
WOTTON KEARNEY
Cyber, Data and Technology APAC Bulletin
Issue 15 (May 2026)

Contents

Please click the heading to navigate to the page

Introduction

Issue 15 of our Cyber, Data and Technology APAC Bulletin is here, covering key developments and insights for insurers, brokers and their customers.

This issue highlights major developments in Australia, including critical lessons from the Medibank case on the limits of legal professional privilege, growing regulatory scrutiny on biometric data following decisions involving Bunnings and 2Apply, and increased enforcement activity from ACMA under spam and telecommunications laws. Cyber governance expectations continue to rise, with proposed amendments to the SOCI Act, updated AML/CTF privacy guidance, and evolving obligations for organisations handling sensitive data and critical infrastructure.

Cyber threat activity also remains elevated with continued ransomware evolution, including the expansion of affiliate models targeting critical networks, and increasing sophistication in supply chain attacks. Australia's broader cyber threat landscape reflects heightened risks across both public and private sectors, alongside emerging concerns such as sanctions exposure in remote hiring practices and large-scale fraud risks in financial systems.

AI, data use and digital innovation remain key focus areas. This edition explores the privacy and security implications of virtual try-on tools, the role of AI within existing consumer protection frameworks, and new global guidance such as NIST's AI cyber framework. Australia's long-term direction is also addressed through national expectations for AI infrastructure investment and regulatory positioning on AI risk.

Across the region, regulatory momentum continues. New Zealand has released its National Cyber Security Strategy and increased focus on children's privacy, while Singapore is advancing AI governance frameworks, mandating stronger cyber standards, and responding to state-linked cyber threats. Thailand is also elevating cybersecurity as a top business risk, alongside increased regional cooperation on cyber resilience and digital trade.

We hope you find this edition both practical and insightful as organisations navigate an increasingly complex cyber, data and technology landscape.

If you'd like to discuss any of the topics covered, please reach out to a member of our team or click here to find out more.

Nicole Gabryk
Partner

Kieran Doyle
Partner

24/7 Cyber Hotline

Wotton Kearney operate a cyber incident response hotline that is monitored 24/7 by our dedicated team of breach response lawyers. By using a lawyer as an incident manager, we can immediately protect key reports and other sensitive communications with your customer and other vendors under legal professional privilege.

Australia

1800 316 706
cyber@wottonkearney.com

New Zealand

0800 9525 2467
nzclaims@wottonkearney.com


Cyber

Limits of Legal Professional Privilege: Lessons Learned From Medibank Case

At a glance:

- The Full Federal Court upholds the primary judgment which rejected Medibank's claim of legal privilege over Deloitte's forensic reports.
- The ruling emphasises that dominant purpose is an objective, factintensive inquiry, assessed by reference to how documents are created, described and used, rather than by subjective intention alone.
- Multipurpose forensic reviews are particularly vulnerable to failing the dominant purpose test, where legal advice does not clearly prevail over other substantial objectives operating in parallel.
- Public statements do not necessarily waive privilege, but they may be powerful evidence of nonlegal purpose at the time a document is commissioned.

Background

The Full Federal Court has recently upheld a firstinstance decision rejecting Medibank's privilege claims over a series of forensic reports prepared by Deloitte following its 2022 data breach[1]. The Court found that the evidence did not establish that the reports were commissioned predominantly for that purpose.

The decision aligns with the earlier Singtel Optus Pty Ltd v Robertson decision and provides a more detailed guidance on how courts approach privilege claims in a corporate cyberincident context, particularly the application of the dominantpurpose test and the types of contemporaneous evidence that may undermine, or support, such claims.

Recap of First Instance Decision

In the first instance decision, summarised here, the Federal Court considered whether various documents produced in response to Medibank's 2022 cyber incident were protected by legal professional privilege. The privilege dispute arose in the context of class action proceedings brought by affected customers following the data breach.

At first instance, the Court drew a distinction between different categories of cyberincident materials. Some cybersecurity and threatresponse documents were accepted as privileged. However, the Court held that three major reports prepared by Deloitte were not protected by legal professional privilege, namely: the PostIncident Review report, the Root Cause Analysis report and the report addressing compliance with APRA Prudential Standard CPS 234.

The primary judge concluded that Medibank had failed to establish that these Deloitte reports were commissioned for the **dominant purpose of obtaining legal advice**. While a legal purpose was present, it was not the "ruling, prevailing or most influential" purpose for which the reports were created.

In the alternative, the primary judge also held that privilege had been waived in part in relation to the PostIncident Review report, on the basis that Medibank's public statements to the ASX public about Deloitte's findings and recommendations were inconsistent with the maintenance of confidentiality.

The Appeal

Medibank appealed the primary judge's findings. The Full Court of the Federal Court (Wigney, Lee and Hespe JJ) reviewed the primary judge's conclusions on two distinct issues:

1. Whether the Deloitte reports were brought into existence for the dominant purpose of obtaining legal advice
2. Whether privilege had been waived by Medibank's public statements.

1. https://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/full/2026/2026fcafc0038

Dominant Purpose: The Full Court's Core Finding

The Full Court unanimously upheld the primary judge's core finding that the Deloitte reports were not created for the dominant purpose of obtaining legal advice.

Subjective Belief vs Objective Assessment

A central theme in the judgment was the distinction between subjective belief and objective assessment. On appeal, Medibank argued that the primary judge misapplied the dominantpurpose test by failing to give determinative weight to the affidavit evidence of its senior executives.

The Full Court rejected that characterisation. While it accepted that Medibank's Chair, CEO and General Counsel genuinely believed that the reports were commissioned to support legal advice, that belief was not determinative. The dominantpurpose inquiry required an objective assessment of all surrounding circumstances:

"The question is not whether the witnesses were honest or even persuasive in describing what they thought. The question is whether, objectively viewed, the legal purpose was the ruling, prevailing or most influential purpose."

The Court emphasised that, for a large, listed entity responding to a major cyber incident, purpose cannot be assessed by reference to the intentions of a small group of senior decisionmakers in isolation. Rather, the inquiry must take into account the full factual context, including how the documents were commissioned, described, used, and embedded within the organisation's overall response.

In that context, the Full Court held that the primary judge was entitled to find that the Deloitte reports served multiple substantial purposes, including regulatory engagement with APRA, governance oversight by the Board, public accountability through ASX disclosures, and forwardlooking remediation. As a result, legal advice could not be characterised as the dominant purpose.

Solicitor-led Structure and the Limits of "Channelling"

The Court also rejected Medibank's reliance on the formal legal framework surrounding the reports. Although the reports were commissioned through external solicitors and the engagement letters contained orthodox privilege language, the Full Court reaffirmed that "channelling" a report through lawyers does not, of itself, determine its character. What mattered was the practical and institutional role the reports were intended to play.

Ultimately, the Full Court concluded that Medibank's appeal amounted to a disagreement with the primary judge's evaluation and synthesis of the evidence. That evaluative exercise was open to the primary judge and disclosed no appealable error. The conclusion that legal advice was not the dominant purpose of the Deloitte reports was therefore upheld.

Was There Waiver of Privilege?

At first instance, the primary judge had concluded that, had privilege existed, it would have been waived in part because Medibank made public statements to the ASX referring to Deloitte's findings and recommendations.

Justice Lee, with whom Wigney and Hespe JJ agreed, held that the primary judge's reasoning on waiver was problematic. The Full Court reaffirmed settled principles that:

- waiver depends on inconsistency with the maintenance of confidentiality, not merely on public references to a privileged process; and
- acknowledging the existence of findings or recommendations does not necessarily disclose the "substance or gist" of a privileged legal communication.

The Court observed that Medibank's highlevel ASX statements were consistent with the conduct of a listed entity informing the market about its response to a cyber incident, while still attempting to preserve confidentiality over the content of any legal advice.

However, that identified error did not assist Medibank. The Full Court dismissed the appeal because the waiver finding was not outcomedeterminative.

Key takeaways

Privilege turns on early purpose-setting, not hindsight

This decision highlights a fundamental point: privilege is not something that can be retrofitted. To determine whether a document attracts legal professional privilege, courts will ask whether, objectively speaking, it was brought into existence for the **dominant** purpose of obtaining legal advice or for use in litigation. Importantly, Courts continue to recognise that properly framed forensic work undertaken for the purpose of enabling legal advice can attract privilege. There remains a clear pathway to protecting the core investigative work where it is appropriately structured and confined to that purpose. As such, proper upfront structuring and early legal involvement is critical, ensuring that the involvement is genuine and substantive, rather than a superficial 'channelling' exercise.

Follow-on and multi-purpose work will not be cloaked with privilege

Difficulties arise where the scope of work expands beyond incident response into broader objectives such as remediation, governance, regulatory engagement or public accountability. In those circumstances, privilege will often not attach, but this is largely because such work may never have been directed predominantly to legal advice in the first place. Properly thought through legal advice should be able to identify early on what work is intended to attract privilege, how that work should be scoped, and what parallel streams may need to be treated differently.

Public statements can inform purpose:

While high-level disclosures do not necessarily waive privilege, they may provide powerful evidence of the purpose for which documents were created. As such, entities should carefully consider, at an early stage, how public, regulatory and stakeholder communications describe external reviews and investigations. Those communications should be aligned with the intended legal purpose of any documents for which privilege is sought.

Conclusion

The Medibank decision makes clear that legal professional privilege in the cyber incident context turns on substance, not form. Courts will apply the dominant purpose test by close reference to objective evidence, including how forensic work is commissioned, deployed and communicated across the organisation, rather than by reliance on labels, engagement structures or asserted intentions.

