensitive information, into publicly available generative AI tools (such as those used to generate text or images), due to the significant and complex privacy risks involved.



2 Be transparent about use of AI systems

Use of AI tools must be clearly explained to external users. Appropriate policies and procedures should be established to facilitate transparency and ensure good privacy governance.

4 Make sure there is a valid basis for any use of personal information with AI systems

Generally speaking, organisations should only use or disclose personal information for the primary purpose for which it was collected, unless they have consent or can establish that the secondary use would be reasonably expected by the individual, and is related (or directly related, for sensitive information) to the primary purpose. Customer expectations can be shaped by what they are told about proposed use of AI systems in relevant privacy policies and notices

3 Comply with collection rules when using AI systems to generate or infer personal information

AI systems should only be used to generate or infer personal information if it is 'reasonably necessary' and is fair and lawful in the circumstances. Organisations should be upfront about their use of AI and where possible allow customers to opt-out (a collection is more likely to be unfair if customers do not realise it is happening and do not have a choice). Privacy laws will apply to information generated by AI even if it is incorrect (such as hallucinations and deepfakes). Organisations should consider ways to ensure the accuracy of AI outputs, and how to obtain consent if using AI to generate or infer sensitive information about a person.

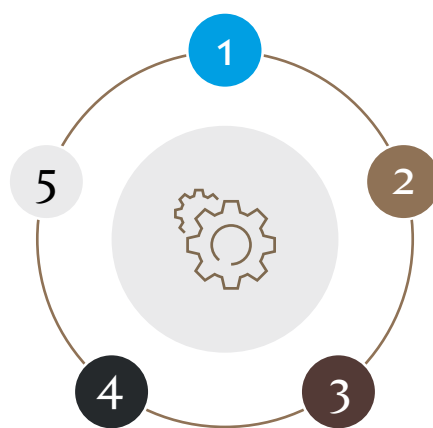
O A I C G U I D A N C E O N D E V E L O P M E N T A N D T R A I N I N G O F A I P R O D U C T S

1 Take reasonable steps to ensure accuracy in generative AI models

Given AI systems are known for producing inaccurate results, developers must take reasonable steps to ensure accuracy, including through using high quality datasets and undertaking appropriate testing. Disclaimers should be used to clearly explain the limitations of any AI system, and additional safeguards should be considered for high privacy risk uses.

5 Before using existing data for AI training purposes, make sure there is an appropriate basis to do so

AI training will likely constitute a secondary use of any existing information collected for other purposes. If they do not have consent, developers must be able to establish that relevant individuals would reasonably expect that their data would be used for that secondary purpose and that it is sufficiently related to the original purpose for which the information was collected. This will usually require clear communication with affected individuals to inform them about the proposed use of their information.



2 Do not assume information can be used to train AI models because it is publicly available

Privacy compliance obligations apply to personal information in the public domain in the same way as they do to private information. Developers proposing to use public data for training an AI model should consider whether the data includes personal information and, if so, whether their collection and use of that information complies with privacy laws. Developers may need to take additional steps – like deleting or anonymising personal information – to ensure that they are compliant.

4 Before using existing data for AI training purposes, make sure there is an appropriate basis to do so

AI training will likely constitute a secondary use of any existing information collected for other purposes. If they do not have consent, developers must be able to establish that relevant individuals would reasonably expect that their data would be used for that secondary purpose and that it is sufficiently related to the original purpose for which the information was collected. This will usually require clear communication with affected individuals to inform them about the proposed use of their information.

3 Take special care with sensitive information

Generally speaking, consent is required to collect sensitive information. This may be problematic where the information is scraped online or collected from a third party. The guidance suggests that a photo of an individual may contain sensitive information where information about the individuals' race, health or political views can be inferred from the photo. This is a controversial view as, taken to a logical extreme, it suggests that consent would be required to use any photo from which an individual can be identified.