The central lesson is not that privilege is unavailable for forensic investigations, but that it must be deliberately and carefully established from the outset. Early, substantive and genuine legal involvement is critical in defining the purpose and scope of investigative work, so that core forensic activity is directed toward enabling legal advice and does not become diluted by parallel operational, governance or regulatory objectives.

This decision provides strong, appellate level authority for the proposition that privilege will attach where legal purpose genuinely predominates, but it will not extend to multipurpose or operational material by default. The practical implication is clear: privilege is best preserved through careful upfront structuring, informed legal judgment and disciplined separation of workstreams, not by reliance on form or hindsight after the fact.

Same Problem, Higher Stakes: Supply Chain Risk in the Age of Software

Supply chain attacks aren't slowing down. Late March 2026 delivered two major reminders of just how quickly a single upstream compromise can cascade across thousands of organisations. The latest compromises affecting widely used open-source software libraries, LiteLLM and Axios, demonstrates how attackers can exploit the ecosystem of dependencies to reach victims they never needed to target directly. Following several major package compromises last year, a clear pattern has emerged, one that is becoming increasingly difficult for boards and insurers to overlook.

LiteLLM

On 24 March 2026, a widely used open-source AI library was quietly weaponised against the thousands of organisations that depended on it. LiteLLM, a tool that acts as a central gateway through which businesses interface with AI services like OpenAI, was compromised by a criminal threat actor and turned into a credential harvesting tool.

Because of how deeply LiteLLM is embedded in the technology stack, this compromise gave attackers access to the AI-related credentials of every organisation running it. What makes this incident so impactful is how it unfolded: LiteLLM was not the original target. It was caught in the downstream blast of an earlier attack on a different tool, one that was in LiteLLM's own software supply chain.[2] The attackers never needed to touch the organisations they ultimately affected. They simply moved through the supply chain until they reached something valuable enough to exploit.

Axios

Axios is one of the most commonly used tools that allows web-based software applications to communicate over the internet, it sees over 100 million weekly downloads. On 31 March 2026, attackers briefly gained control of an account used to publish official Axios updates and used it to release altered versions of the software.

Rather than changing Axios itself, the attackers quietly added an extra hidden component that activated automatically when the software was installed.[3] That component was designed to give attackers remote access to the affected computer, potentially allowing them to view data or move further into connected systems. The altered versions were removed within hours, but any organisation that installed them during that window is advised to treat the affected systems as potentially compromised and take precautionary steps, including resetting access credentials.

The Regulatory Lens

This is the nature of systemic supply chain risk, and it is the risk that regulators, insurers, and advisors are increasingly focused on. The exposures here was not a failure of any single organisation's security controls, but rather a failure of the ecosystem of trust that modern technology environments are built upon.

Australian organisations operating under APRA's CPS234 and CPS230 are required to understand and govern the risks introduced by third parties and material service providers (their supply chain). *The Security of Critical Infrastructure Act* (Cth) (**SOCI**), Australian Energy Sector Cyber Security Framework (**AESCSF**) and other legislation / frameworks impose equivalent considerations for operators in critical sectors.

What unites these frameworks is a consistent regulatory expectation: that boards and senior leadership can demonstrate active oversight of the risks that live beyond its own perimeter in its supply chain.

The Governance Gap

The harder question these incidents raise is not whether organisations had the right security tools in place, but rather if they had meaningful visibility into their supply chain risk in the first place. The rapid development and deployment of software-based solutions across business operations has introduced a new layer of technology dependency that has, in many cases, moved faster than the governance frameworks designed to manage it. Notably, as artificial intelligence becomes a routine part of business operations, the pressure to integrate AI-enabled tools quickly has only accelerated this trend, often without corresponding scrutiny of the risks embedded in the underlying technology stack.

2. For more information on how the attack was executed, and the indicators of compromise, see LiteLLM's Security Update post.
3. For more information on how the attack was executed, and the indicators of compromise, see Elastic Security Lab's article.

Developers and technology teams integrating digital capabilities routinely rely on open-source components that carry no contractual protections, no audit rights, and no notification obligations in the event of compromise.[4] When one of those components holds the keys to an organisation's entire environment (as both the LiteLLM and Axios incidents were designed to target), the consequences are a material business risk with regulatory, operational and reputational ramifications.

What Boards Should Be Asking

For boards and risk leaders, the right response to incidents like this is to act before exposure occurs and to ask the right strategic questions:

- Does our supply-chain risk framework account for the software tools and dependencies our teams are adopting?
- Do we have the visibility to know what sits between our organisation and the software we rely on?
- What percentage of our technology estate depends on components with no contractual recourse?
- If one of those dependencies were compromised tomorrow, would we know quickly enough to respond?

Supply chain risk has always been difficult to govern precisely, because it asks organisations to take responsibility for the risks that originate outside their control. However, in an era where supply chain risks exist across every function of the business, providing effective management and aligning with regulatory expectations has never been more challenging.

4. Most popular open-source software licenses provide little-to-no warranties and exclude liability entirely, meaning organisations adopt these tools largely at its own risk. For examples of common open-source licenses, see choosealicense.com. We recommend seeking legal advice before choosing how to license software, WK's team can assist.

Mandatory Ransomware Update

Organisations with an annual turnover exceeding AUD $3 million have been required to report ransomware or cyber extortion payments to the Australian Signals Directorate (**ASD**) within 72 hours of making a payment.

Australia has now entered Phase 2 of the mandatory ransomware reporting regime, adopting a combined education, compliance and enforcement approach. Penalties of up to 60 penalty units, currently AUD $19,800, may be imposed where a captured entity fails to report a ransomware payment within the required 72hour timeframe.

New data released under the scheme indicates that, at the time of writing, large organisations continue to make ransomware payments despite ongoing guidance from the ASD discouraging payment. The Department of Home Affairs has reported that between seven and 13 captured entities, being organisations with annual turnover of at least AUD $3 million, paid a ransomware demand each month. Equating to 75 captured entities making ransomware payments over the period from June 2025 to January 2026.

In addition, organisations operating in the critical infrastructure sector reported a further 19 ransomware payments during the same period. This brings the total number of known ransomware payments made by Australian organisations since the commencement of mandatory reporting obligations to 94.

Why Ransomware Payments Continue to Occur

The available reporting data confirms that ransomware payments continue to be made by Australian organisations, despite possible penalties. Factors often associated with ransom payment decisions may include:

- **Criticality of systems and services**
  Where ransomware impacts systems that support core business functions, essential services or safetycritical operations, organisations may have limited tolerance for prolonged outages. In these circumstances, even short operational delays can result in significant financial loss, regulatory exposure or broader service consequences, increasing the pressure to restore systems as quickly as possible.
- **Data extortion and downstream exposure**
  Many ransomware incidents involve the exfiltration of sensitive data in addition to system encryption. Threats to publish or misuse that data can raise concerns around regulatory scrutiny, legal liability and reputational harm, particularly where affected information includes personal, customer or commercially sensitive data.
- **Decisionmaking under extreme time pressure**
  Ransom demands are typically accompanied by short deadlines and escalating threats. Payment decisions may be made while technical investigations are ongoing and before the full scope of compromise, recovery options or legal implications are fully understood.

Implications for Insurers and Insureds

The persistence of ransom payments reflects the operational and commercial pressures organisations face during severe cyber incidents rather than compliance attitudes. For insurers, this highlights the importance of understanding insureds' system criticality, resilience measures and incident response frameworks.

For insureds, the evolving threat landscape reinforces the need for advance planning. Clearly mapped system dependencies tested incident response and recovery strategies and predefined escalation and reporting processes are key to managing ransomware incidents while limiting both operational disruption and regulatory risk.

Australia's Cyber Threat Landscape

Australia enters 2026 with cyber risk remaining persistently elevated across healthcare, financial services, government, education, and professional services. Early 2026 threat intelligence indicates sustained exploitation activity, with no signs of stabilisation across these sectors. Cyber risk should now be understood as a continuous operational condition rather than an episodic disruption.[5]

AI-enabled acceleration of cyber attacks

The integration of artificial intelligence into cyber attacks has altered the threat environment facing Australian organisations. Threat actors are now deploying AIdriven automation at scale, accelerating reconnaissance, phishing, and vulnerability exploitation in ways that significantly increase both the speed and volume of attacks. Early 2026 intelligence confirms this shift is widespread and shows no signs of abating.[6]

Incident data gives weight to this assessment. A majority of organisations globally have experienced an AIled or AIassisted cyber incident in the past 12 months, rising to approximately 70% in some sectors.[7] These incidents continue to arise through familiar vectors, including phishing, credential compromise, and exposed cloud services.[8] AI has not fundamentally altered where organisations are vulnerable. It has amplified how quickly and consistently those vulnerabilities are exploited.[9]

Where automated and self-directed attack tools are deployed, the average time to compromise has compressed from hours to seconds, significantly narrowing the window for detection and human intervention.[10] The result is a growing mismatch between attack velocity and organisational response capability. Many organisations remain reliant on reactive detection, with a substantial proportion only responding once an incident has already caused damage.[11] This exposes the limitations of governance, escalation, and decisionmaking frameworks that were not designed for the pace at which threats now move.[12]

As attack speed increases, the tolerance for delay has faded. Whether an incident is contained or escalates is now largely determined by the controls, authority structures, and escalation pathways established before compromise occurs.

Geopolitical escalation and indirect exposure

Geopolitical developments are reshaping Australia's cyber risk environment in ways that are both indirect and difficult to predict. Cyber operations are now routinely deployed alongside military, economic, and diplomatic measures, with malicious activity increasingly directed at globally connected platforms and shared digital infrastructure.[13] Compromising widely used cloud services, software platforms, or managed service providers allows threat actors to affect large numbers of organisations simultaneously through a single point of failure. Rather than targeting individual organisations directly, attackers can exploit shared dependencies to amplify disruption across sectors and jurisdictions.

The escalation of conflict in the Middle East in early 2026 demonstrates this directly. Heightened cyber activity by state-aligned actors and proxy groups extended well beyond the immediate conflict zone, propagating through third-party dependencies embedded across jurisdictions.[14] The cyber incident affecting medical technology manufacturer Stryker is a clear example. While Australia was not a party to the underlying conflict, Australian hospitals moved into alert status due to their reliance on Stryker systems. This demonstrates how offshore geopolitical escalation can rapidly translate into domestic operational risk through supplier dependencies alone.[15]

For boards, the implication is not that geopolitical events can be predicted or controlled, but that cyber oversight must account for how external disruption spreads through technology dependencies and supply chains.

5. World Economic Forum, Global Cybersecurity Outlook 2026 (Insight Report, January 2026).
6. SecurityBrief Australia, 'Australia Warned Over AIFuelled Surge in Cyberwarfare' (2026).
7. Armis, A World Under Pressure: Cyberwarfare in an Age of AIFueled Escalation (2026) 6–7, 15.
8. Cloudflare, 2026 Threat Intelligence Report (March 2026).
9. Armis (n 3) 16–17.
10. Armis (n 3) 2–4.
11. Armis (n 3) 8–9.
12. World Economic Forum, Global Cybersecurity Outlook 2026 (n 1) ch 3.2.
13. Ibid.
14. Lean Security, Weekly Australian Cyber Threat & Vulnerability Deep Dive (February–March 2026).
15. ABC News, 'Australian Hospitals on Alert After Iranian Hackers Attack Medical Technology Company Stryker' (13 March 2026).

Supply chain concentration and accountability

Supply chain concentration and third-party dependency remain structural drivers of cyber risk, independent of attacker intent. Reporting in early 2026 continues to highlight recurring incidents involving misconfigured cloud environments, permissive identity settings, and vulnerable APIs within vendor systems, particularly those operating at scale.[16]

Failures within globally concentrated providers can generate simultaneous downstream impacts across multiple organisations. The February 2026 incident involving fintech platform youX illustrates this directly. Although the compromise occurred within youX's environment, multiple broker organisations were affected through their reliance on the platform, exposing a significant volume of personal and sensitive information.[17]

This dynamic sharpens the question of accountability. Organisations remain exposed to regulatory, contractual, and reputational consequences even where compromise occurs entirely within a supplier environment beyond their direct control. Governance frameworks that focus primarily on internal controls, without equivalent emphasis on dependency risk, supplier assurance, and escalation rights, are increasingly misaligned with how cyber risk manifests in practice.

16. Cloudflare (n 4).
17. Lean Security, *Australian Cyber Incident Briefing: youX Platform Compromise* (February 2026).

Practical recommendations

In the current threat environment, organisations may wish to take the following steps.

1. **Incident response readiness and testing**
   Organisations should ensure incident response arrangements are operational and decisionready, rather than purely documented. This includes preauthorising timecritical decisions and engaging key external advisers – including forensic, legal, communications, and insurance specialists – in advance of any incident. Readiness should be regularly tested through realistic scenarios that validate escalation pathways from detection to executive decisionmaking, including outside normal business hours.

2. **Stakeholder and regulatory notification preparedness**
   Boards and executive teams should actively prepare to meet stakeholder, regulatory, and contractual notification obligations. This requires a clear understanding of notification triggers, defined decisionmaking authority, and established coordination mechanisms across internal teams and external forensic and legal advisers.

3. **Supply chain and third-party risk accountability**
   Organisations should extend cyber oversight beyond internal systems to reflect dependency on suppliers, cloud providers, and shared platforms. Clear ownership of third-party cyber risk should be established, supported by appropriate assurance over critical vendors and defined escalation and response rights for incidents originating within supplier environments.

4. **Data holdings and shared data exposure**
   Organisations should maintain an accurate and current understanding of the data they hold, including its volume and sensitivity, particularly where data is shared with third parties. Regular review of data retention practices and accountability arrangements helps reduce exposure and ensures that notification and liability risks are understood before incidents occur.

2Apply rental application app ruled to have unlawfully collected data

In a first-of-its-sector determination, the Office of the Australian Information Commissioner (**OAIC**) has found that rental application platform 2Apply[18] 'interfered with the privacy of individuals whose personal information was collected'.[19]

Determination and declarations

Subject to Part V of the *Privacy Act 1988* (Cth) (**Privacy Act**), the OAIC is empowered to investigate acts or practices that may be an interference with the privacy of an individual or a breach of Australian Privacy Principle (**APPs**).

On 1 April 2026, the OAIC released its decision and reasons for decision following a commissioner-initiated investigation into 2Apply's practices in relation to the collection and use of personal information. The OAIC ruled that 2Apply had:

1. collected 'personal information that is not reasonably necessary for its functions or activities, in breach of Australian Privacy Principle (**APP**) 3.2'; and
2. collected 'personal information by unfair means, in breach of APP 3.5.'[20]

Accordingly, the Commission made several declarations in respect of 2Apply, including that it stop collecting certain types of information and conduct an external review of its practices and mitigation measures at its own expense (and to be shared with the OAIC).

Context

From its reasons, the OAIC selected the rental technology (**RentTech**, as referred to in the Decision) sector as a regulatory priority because it sits at the centre of a structurally imbalanced and highrisk market. The Commissioner recognised an inherent and significant power imbalance in the rental sector, compounded by Australia's ongoing rental crisis, which leaves individuals with limited choice and heightened vulnerability when seeking housing.

In practice, prospective tenants are often compelled to use third-party digital platforms chosen by agents, with no realistic ability to refuse or negotiate the terms on which their personal information is collected. In this context, the collection of personal information occurs under pressure, rather than through genuine choice or meaningful consent, in circumstances where housing is an essential need rather than an ordinary consumer service.

The OAIC was further concerned that RentTech platforms operate at scale and routinely collect large volumes of sensitive and nonessential personal information, increasing the risk of unfairness, discrimination and harm if that information is misused or compromised. The Commissioner emphasised that these platforms are not passive intermediaries but active collectors and designers of data-gathering processes, including interface design that can pressure individuals into disclosing more information than required.

Given the sector's reach, its role as a gatekeeper to housing and the cumulative privacy and security risks arising from excessive data collection, the OAIC viewed regulatory intervention as necessary to set clear standards and drive systemic change across the industry.

APP 3.2

APP 3.2 requires an APP entity to collect only personal information that is reasonably necessary for one or more of its functions or activities, applying an objective standard that goes beyond what may be merely helpful, convenient or desirable.

The OAIC found that APP 3.2 had been breached because the 2Apply platform systematically collected personal information that was not required to assess a person's suitability for a rental property or to facilitate the processing of tenancy applications.

In particular, the Commissioner identified categories of information that did not meaningfully establish an applicant's identity, capacity to pay rent, or likelihood of caring for the property. These types of personal information included gender, detailed dependant information, student and bankruptcy status, citizenship / visa details, bond / rent assistance status, prior living arrangements, vehicle details and emergency contacts.

18. 2Apply is a web-based rental application platform provided by IRE Pty Ltd, trading as InspectRealEstate.
19. IRE Pty Ltd (Privacy) [2026] AICmr 24 (1 April 2026) [1] (Decision).
20. Decision [1].

While the collection of the information above in the context, per the OAIC's determination, was in itself a breach of APP 3.2, the OAIC raised additional concerns compounding the impact of the breach, including:

- **Heightened discrimination risk:** the routine collection of several of these data points increased the risk of unlawful discrimination and profiling in the tenancy application process, particularly in light of federal and state antidiscrimination laws and the preexisting power imbalance faced by rental applicants (as discussed above).
- **Overcollection at the outset**: much of the information was collected from all applicants as a default, despite only ever being relevant, if at all, to successful tenants or later stages of the rental process.
- **Availability of less intrusive alternatives**: reasonable, less privacy-intrusive means were available to achieve the same purposes, particularly in relation to identity verification.

In collecting this breadth of information as a default practice, 2Apply went beyond what a reasonably informed entity would consider necessary, resulting in excessive data collection and an increased risk of privacy harm, contrary to APP 3.2. The Commissioner accordingly declared that 2Apply not collect, or reduce the information it collects, in relation to various types of personal information.

APP 3.5

APP 3.5 requires personal information to be collected by lawful and fair means, directing attention not just to *what* information is collected, but *how* and *in what circumstances* the collection occurs.

The OAIC found that the unfairness arose not simply from the fact of collection, but from the circumstances in which the collection occurred. The Commissioner had regard to the collection taking place within a rental application context characterised by limited choice and a significant power imbalance (as discussed above), combined with the respondent's practice of excessive and default data collection from all applicants at the outset. This was exacerbated by the security and harm risks associated with the volume of information collected, and the use of Online Choice Architecture techniques that pressured applicants to provide more personal information than they otherwise would.

Taken together, these factors rendered the means of collection unfair, resulting in a breach of APP 3.5.

Key takeaways for organisations

The 2Apply determination is a timely reminder that privacy compliance is not just about having a collection notice or obtaining information for a broadly legitimate business purpose, it is also about whether each category of personal information is objectively necessary, collected at the right point in the process, and requested in a way that is fair in the circumstances.