OAIC GUIDANCE ON TRACKING PIXELS

1 Tracking pixels are not prohibited but due diligence is required

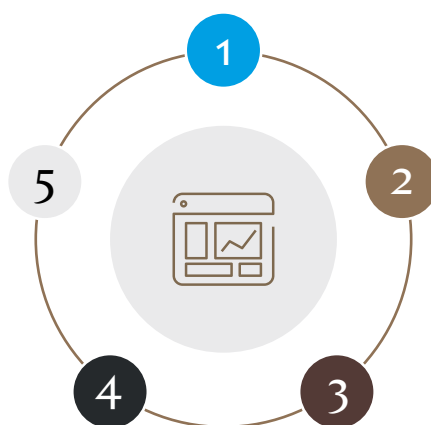
While tracking pixels are not prohibited under the Privacy Act, the onus is on organisations deploying this type of technology (rather than the underlying technology providers) to conduct appropriate due diligence to ensure that their use complies with the Act and the APPs.

5 Regularly review use of tracking pixels

Organisations should conduct regular, ongoing reviews of the tracking technologies deployed on their websites to ensure that their use remains appropriate and complies with privacy obligations. It will be especially important to do this as ongoing privacy reforms take shape, with the next tranche of reforms likely to directly impact on the use of tracking technologies (eg by expanding the scope of the concept of 'personal information' under the Privacy Act and imposing a new obligation to ensure that all collection, use and disclosure of personal information is 'fair and reasonable').

2 Configure tracking pixels to minimise the amount of data collected

Organisations should adopt a data minimisation approach by configuring tracking pixels to collect the minimum necessary information. Pixels should not be used to collect sensitive information without consent. In some cases, where even the fact that a person has visited a website may constitute sensitive information (such as for websites providing mental health or counselling services), tracking pixels should not be used at all.



4 When using tracking pixels for direct marketing, make sure to provide a simple means to opt-out

Organisations that use information collected through tracking pixels to target individuals with online ads must ensure that such targeting complies with rules on direct marketing, including by ensuring that individuals have consented or been notified about the use of their information for this purpose and by providing a simple means for them to opt-out. The guidance suggests the opt-out could be presented as a banner or pop-up when a user first visits a relevant website that uses tracking pixels.

3 Provide clear notice about use of tracking pixels

To ensure that collection of information using tracking pixels is fair, organisations should be transparent about their use of pixels. The guidance notes that a privacy policy is not a substitute for a privacy collection notice, and that information about the use of tracking pixels may need to be presented in different ways in order to ensure that individuals receive adequate notice.

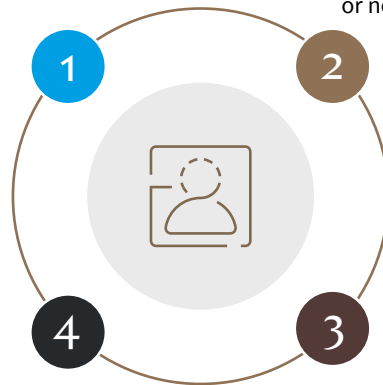
OAIC GUIDANCE ON FACIAL RECOGNITION TECHNOLOGY

1 Only use FRT when necessary and proportional

The OAIC considers that FRT is highly intrusive to an individual's privacy. Personal information should only be used for FRT when it is reasonably necessary – this involves consideration of proportionality and whether other less privacy intrusive means are available to achieve the same outcome (eg alternatives to use of FRT for safety and security may include standard CCTV coverage, security guards, and training for staff on how to identify and deal with safety and security issues). A privacy impact assessment (PIA) should be completed before using FRT to ensure privacy risks are identified and considered.

2 Consider consent and transparency requirements

FRT systems rely upon sensitive information (in the form of biometric information and biometric templates). Generally, this information must only be collected with consent. To be effective, consent must be adequately informed, voluntary, current and specific and given by a person with appropriate capacity. A simple notice indicating FRT is in use will not necessarily be sufficient to establish consent. Individuals should be told that an image will be taken of their face, that biometric data will be generated from the image to be compared against other images, and actions that may be taken if there is a match. They must receive this notice before being subjected to FRT so they can decide whether or not to proceed.



4 Implement strong governance procedures

Organisations using FRT must have clear governance arrangements in place to address privacy risks, which should be regularly reviewed. Apart from carrying out a PIA before using FRT, governance frameworks should include regular training and supervision of staff responsible for handling personal information, controls on system access and entering reference images, a clear data retention / destruction protocol, complaints handling processes, and provision for ongoing review / audit to ensure ongoing compliance.

3 Identify and address risk of errors, bias and discrimination

Before using a new FRT system, an organisation should carry out appropriate testing and trials to ensure that the system will produce accurate results. Controls should be in place to ensure that reference images used by the system are also accurate and up-to-date. Risk of bias or discrimination affecting different demographic groups should be considered as part of testing. Organisations should carry out their own due diligence before relying on third party FRT systems, including by confirming that the system has been subject to robust testing to control for risk of errors, bias and discrimination.

In announcing the AI guidance documents, Privacy Commissioner Carly Kind indicated that the OAIC expects ‘organisations seeking to use AI to take a cautious approach, assess risks and make sure privacy is a key consideration.’ However, the OAIC’s guidance does not necessarily aim to discourage the use of new technologies. Rather, the announcement that accompanied the release of the guidance indicated that the OAIC was focussed on ‘improving compliance through articulating what good looks like.’ This should give organisations confidence that privacy issues should not act as a hard blocker provided that they are prepared to adopt a responsible and considered approach to the implementation of new technologies.

Certainly, the OAIC’s new guidance documents should be essential reference points for businesses looking to develop or use these technologies. Although the guidance is not binding of itself, it does provide clear insight into the way in which the OAIC is thinking about the issues and serves as an indicator of how the OAIC may seek to enforce the law in this area (though notably, earlier in the year, the [OAIC discontinued an investigation](#) into pixel technology on the basis that, given the current state of the law, ‘any litigation or investigation by the OAIC would be on uncertain legal footing’ – slow progress on privacy reforms may force the OAIC to revisit this approach and consider enforcement action even where the state of the law remains uncertain). Businesses that are able to closely follow the best practices outlined in the guidance will be less likely to be in the crosshairs for any future enforcement action.

Of course, privacy is not the only compliance issue that organisations should be mindful of when implementing new technologies. For example, shortly before the release of the OAIC’s guidance on generative AI, the Department of Industry, Sciences and Resources released two consultation papers on proposed guardrails to protect against risks presented by AI more broadly. The proposed guardrails reinforce the importance of thinking holistically about potential risks when experimenting with these technologies. You can read more about KWM’s take on the proposed AI guardrails [here](#), and if you find yourself confused about the rapidly evolving regulatory landscape in this space, you can always consult the KWM map of AI regulation in Australia [here](#).



ENFORCEMENT TRENDS

Recent enforcement activity

The Australian Information Commissioner (**AIC**) has recently increased enforcement activity for alleged breaches of the Privacy Act. This is consistent with recommendations from a strategic review of the OAIC completed in early 2024, which amongst other things recommended a shift towards a more risk-based and education and enforcement focused posture. The AIC's most recent corporate plan indicates an intention to focus on regulatory action where there is a 'high risk of harm to the community' as well as a strategic workforce plan to identify the roles, skills and future training needed to make sure that the OAIC and its personnel can effectively deliver on its enforcement priorities. This renewed focus on enforcement has been supported by recent statutory increases in pecuniary penalties for serious interferences with privacy and the proposed new enforcement regime contained in the *Privacy and Other Legislation Amendment Bill 2024* (the **Bill**).

Of particular interest is the AIC's approach to the number of contraventions of civil penalty provisions which are said to arise from an alleged breach of Australian Privacy Principle 11.1 (being the requirement to take 'reasonable steps' to protect personal information from unauthorised access, misuse or disclosure). In the AIC's civil penalty proceeding against Australian Clinical Labs (**ACL**) (**ACL Proceeding**)⁵ in relation to a cyber-attack, the Commissioner alleges that separate contraventions of section 13G (serious or repeated interference with privacy) arise in respect of each of the individuals about whom the entities hold information (alleged to be 21.5 million people), giving rise to a separate pecuniary penalty of \$2.2m for each individual (under the old penalty regime). Under the AIC's formula, the notional maximum penalty in the ACL Proceeding would be \$47.3 trillion.