For organisations that collect customer, employee or applicant information, the decision underscores the increasing regulatory focus on data minimisation, fairness of collection practices, and interface design. In practical terms, organisations should treat this decision as an opportunity to review whether its current data collection settings have evolved beyond what is genuinely required. Some practical steps might include:

- **Map personal information across processes:** Identify what information is collected, when it is collected, why it is collected, who it is shared with, where it is stored and how long it is retained. This can help surface over-collection, duplication and unnecessary retention.
- **Test whether collection occurs at the right stage:** Consider whether certain information is only needed later in the customer or applicant journey, rather than being collected by default at the outset.
- **Review digital forms and user experience design:** Examine whether online forms, mandatory fields, prompts or workflows may be nudging individuals to provide more information than is genuinely required.
- **Assess whether less intrusive alternatives are available:** Where the organisation's objective can be achieved in a lower-risk or less privacy-intrusive way, those alternatives should be considered and, where appropriate, adopted.
- **Refresh governance, policies and internal decision-making:** Document the rationale for collecting each category of information and ensure privacy, legal, product and operational teams are aligned on those decisions.
- **Seek legal and privacy advice early:** Targeted advice can help test whether collection practices are likely to satisfy APP 3.2 and APP 3.5, particularly where collection occurs through digital platforms, third-party tools or high-volume processes.

Understanding Sanctions Risk in Remote Hiring - A Case Study of North Korean IT Workers

Recent investigations have highlighted the sanctions risks associated with remote hiring, particularly where workers' true identities and locations are obscured. This issue has taken on heightened significance under Australia's sanctions regime, which operates on a strict liability basis. The focus is not on what an organisation knew or intended, but on whether it took reasonable precautions and exercised due diligence. For organisations engaging remote or offshore workers, this framework increases the importance of robust hiring, onboarding, payment and ongoing monitoring controls to mitigate sanctions exposure.

What happened

Last month, *60 Minutes* [21] reported on a coordinated scheme involving IT workers linked to the Democratic People's Republic of Korea (DPRK). The investigation documented how these workers obtained remote IT roles with Australian and international organisations while concealing their true identity and location. Once engaged, salaries and contract fees were redirected to the DPRK regime, generating foreign revenue that international authorities have linked to nuclear weapons and ballistic missile programs. These findings align with previous warnings issued by the Department of Foreign Affairs and Trade (**DFAT**) about the sanction's risks associated with overseas labour and remote IT services. [22]

How sanctions law applies to remote hiring of DPRK workers

At a high level, sanctions are legal restrictions imposed by the government to limit certain dealings in response to matters of international concern.

In the case of the DPRK, international and domestic sanctions are expressly aimed at preventing the regime from generating foreign income through overseas labour, including remote IT services. Regulations made pursuant to s 10 of the *Autonomous Sanctions Act 2011 (Cth)* [23] (**Sanctions Act**) Australian persons are prohibited from making assets available, or providing services, where those dealings directly or indirectly benefit a sanctioned regime. Therefore, if an Australian organisation unknowingly engages a DPRK IT linked worker and pays for services, that payment may amount to a prohibited dealing, even where the worker's true identity or location has been concealed.

Consequences of breaching sanction laws

Contravening Australian sanctions law can have serious consequences. Under section 16 of the Sanctions Act [24] a breach of a sanctions prohibition is a criminal offence. Corporations are subject to strict liability, meaning intent or knowledge of their wrongdoing is not required, and penalties can reach up to $3.3 million. However, a limited defence is available where a company can show it took reasonable precautions and exercised due diligence [25]. For businesses that rely on remote hiring and overseas contractors, this makes sanctions due diligence critical.

Mandatory due diligence - what Australian organisations should be doing

The Australian Sanctions Office (**ASO**) emphasises a risk based, proportionate approach rather than a checklist exercise. Due diligence generally operates at two levels. At a baseline level, organisations should have appropriate governance arrangements, periodically assess their exposure (including reliance on overseas labour), screen counterparties against Australia's Consolidated List, train staff on sanctions risks, and implement suitable access controls for remote workers.

21. 60 Minutes Australia, 'IT workers at big tech companies revealed as North Korean spies | 60 Minutes Australia' (YouTube, 29 March 2026) 00:00:00–00:27:22 <https://www.youtube.com/watch?v=klcw6vpmAHI>
22. Department of Foreign Affairs and Trade (Cth), *Cyber Risks of DPRK IT Workers to Australian Businesses* (Advisory Note, 6 November 2025) < https://www.dfat.gov.au/international-relations/security/sanctions/guidance/cyber-risks-dprk-it-workers-australian-businesses> and Department of Foreign Affairs and Trade (Cth) , *Democratic People's Republic of Korea (DPRK) Information Technology (IT) Workers* (Advisory Note, 24 February 2026) < https://www.dfat.gov.au/international-relations/security/sanctions/guidance/cyber-risks-dprk-it-workers-australian-businesses>.
23. *Autonomous Sanctions Act 2011* (Cth) ('Sanctions Act') s 10.
24. Ibid s 16
25. *Department of Foreign Affairs and Trade (Cth), Sanctions Compliance Toolkit (Compliance Toolkit, 24 February 2026), <https://www.dfat.gov.au/international-relations/security/sanctions/guidance/sanctions-compliance-toolkit>*

Where higher-risk activities are involved, such as engaging remote IT workers through online platforms, additional controls are expected. These may include enhanced identity and location verification, cautious payment arrangements through established financial channels, and ongoing monitoring to confirm that key assumptions remain accurate over time.

Moving forward

Remote work and global talent platforms are now a standard feature of many Australian businesses. As the DPRK IT worker scheme illustrates, these models can expose organisations to sanctions risk where identity, location and payment flows are not properly verified.

Australia's strict liability sanctions regime means the key question is whether reasonable precautions and due diligence were in place at the time services were provided and payments made. For organisations engaging remote or offshore workers, particularly in higherrisk roles such as IT and data access functions, sanctions compliance must be treated as an ongoing operational risk. Embedding sanctions risk into workforce governance helps reduce the likelihood of inadvertent breaches while allowing organisations to continue benefiting from flexible and global hiring models.

From penalty to private action: the next phase of the ACL Medlab litigation

Australian Clinical Labs Limited (**ACL**) is now facing class action proceedings arising out of the 2022 cyberattack on its former subsidiary, Medlab Pathology the latest, and perhaps consequential, development in one of Australia's most closely watched privacy and cyber enforcement matters.

The proceedings follow the Federal Court's October 2025 decision imposing a $5.8 million civil penalty on ACL for breaches of the *Privacy Act 1988* (Cth) in connection with the Medlab incident. That decision was historic as the first civil penalty handed down under the Privacy Act and set a new benchmark for how courts assess organisational cyber governance, breach response, and accountability. What is now emerging is the private litigation layer that many commentators expected to follow.

The class action follows a now familiar trajectory, a significant cyber incident prompts regulatory investigation, and once the facts are established through regulator findings and court judgments, private claimants assess whether that record can sustain claims for loss or damage. In the ACL matter, that foundation is already well established. The Medlab cyberattack involved the theft and dark web publication of sensitive health and personal information, deficiencies in cybersecurity preparedness, and delays in detecting, assessing and notifying the breach findings that underpinned the Federal Court's penalty decision and now provide the factual framework against which the class action will be assessed.

What makes the case particularly notable is the extended arc of the litigation. The cyberattack occurred in early 2022, regulatory proceedings commenced more than a year later, and the penalty decision was handed down in late 2025. The class action prolongs that arc further, reinforcing that cyber events can give rise to multi-year legal exposure as regulatory outcomes feed into subsequent private claims.

The proceedings also illustrate how cybersecurity increasingly sits at the intersection of governance, disclosure and enterprise risk. The Court's earlier findings focused on systemic shortcomings rather than isolated technical failures, including inadequate resourcing, limited boardlevel oversight and the handling of acquisitionrelated cyber risk. Those same themes are likely to feature prominently in the private litigation phase, where causation and loss will be assessed against the organisation's governance record.

Viewed in this light, the ACL class action is less about a single pathology provider and more about how cyber risk is now judicialised in Australia. Cyber incidents increasingly generate layered consequences across regulators, courts and claimant groups over multiple years, with each phase informed by the last and early failures in preparedness and response can crystallise into long-tail legal exposure long after the immediate incident has passed.

Proposed Amendments to the SOCI Act and CIRMP Rules

Earlier this year, an Independent Review led by Dr Jill Slay AM (**Independent Review**) into the *Security of Critical Infrastructure Act 2018* (**SOCI Act**) was delivered. Which found that while the SOCI Act has in-built a strong foundation for safeguarding critical infrastructure assets, and significantly improving national security and resilience, the evolving threat landscape means the framework itself must continue to adapt.[26]

The Independent Review included several recommendations, and the Department of Home Affairs (**Department**) is now progressing the first tranche of initiatives, including:

- proposed amendments to Ministerial Directions Powers in Part 3 of the SOCI Act; and
- Exposure Draft of the enhancements of the Critical Infrastructure Risk Management Program (**CIRMP**).

The Department will consult on both initiatives until 1 May 2026.

Ministerial Directions Powers

The amendments to the ministerial directions powers includes five targeted measures aimed at providing "*greater flexibility and precision*" in managing risks to critical infrastructure. Section 32 of the SOCI Act enables the Government to issue directions to reporting entities or operators of critical infrastructure asset to refrain from undertaking specified acts or activities.