The AIC's approach to civil penalties is interesting in light of recent reforms which significantly increased penalties for contraventions of certain provisions of the Privacy Act (from \$2.2m to \$50m or 30% of the value of the contravention or 30% of adjusted turnover during the contravening period). These changes followed submissions from the AIC and other stakeholders to materially increase penalties. It is unclear why such significant penalty increases would have been necessary if, under the older regime, the AIC was able to seek penalties in the trillions of dollars.

In most cases where multiple contraventions arise resulting in a very large notional maximum penalty, the maximum penalty is – practically – of limited relevance in the assessment of the appropriate penalty to impose. This is because the Court is required to determine whether the penalty is: 1) just and appropriate in the circumstances; and that 2) the total penalty for related offences does not exceed what is proper for the entire contravening conduct.⁶ However, in the ACL Proceeding, if there is only one or a small number of contraventions (rather than a contravention for each individual in respect of whom the entities hold information), then the maximum penalty would have a very real role to play as it would effectively act as a cap on the overall penalty that could be awarded.

⁵ OAIC, 'OAIC commences Federal Court proceedings against Australian Clinical Labs Limited' (3 November 2023).

⁶ *Construction, Forestry, Mining and Energy Union v Cahill* (2010) 269 ALR 1; *Australian Competition and Consumer Commission v Australian Safeway Stores Pty Ltd* (1997) 145 ALR 36.

In addition to increased enforcement activity by the AIC, multiple class actions have been commenced against entities impacted by data breaches in the last two years. The Privacy Act does not provide a private right for individuals to commence proceedings against an entity in respect of breaches of the Australian Privacy Principles. Instead, the class action claimants need to allege indirect breaches under other causes of action, including




- **Breach of contract:** customer agreement included an implied term that the entity would comply with the Privacy Act
- **Misleading or deceptive conduct:** the entity represented to customers that they would comply with the Privacy Act
- **Equitable breach of confidence:** the data breach of the third party meant that the entity had misused or disclosed the customer’s confidential information
- **Negligence:** the entity was subject to, and failed to meet, a duty of care to ensure that the personal information was not stolen, and
- **Breach of continuous disclosure obligations:** the entity did not inform the market about alleged deficiencies in its cyber security controls.

The Bill provides for an introduction of a statutory tort for invasion of privacy, which would offer a further purpose-made cause of action that claimants may look to exercise alongside those mentioned above — see our article [here](#), including on the potential impact of the new tort on litigation in this area.

The multi-regulator approach to privacy law enforcement

In Australia, breaches of the Privacy Act can overlap with other regulatory schemes, drawing in different regulatory bodies like the Australian Financial Complaints Authority (AFCA), the Australian Communications and Media Authority (ACMA), and the Australian Securities and Investments Commission (ASIC). This overlap occurs because the Privacy Act is a broad law that applies to many organisations and individuals, while other regulatory schemes have more specific focuses.

It’s not just the OAIC!

 AFCA	 ACMA	 ASIC
<p>AFCA is an external dispute resolution scheme that deals with complaints about financial products and services. It is overseen by ASIC. AFCA can consider complaints about breaches of the Privacy Act that relate to financial products and services.</p> <p>For example, a consumer could complain to AFCA if a bank disclosed their personal information without their consent.</p>	<p>ACMA is responsible for regulating the communications and media industry. It has specific powers to enforce privacy protections that apply under telecommunications legislation.</p> <p>These protections apply to telecommunications companies and internet service providers. ACMA can investigate and take action against companies that breach these protections.</p>	<p>ASIC is responsible for regulating financial markets and services. It has the power to take action against companies whose breaches of the Privacy Act in relation to financial products and services contravene provisions of the Corporations Act.</p> <p>For example, ASIC could take action against a financial advisor who misused a client’s personal information.</p>
<p>As at July 2024, AFCA had 220 open complaints in relation to the Latitude Finance cyber-attack.</p> <p>AFCA is currently working on a lead case in relation to the cyber-attack.</p>	<p>ACMA has filed proceedings in the Federal Court against Optus, alleging that it failed to protect the confidentiality of its customers’ personal information from unauthorised interference or unauthorised access as required under the <i>Telecommunications (Interception and Access) Act 1979</i> (Cth).</p>	<p>On 5 May 2022, following proceedings commenced by ASIC, the Federal Court declared that RI Advice Group, a holder of an Australian Financial Services Licence, contravened s 912A(1)(a) and (h) of the <i>Corporations Act 2001</i> (Cth) as a result of its failure to have documentation and controls in respect of cyber security and cyber resilience in place to manage associated risk.</p>

In some cases, multiple regulators may have jurisdiction over a privacy breach. In the future, we expect this will lead to jurisdictional battles, with each regulator asserting its authority, with the potential for delay, cost and confusion for the parties involved. Common examples include:

- A bank discloses a customer’s personal information to a third party without their consent. This could be a breach of both the Privacy Act and financial services laws. AFCA, ASIC and the OAIC could take action.
- A telecommunications company fails to protect a customer’s personal information from unauthorized access. This could be a breach of both the Privacy Act and the Telecommunications Act. Both ACMA and the OAIC could take action.
- A financial advisor uses a client’s personal information for their benefit. This could be a breach of both the Privacy Act and the financial services regulations. Both ASIC and the OAIC could take action.

CASE STUDY:

Concurrent Optus Disputes

In September 2022, Australian telecommunications company Optus suffered a data breach that affected up to 10 million current and former customers (comprising a third of Australia’s population). The hacker responsible obtained access to a wide range of information, including names, dates of birth, home addresses, telephone numbers, email contacts, and numbers of passports and driving licences.

Class Action	OAIC RCI	OAIC CII	ACMA
On 26 September 2022, Slater & Gordon announced they were investigating ‘a possible class action against Optus on behalf of current and former customers ... affected by the unauthorised access to customer data’.	On 28 September 2022, Maurice Blackburn made a similar announcement, and announced on 7 October 2022 that it had lodged a representative complaint with the OAIC.	On 11 October 2022, the OAIC announced it had commenced an investigation into the ‘personal information handling practices’ of Optus in regard to the cyber-attack.	On 11 October 2022, ACMA announced it had commenced an investigation in relation to the cyber-attack. ACMA has now commenced proceedings against Optus.

The lack of clear and consistent standards across different legislation, regulators and courts creates significant uncertainty for businesses facing litigation. This uncertainty makes it difficult to assess risk, develop effective legal strategies, and predict potential outcomes. Furthermore, the potential for overlapping penalties and remedies from different regulators can increase the financial stakes of litigation.

As we canvassed in [a previous KWM Insight](#), the courts have recently decided that a multiplicity of court cases and administrative investigations into the same incident may run in parallel. The complexity of simultaneous regulatory interventions into one set of facts is only compounded by the potential for concurrent investigations by the OAIC, which can include representative complaints on behalf of a compensable class.

As noted above, Australia is also experiencing a surge in class action lawsuits related to data breaches. The lawsuits represent a mix of consumer-based claims (three in total) and shareholder claims (one). As such, companies unlucky enough to experience a major data breach are likely to face running battles on multiple fronts as both regulators and plaintiffs continue to explore different legal actions in search of appropriate recourse.





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 +61 438 297 018
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