There are several pre-conditions to the exercise of this power, therefore the Department proposes to:

- replace the existing requirement for an '*adverse security assessment*' from the Australian Security Intelligence Organisation (**ASIO**) with a requirement to obtain ASIO advice;
- enable the Minister to impose targeted conditions where risks arising from ownership, control or governance give rise to a material national security concern;
- permit the temporary deferral of continuous disclosure obligations to ASIC under the *Corporations Act 2001 (Cth)*, where disclosure of high risk cyber incidents could compromise national security;
- allow coordinated action with a specific vendor or its products, equipment, services or technologies present systematic supply chain vulnerabilities, including directions to cease use, isolate technologies or implement procurement restraints; and
- increase penalties for non-compliance with ministerial director powers from $412,500 to $3.3 million.

Enhancements to the Critical Infrastructure Risk Management Program Rules

Additionally, the Department is proposing amendments to the *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023* (**CIRMP Rules**) for specific asset classes, across energy, communications, water and sewage, and transport.[27]

Key proposed amendments include:

- Cyber security framework uplift: require entities to comply with maturity level 2 of their chosen cyber maturity framework, for example Essential Eight, ISO 270001, NIST CSF 2.0;
- Critical systems network protection: require entities to include in their CIRMP how they have segregated between their asset's critical systems, and other internet connected, or less secure components, that could result in the compromise of, substantive loss of access to, or deliberate or accidental manipulation of a critical system;
- Multi-factor authentication: where not already present, entities must outline in their CIRMP how phishing resistance MFA is used to authenticate users, privileged and unprivileged users of critical systems and remote access; and

26. See https://www.homeaffairs.gov.au/help-and-support/how-to-engage-us/consultations/consultation-ministerial-directions-powers-and-draft-of-amended-cirmp-rules
27. This will include critical energy market operator assets, critical electricity assets, critical gas assets, critical liquid fuel assets, critical water assets, critical broadcasting assets, critical domain name systems, critical freight service assets, critical freight infrastructure assets.

- Personnel security hazard risks: require entities to establish and maintain a personnel security plan. This will involve mandatory AusCheck background checks for critical works every 5 years.

For SOCI regulated organisations, the proposed reforms will:

- increase scrutiny of ownership, governance and supplychain arrangements, with a greater likelihood of targeted ministerial intervention where national security risks are identified;
- require higher baseline cyber security maturity, including demonstrable controls around network segmentation, phishingresistant multifactor authentication and personnel security;
- impose more prescriptive CIRMP documentation and uplift expectations for how risks to critical systems are identified, managed and evidenced;
- expose entities to materially higher penalties for noncompliance; and
- require early planning to ensure governance, risk management and incident response frameworks can meet the enhanced regulatory expectations.

Organisations should begin assessing gaps against the proposed requirements and consider whether to engage in the consultation process ahead of implementation.

CBA probes 1b in suspected fraudulent home loans

On 27 February 2026, Commonwealth Bank of Australia (**CBA**) reported itself to police and regulators after identifying up to $1 billion in potentially fraudulent home loans following an internal review of home loan documentation and compliance processes.[28] The investigation into Australia's largest bank was triggered by internal whistleblower complaints, first made on 15 February 2025, through CBA's internal reporting mechanisms and has focused on loans originated through broker and referral channels[29].

CBA intensified its assessment after police disclosed the existence of a criminal network known as the Penthouse Syndicate, which allegedly circumvented National Australia Bank's (**NAB**) lending controls and allegedly defrauded NAB out of around $150 million[30]. While there has been no public suggestion that the same network was directly involved in the CBA matter, the NAB case heightened industry and regulatory focus on third-party origination risks and the potential for coordinated, documentbased fraud across the home lending market.

Emerging fraud techniques and AI-enabled document manipulation

The suspected misconduct centres on the use of forged or manipulated documents, including income statements and other financial records submitted in support of home loan applications.[31] Some of the materials under review are believed to have been created or altered using artificial intelligence, adding a further layer of complexity to detection efforts[32]. AI-enabled document manipulation represents a shift away from traditional forgery techniques.

This evolution challenges legacy control assumptions that document fraud will exhibit obvious errors or inconsistencies. Where approval processes rely on visual inspection or static rules, AIgenerated or AIenhanced documents may be difficult to distinguish from genuine materials. This can compress the time between control failure and material exposure, particularly where similar documentation is reused across multiple applications.

Governance, assurance, and regulatory scrutiny

If confirmed, the scale of the suspected fraud would make it the largest fraud incident involving an Australian bank. Beyond the immediate financial implications, the matter raises broader questions about the adequacy of governance frameworks supporting third-party origination. These include the effectiveness of broker monitoring, the frequency and depth of assurance testing, and the speed at which emerging risk patterns are escalated and acted upon.

CBA has referred the matter to NSW Police, with the State Crime Command's Financial Crimes Squad engaging with the bank to determine the scope of affected loans. Regulators, including ASIC, have also been notified.[33] In that context, scrutiny is likely to extend beyond individual transactions to systemic issues, including how institutions calibrate controls in higher-risk channels and how quickly those controls adapt as fraud techniques evolve.

Looking ahead

CBA has characterised the issue as an industrywide challenge, noting sustained increases in attempted fraud as criminals adapt their methods using new technologies. That framing reflects broader structural pressures facing the home lending market, including complex intermediary networks, increasing automation, and commercial incentives to streamline approval processes.

Looking forward, supervisory expectations are likely to place greater emphasis on proactive detection, continuous control testing, and demonstrable oversight of broker and referral programs. Rather than focusing solely on postincident remediation, institutions may be expected to show that their lending and verification frameworks are capable of responding dynamically to sophisticated, technologydriven fraud risks, particularly in channels where reliance on externally sourced documentation is greatest.

28. CBA calls police to investigate $1b in suspected home loan fraud
29. Ibid.
30. Ibid.
31. CBA calls in police, $1 billion in fraudulent loans as banks battle AI forgeries | news.com.au — Australia's leading news site for latest headlines
32. CBA self-reports to police over AI $1bn loan fraud - Cyber Daily
33. CBA calls police to investigate $1b in suspected home loan fraud


Privacy / Data

Bunnings v OAIC decision on FRT | Biometric Data and the Privacy Act

The Administrative Review Tribunal (**ART**) decision in *Bunnings Group Limited and Privacy Commissioner* [2026] ARTA 130 offers important guidance on the application of Australian privacy law to facial recognition technology and other highrisk or privacy-intrusive technologies.

Although the Tribunal accepted that Bunnings could rely on a permitted exception under the *Privacy Act 1988* (Cth) to collect biometric data for crime prevention purposes, it nonetheless upheld findings that Bunnings' privacy governance and notification practices fell short of the Australian Privacy Principles (**APPs**).

The decision makes clear that reliance on a collection exception does not discharge broader compliance obligations and serves as a signal that regulators will closely scrutinise the governance, assessment and communication frameworks underpinning the deployment of privacyintrusive technologies.

Background

The proceedings arose from an OAIC investigation into Bunnings' use of facial recognition technology in several retail stores. Following complaints and ownmotion inquiries, the Privacy Commissioner found that Bunnings had interfered with individuals' privacy, including through inadequate governance and notification practices. Bunnings appealed the determination, and the matter was considered by the Administrative Review Tribunal, which delivered its decision on 4 February 2026.

Tribunal findings

Beyond the question of whether a permitted collection exception applied, the Tribunal affirmed the Privacy Commissioner's findings that Bunnings did not comply with its obligations under APP 1 and APP 5. Although the underlying collection was accepted for a limited purpose, the Tribunal found that Bunnings' privacy governance and notification practices were deficient, including the absence of a formal, documented privacy risk assessment, adequate internal policies and procedures, and appropriate customer notice. The Tribunal also confirmed that biometric information collected in real time or retained only briefly may nevertheless constitute "collection" for the purposes of the Privacy Act.

Observations on the implications of the decision

Necessity and proportionality

The Tribunal's reasoning suggests that questions of necessity and proportionality will be assessed in a practical and contextspecific manner. In this case, the seriousness of the problem being addressed and the absence of equally effective alternatives were relevant considerations. Organisations may therefore need to be able to articulate not only the objective of a technology, but also why its use is appropriate when weighed against the associated privacy impacts.

Governance and notification

The decision also illustrates that reliance on a collection exception does not remove the need for robust privacy governance and clear notification practices. Deficiencies in these areas were central to the findings of noncompliance, notwithstanding that the underlying collection was accepted as permissible. This underscores the importance of governance, documentation and transparency as ongoing compliance considerations, rather than matters addressed solely at the point of deployment.

Treatment of transient data

The Tribunal's confirmation that shortlived or automated data capture can amount to collection under the Privacy Act may have broader relevance for technologies that process personal information in real time or without longterm storage. Organisations using such systems may need to reconsider assumptions about whether their data handling practices fall within the scope of the Act.

Regulatory context

In responding to the decision, the OAIC emphasised that the outcome was consistent with its existing approach to biometric and emerging technologies. From a corporate perspective, this indicates that reliance on limited exceptions to consent requirements will continue to be assessed against factors such as suitability, effectiveness, proportionality, the availability of less privacyintrusive alternatives, and how those assessments are undertaken and documented.

Practical considerations for organisations

In light of the decision, organisations that are deploying, or considering the deployment of, highrisk or privacyintrusive technologies should review their existing governance frameworks to ensure that assessments of necessity, proportionality and risk are clearly articulated, appropriately documented and remain fit for purpose over time. Ongoing review of privacy impact assessments, notification practices and internal controls can assist organisations in demonstrating compliance and reducing regulatory and reputational exposure.

Lycamobile Enforcement Outcome - An Insight into Regulatory Expectations

In February 2026, Lycamobile Pty Ltd paid a $376,200 penalty after an Australian Communications and Media Authority (**ACMA**) investigation found that it breached the *Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020*. ACMA found that Lycamobile failed to consistently apply required identityverification checks for mobile number transfers, resulting in unauthorised transfers and consumer losses of at least $175,000. In issuing the penalty ACMA rejected Lycamobile's submission that the flaws were "unidentified", stating the company "should have had robust systems in place" to ensure its compliance processes could not be compromised.[34]

In addition to financial penalty, ACMA accepted an 18month courtenforceable undertaking from Lycamobile.[35] The undertaking requires Lycamobile to remedy past non-compliance and implement an independent comprehensive review, remediation and assurance program, including:

- **Independent technical assurance:** Appointment of an ACMA-approved independent consultant to conduct security and penetration testing of porting-related systems during the undertaking period.
- **Root-cause analysis:** Preparation of a report identifying the causes of security or compliance failures, assessing control effectiveness, and recommending improvements across systems, processes, governance and training.
- **Board accountability:** Provision of the consultant's report to ACMA and the Board, together with a board-approved implementation plan addressing each recommendation and associated timeframes.
- **Ongoing assurance:** Regular internal audits of port-in activity, with outcomes reported to the Board and periodically provided to ACMA, including remediation of any identified non-compliance.
- **Training and records:** Mandatory training for relevant personnel and maintenance of records to support ongoing regulatory oversight.

A Recurring Pattern of Regulatory NonCompliance

Lycamobile's breach forms part of a broader pattern of regulatory noncompliance within the telecommunications sector. ACMA noted that this was the fifth instance in 2026 in which it had identified breaches of these requirements and has issued a notice to all telecommunications providers warning that identityverification systems "must not have vulnerabilities that scammers can target."[36]

Recent enforcement activity illustrates this trend:

- In November 2025 Optus was fined $826,320 after an ACMA investigation found breaches of antiscam and identityverification obligations.[37] Scammers exploited a vulnerability in a third-party identityverification system, enabling them to bypass verification steps, take control of customers' mobile services and access bank accounts, resulting in reported losses of $39,000.
- In July 2024, Telstra was fined $1.5 million after ACMA found it had failed to apply mandatory customer authentication checks in over 168,000 highrisk transactions, including SIMswap requests.[38]
- In January 2024, Medion Australia (operator of ALDI mobile) was fined approximately $260,000 after identity verification failures allowed scammers to take control of customer's phone numbers, leading to losses of more than $160,000.[39]

34. *Australian Communications and Media Authority, Investigation Report (Investigation Report, 04 February 2026) < https://www.acma.gov.au/sites/default/files/2026-02/final_findings_investigation_report_-_lycamobile_pty_ltd_-_11_september_2025_redacted.pdf >.*
35. *Lycamobile Pty Ltd, Enforceable Undertaking Given to the Australian Communications and Media Authority By Lycamobile Pty Ltd Acn 139 717 212 Under Section 572b Of The Telecommunications Act 1997 Cth (Redacted Enforceable Undertaking, 23 December 2025) <https://www.acma.gov.au/sites/default/files/2026-02/enforceable_undertaking_-_lycamobile_pty_ltd_-_23_december_2025_redacted.pdf>.*
36. *Australian Communications and Media Authority, Lycamobile pays $376K in scam rule crackdown (Web Page, 04 February 2026) < https://www.acma.gov.au/articles/2026-02/lycamobile-pays-376k-scam-rule-crackdown >.*
37. *Australian Communications and Media Authority, Optus penalised $826K for breaching anti-scam rules (Web Page, 19 November 2025) < https://www.acma.gov.au/articles/2025-11/optus-penalised-826k-breaching-anti-scam-rules>.*
38. *Australian Communications and Media Authority, Telstra penalised $1.5m for scam rule breaches (Web Page, 17 July 2024) < https://www.acma.gov.au/articles/2024-07/telstra-penalised-15m-scam-rule-breaches>.*
39. *Australian Communications and Media Authority, Medion pays $259,000 penalty for breaches of anti-scam rules (Web Page, 17 January 2024) < https://www.acma.gov.au/articles/2024-01/medion-pays-259000-penalty-breaches-anti-scam-rules>.*

Lycamobile itself has previously been the subject of ACMA enforcement, including penalties in 2021[40] and 2022[41] for failures relating to customer identification obligations and compliance with enforceable undertakings.

What Do These Undertaking Signal About Regulatory Expectations?

Taken together, the enforcement measures reflect heightened regulatory scrutiny of organisations' governance and assurance frameworks, with a focus on preventing the foreseeable misuse of highrisk operational processes.

In particular, the Lycamobile outcomes point to regulatory expectations including:

Clear ownership of high-risk processes, with accountability resting at a level capable of exercising effective oversight, rather than being confined to frontline operational teams.

System-enforced compliance controls that prevent non-compliant outcomes by default, rather than relying on manual checks, discretion or assumptions about customer legitimacy.

Proactive and ongoing assurance, including regular testing, audits and independent review, to identify and address weaknesses before they result in consumer harm.

Board-level visibility and accountability, ensuring that compliance risks associated with access-enabling processes are escalated, reported and addressed as governance issues, rather than treated as isolated operational failures.

Remediation as a continuous process, focused on structural improvement and prevention of recurrence, rather than reactive fixes following regulatory intervention.

The emphasis on independent review, board oversight, recurring audits and formal reporting reflects an expectation that controls are not merely documented, but actively governed, tested and effective over time.

Conclusion

ACMA's enforcement action against Lycamobile demonstrates that regulatory scrutiny now extends beyond identifying what went wrong to examining how risk was identified, owned and assured before consumer harm occurred. Where failures are foreseeable and preventable, the absence of robust governance, accountability and assurance frameworks is treated as a regulatory failure in its own right, particularly where those weaknesses expose consumers to identity compromise and financial loss.

40. Australian Communications and Media Authority, *Investigation and infringement notice Lycamobile – May 2021* (Web Page, May 2021) < https://www.acma.gov.au/publications/2021-05/report/investigation-and-infringement-notice-lycamobile-may-2021>.
41. Australian Communications and Media Authority, *Investigation report and formal warning: Lycamobile December 2022* (Web Page, December 2022) < https://www.acma.gov.au/publications/2022-12/report/investigation-report-and-formal-warning-lycamobile-december-2022>

ACMA Penalises Lululemon for Unsubscribe Failures Under Spam Laws

The Australian Communications and Media Authority (**ACMA**) has imposed a $702,900 penalty on Lululemon Athletica Australia Pty Ltd for breaches of the *Spam Act 2003* (Cth), after the company sent over 370,000 emails without a functional unsubscribe mechanism.[42] ACMA found that Lululemon misclassified certain emails as service messages, despite them containing promotional content and links, bringing them within the definition of commercial electronic messages. The regulator reiterated that any message with marketing content must include a legally compliant unsubscribe facility, regardless of any secondary transactional purpose. In addition to the penalty, Lululemon entered into a court-enforceable undertaking requiring improvements to its spam compliance processes.

42. Australian Communications and Media Authority, 'Lululemon Penalised $702K for Spam Breaches' (Media Release, 11 March 2026) <https://www.acma.gov.au/articles/2026-03/lululemon-penalised-702k-spam-breaches>

Australia's Social Media Minimum Age Law: Privacy and Cybersecurity Implications for Digital Platforms

On 17 March 2026, the Office of the Australian Information Commissioner (**OAIC**) published guidance on age assurance technologies aimed at ensuring Australians' privacy is protected when age checks are used to control access to online services and content. Age checks are becoming more widespread following the start of the Social Media Minimum Age (**SMMA**) scheme in Australia and the introduction of new age assurance obligations on 9 March 2026 under eSafety-registered Age-Restricted Material Codes.[43]

Australia's Social Media Minimum Age Law: Privacy and Cybersecurity Implications for Digital Platforms

Australia's *Online Safety Amendment (Social Media Minimum Age) Act 2024* introduces a prohibition on children under the age of 16 holding social media accounts and requires platforms to take reasonable steps to verify a user's age. Penalties for noncompliance can be significant, reaching up to AUD $50 million. While the reform is framed as a child safety measure, its farreaching consequences arise from the technical and organisational choices platforms make when implementing age verification.[44]

The regime marks a clear shift away from traditional selfdeclared age gates toward more active forms of age assurance. Against this backdrop, the OAIC's published guidance in March 2026 to address accessibility and privacy concerns. The guidance suggests that vendors should treat verification as a privacy-by-design exercise: implement only what is necessary and proportionate to the risk, avoid using age checks as a "blank cheque" to collect personal or sensitive information (including biometrics), and adopt data-minimising approaches supported by strong security and due diligence across any third-party ecosystem. Where sensitive information is used, entities should ensure informed consent, tight governance and clear privacy notices, with accessible complaints pathways.

Why age verification changes the data risk profile

While the SMMA Act does not mandate the use of governmentissued identification, it permits a range of methods, including third-party verification services, biometric tools, and automated age estimation technologies. This flexibility is designed to avoid the routine collection of formal identity documents, but it does not eliminate data protection risk. Although these tools may not establish identity in a legal sense, they often rely on information that is sufficiently similar in nature to give rise to comparable security and governance challenges. Age verification systems commonly depend on data that is persistent, difficult for users to change, or capable of being correlated with other information over time. Images, biometric templates, device signals, behavioural patterns, and verification tokens can all function as stable identifiers when aggregated or reused.

Compared with a simple selfdeclared age value, this type of data is inherently harder to manage. It cannot be easily rotated or invalidated if compromised, and its sensitivity can increase significantly when combined with other datasets held by large platforms. At scale, these characteristics mean that age verification systems may represent a materially different risk profile from earlier, lowfriction age gate models, even if each individual data element appears limited in isolation.