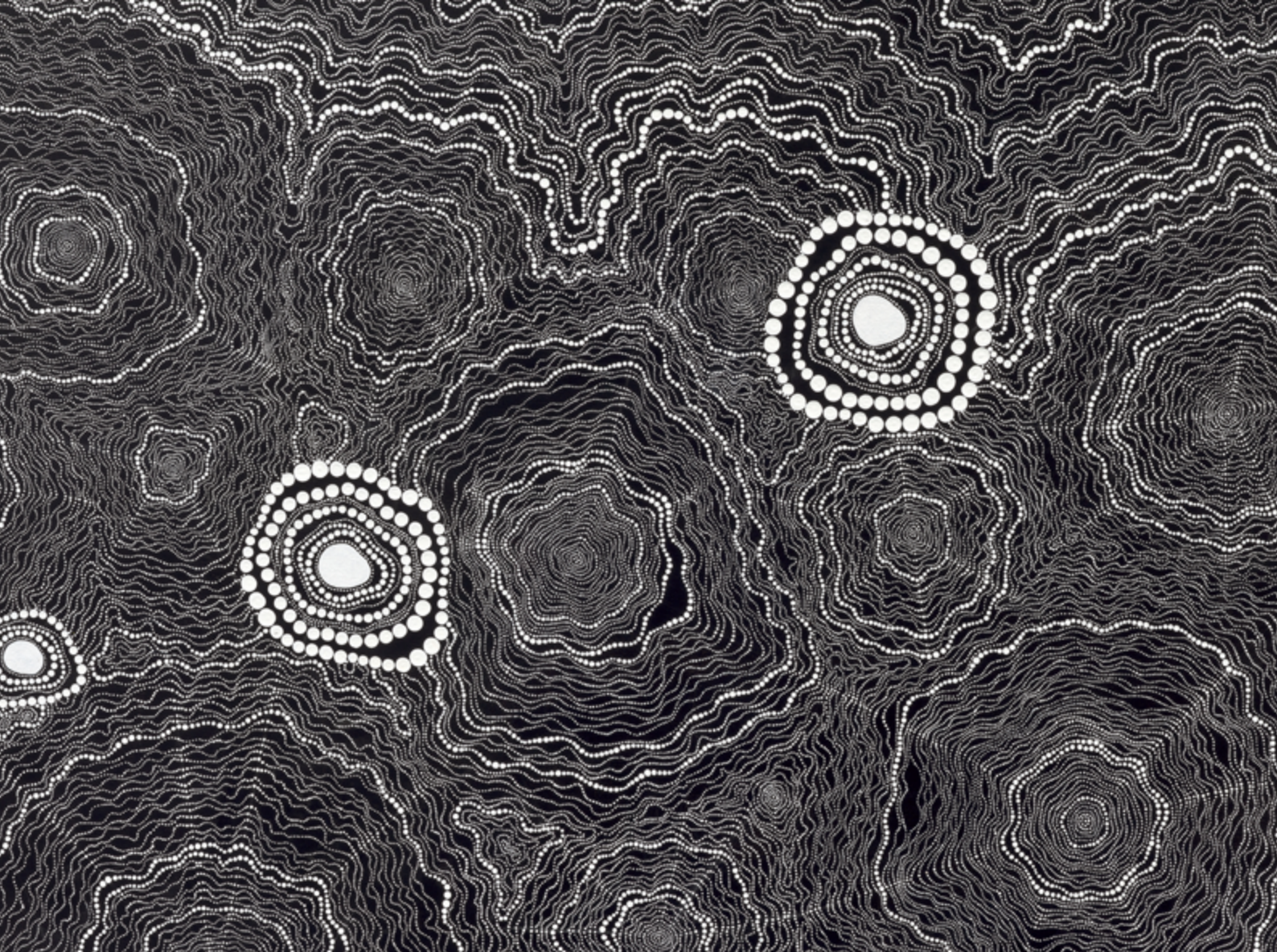
PARTNER
MELBOURNE

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

Additional contributions & acknowledgements

Cal Samson, Kendra Fouracre, Lauren Bourke, Kai Nash, Luke Hawthorne, Eli Solomon, Callum Christodoulou, Vanessa Sporne





ABOUT KING & WOOD MALLESONS

A firm born in Asia, underpinned by world class capability. With over 3000 lawyers in 29 global locations, we draw from our Western and Eastern 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.

Disclaimer

This publication provides information on and material containing matters of interest produced by King & Wood Mallesons. The material in this publication is provided only for your information and does not constitute legal or other advice on any specific matter. Readers should seek specific legal advice from KWM legal professionals before acting on the information contained in this publication.

Asia Pacific | North America

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

www.kwm.com

© 2024 King & Wood Mallesons



JOIN THE CONVERSATION



SUBSCRIBE TO OUR WECHAT COMMUNITY.
SEARCH: KWM_CHINA