Cybersecurity implications of identityadjacent data

From a cybersecurity perspective, the concern is not that age verification data is always highly sensitive in isolation, but that it can retain leverage over time. Data that can be reused across contexts, linked to other accounts, or exploited for impersonation and fraud tends to remain valuable long after initial collection. Where platforms process this information at scale, verification systems may become concentrated repositories of highutility data that warrant increased defensive attention.

This does not mean that breaches or misuse are inevitable. It does mean, however, that the consequences of a failure may be more severe than under selfattestation models. The possibility of linkage, replay, or repurposing materially changes the impact assessment where verification

43. Office of the Australian Information Commissioner, *Privacy Guidance on Age Assurance Technologies* (Guidance, 17 March 2026) <https://www.oaic.gov.au/__data/assets/pdf_file/0017/262043/OAIC-privacy-guidance-on-age-assurance-technologies.pdf>.

44. *Hafiz Ahmed, 'The Cybersecurity Implications of Australia's Landmark Social Media Ban' (Web Page, ISACA, 20 March 2026) <https://www.isaca.org/resources/news-and-trends/industry-news/2026/the-cybersecurity-implications-of-australias-landmark-social-media-ban>*

data is exposed, particularly where protective controls have not kept pace with the sensitivity of the system.

Governance complexity and internal data flows

Age verification also creates governance challenges because it sits across multiple organisational functions. Verification processes necessarily interact with onboarding, content access controls, customer support, and in some cases trust and safety enforcement. If these interactions are not carefully constrained, verification data can gradually flow into analytics, profiling, or other operational systems through shared infrastructure or permissive access controls.

Over time, this can dilute original purpose limitations and make it more difficult to demonstrate compliance with privacy principles. Even where policies are clear, architectural decisions may undermine them in practice if verification outputs are not cleanly separated from broader user datasets.

Designing verification systems to limit exposure

One way to manage these risks is to treat age verification as a narrow, purposelimited function and reflect that constraint in both system design and governance structures. Approaches that emphasise minimal disclosure reduce the likelihood that verification data evolves into a secondary identity layer. Techniques such as local or ondevice processing, binary or tokenised outcomes, and strict segregation from social, advertising, and analytics systems can materially reduce exposure if something goes wrong.

Retention discipline is particularly important where biometric or imagebased inputs are used, as the risk profile of stored data changes quickly once verification is complete. The longer such information is retained, the harder it becomes to justify its ongoing presence.

Third-party verification and layered assurance models

Where platforms rely on third-party verification providers, risk does not disappear but shifts. External services introduce dependency, concentration, and contractual risks, especially where the same provider supports multiple large platforms. Without clear limits on secondary use, strong security assurances, and effective oversight, verification data may be retained or repurposed beyond the platform's original intent.

The Act also allows for layered or riskbased verification approaches. These models can reduce unnecessary data collection, but they place heavy reliance on the design and governance of escalation logic. Poor calibration may result in routine escalation to more intrusive processes, weakening the intended privacy benefits.

Looking ahead

The SMMA Act and the OAIC's age assurance guidance illustrate how safetyfocused regulation can reshape data and cybersecurity risk in ways that are not immediately apparent from the legal text alone. The central issue is not simply whether reasonable steps were taken, but whether those steps were designed in a way that avoids creating new concentrations of sensitive information and new avenues of exposure. Decisions made during system and governance design will play a decisive role in shaping both regulatory outcomes and cyber risk over time.

Know your privacy obligations under the Anti-Money Laundering / Counter-Terrorism Financing (AML/CTF) Act: Updated OAIC guidance

On 27 February 2026, the Office of the Australian Information Commissioner (OAIC) released updated guidance on how businesses must handle personal information under Australia's AntiMoney Laundering and CounterTerrorism Financing regime. The guidance accompanies significant AML/CTF reforms that both update obligations for existing reporting entities and extend the regime to newly regulated industries.[45]

A key message from the OAIC is that organisations can meet their AML/CTF obligations without collecting or retaining more personal information than necessary. Privacy compliance is not an obstacle to AML/CTF compliance, but an integral part of it.

Who is affected

All AML/CTF reporting entities are subject to obligations under the *Privacy Act 1988* (Cth) (**Privacy Act**) and the Australian Privacy Principles when handling personal information for AML/CTF purposes. This includes newly regulated "Tranche 2" sectors such as legal, real estate and accounting services. It also includes small businesses with annual turnover of less than $3 million (AUD) that were previously exempt from the Privacy Act, but only in relation to their handling of personal information for AML/CTF compliance purposes.

Note that privacy laws do not prevent the collection of required information (including sensitive information) to meet AML/CTF rules; however, additional safeguards have been put in place to guide entities on how personal information is to be collected, used, stored, and disposed of.

Data collection limited to what is "reasonably necessary"

The updated OAIC guidance reinforces that reporting entities are required to limit the collection of personal data to what is "reasonably necessary" to fulfil AML/CTF Know-Your-Customer legal obligations. The OAIC cautions against excessive or speculative data collection. In particular, collecting more information than required does not improve AML/CTF compliance outcomes, but instead increases privacy and cybersecurity risks.

No blanket requirement to retain full ID document copies

One of the most practical clarifications in the guidance is that reporting entities are not required to retain full copies of identity documents, such as passports or driver licences, solely for AML/CTF record-keeping. Instead, entities are required to retain only the information required by the AML/CTF Rules, such as the individual's name, address and date of birth, the type and number of the identification document, the expiry date, and the outcome of the verification process.

This change applies from 31 March 2026 for existing Tranche 1 reporting entities and from 1 July 2026 for newly regulated Tranche 2 entities. Copies of identification documents collected before these dates may be retained for the mandatory sevenyear AML/CTF retention period, after which they must be securely destroyed.

Privacy notices and security remain essential

Reporting entities are expected to maintain clear and up-to-date privacy policies and customer notices explaining how personal information is collected and used for AML/CTF purposes. The OAIC recognises that these notices may need to be modified or withheld in limited circumstances to avoid breaching AML/CTF tipping-off prohibitions.

Entities must also take reasonable steps to protect AML/CTF-related personal information. This includes implementing appropriate cybersecurity controls, restricting access to sensitive information, and maintaining an incident response plan to manage potential data breaches.

What this means in practice

For Tranche 1 entities, the updated guidance reinforces the importance of embedding privacy compliance within existing AML/CTF programs. For Tranche 2 entities, it provides a roadmap for building privacy, data governance, and cybersecurity controls into new AML/CTF compliance frameworks. By integrating privacy principles into AML/CTF processes, businesses can meet their regulatory obligations while reducing both cyber risk and reputational exposure.

45. Office of the Australian Information Commissioner, *Know Your Privacy Obligations under the Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Act: Updated OAIC Guidance* (Media Release, 27 February 2026) .

Virtual TryOn Tools and Biometric Data: Privacy and Security Risks

Virtual Try On (**VTO**) tools are increasingly used by retailers and consumer-facing organisations to enhance customer experience, allowing users to preview eyewear, cosmetics or clothing via device camera or uploaded image. Despite their seemingly low-risk, consumer-facing nature, these tools can involve the collection and processing of biometric data, carrying heightened privacy, security and regulatory risk.

As biometric data becomes embedded in everyday digital services, organisations adopting VTO technology must weigh customer experience benefits against the governance, compliance and security implications of deploying tools that analyse human physical characteristics.

How VTO Tools Operate

VTO tools typically require a user to upload an image or activate a live camera feed. The software detects facial landmarks such as eye position, nose or jawline, or estimates body shape and measurements, to accurately position digital products. Examples include estimating pupillary distance for eyewear or generating a simplified three-dimensional body model to assess garment fit.

Although the output may resemble a simple visual filter, the underlying processing may involve the creation of biometric identifiers or measurements unique to the individual. This raises important questions about whether the data processed constitutes biometric information under applicable privacy laws.

Data Collection, Transmission and Retention Risks

The lowest-risk implementation of VTO technology performs all processing locally on the user's device, retaining or transmitting no images or derived biometric data beyond the session. Some vendors represent that their tools operate in this way.

However, independent research and technical testing have identified cases where VTO implementations transmitted images or encoded biometric representations to vendor-controlled or third-party servers, sometimes inconsistently with user-facing disclosures. Reviews of retail VTO websites have found that many transmitted images off-device, and a proportion retained them for extended periods.[46]

Where data flows are opaque or inaccurately described, organisations risk compliance liability, regulatory investigation and reputational damage, particularly if practices come to light following a cyber incident or audit.

Retained images or biometric templates become highvalue data assets that can be used for re-identification, tracking or profiling, particularly when linked with account details, contact information or transaction history. Unlike passwords or account credentials, biometric attributes cannot be changed following compromise.[47]

Secondary Use and Purpose Expansion

Beyond breach scenarios, organisations should consider secondary use risk: biometric data collected for VTO functionality may later be repurposed for analytics, targeted advertising or machine learning model training.

Unless these uses are clearly disclosed and appropriate consent obtained, they may exceed reasonable user expectations and give rise to legal and regulatory risk. Purpose expansion also increases the sensitivity, scale and longevity of the data, amplifying potential impact if controls fail.

Practical Safeguards and Governance Considerations

Organisations deploying or integrating VTO tools should treat them as a form of high-risk data processing and apply proportionate safeguards, including:

- Clear, accurate disclosure of what data is collected, whether biometric data is generated, where processing occurs, who receives it and how long it is retained.
- Explicit consent where biometric data is stored, transmitted off-device or used beyond the immediate try-on session.

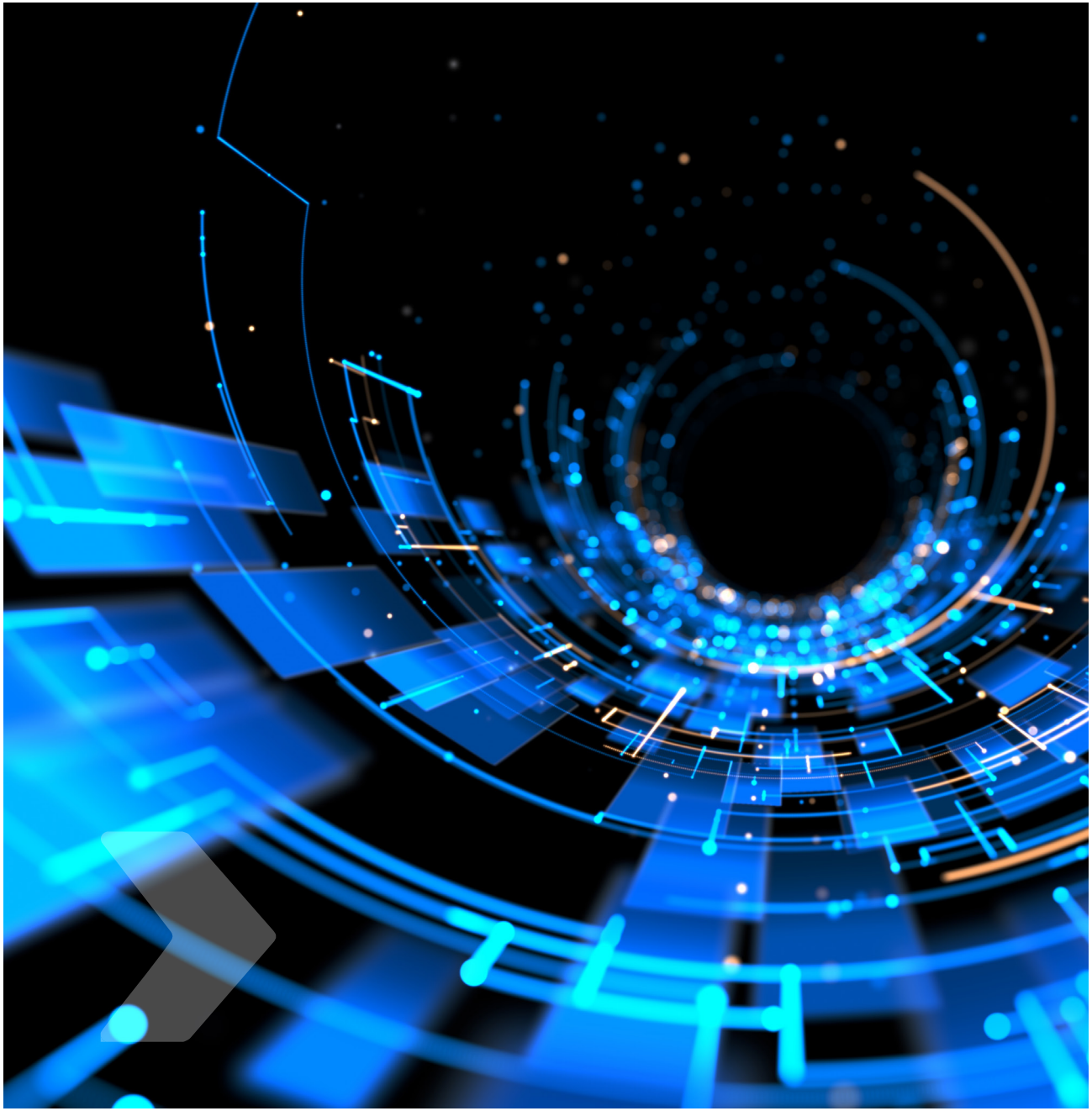
46. Abdelrahman Ragab, Mohammad Mannan and Amr Youssef, 'Try On, Spied On?: Privacy Analysis of Virtual Try-On Websites and Android Apps' in Sokratis Katsikas et al (eds), ESORICS 2023 Workshops (Springer, 2024) 232, 232–3 <https://doi.org/10.1007/978-3-031-54204-6_13>.

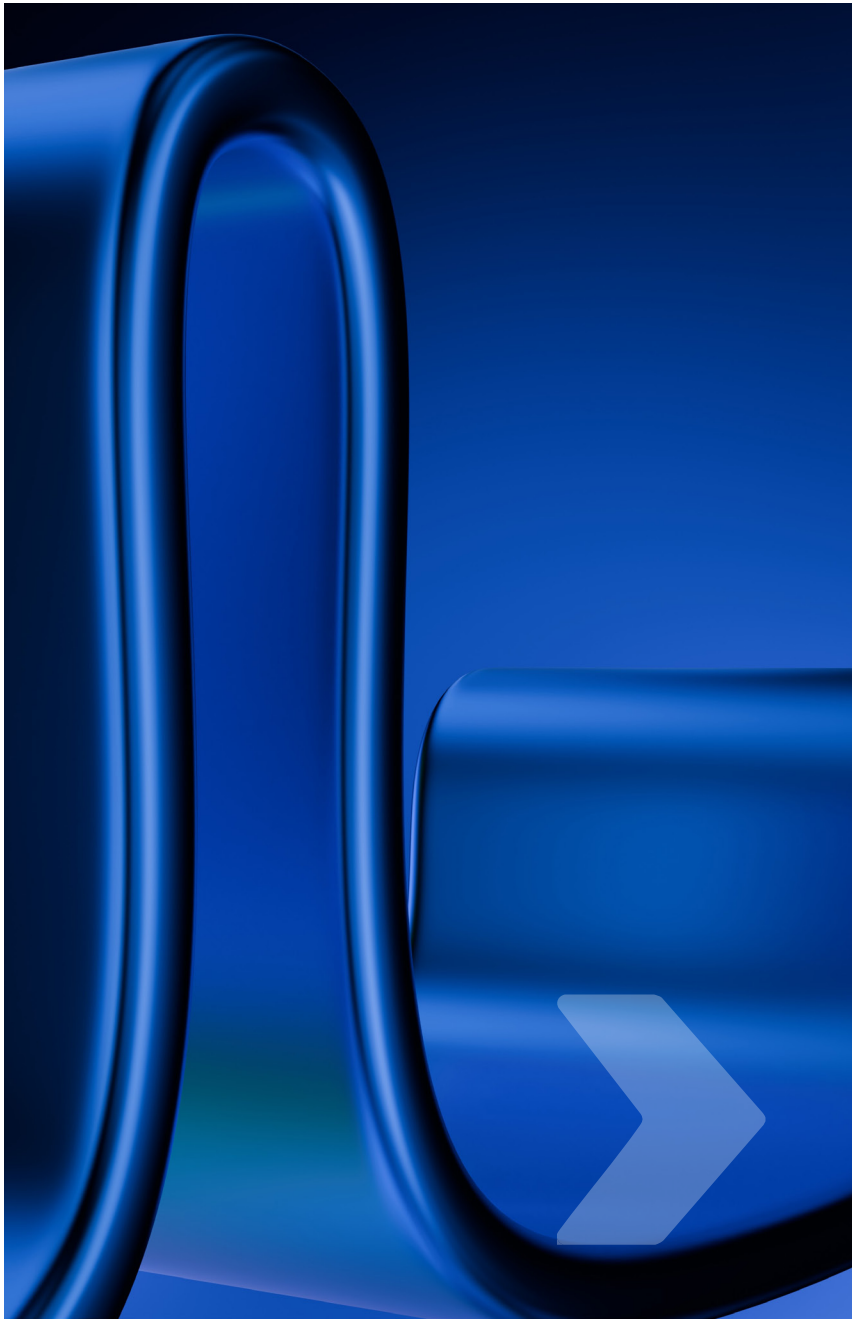
47. Purdue Global Law School, 'Virtual "Try-On" Technologies Face Mounting Legal Challenges' (News and Commentary, 7 August 2023) available at: https://www.purduegloballawschool.edu/blog/news/virtual-try-on-technologies (accessed 9 April 2026); Song-yi Youn, Joohye Hwang, Li Zhao and Jong-Bum Kim, 'Privacy paradox in 3D body scanning technology: the effect of 3D virtual try-on experience in the relationship between privacy concerns and mobile app adoption intention' (2023) Humanities and Social Sciences Communications 10:208 https://doi.org/10.1057/s41599-023-01632-y

- Preference for on-device or ephemeral processing, with no retention of raw images and data minimisation to what is strictly necessary.
- Robust third-party vendor due diligence, with contractual controls governing data use, retention, security obligations, subprocessors and audit rights.
- Recognition of the elevated impact of biometric data compromise, and implementation of commensurate technical and organisational security controls.

Conclusion

VTO tools illustrate how seemingly low-impact consumer features can quickly evolve into biometric data processing at scale. As these technologies become more prevalent, organisations should assess them not simply as marketing enhancements, but as systems that may introduce material privacy, security and regulatory risk. This is particularly important as regulators increasingly focus on privacypreserving design and data minimisation. Applied thoughtfully, these governance principles can allow VTO tools to deliver convenience and innovation without expanding biometric surveillance or creating avoidable liability.





High Court Confirms NCAT's Power to Award Privacy Compensation

The High Court has confirmed that New South Wales Civil and Administrative Tribunal (**NCAT**) has power under s 55(2)(a) of the *Privacy and Personal Information Protection Act 1998 (NSW)* to award compensation for privacy breaches. In doing so, the Court held that the making of a compensation order under that provision is an exercise of administrative, not judicial, power for the purposes of Chapter III of the Constitution. The Court distinguished *Brandy v HREOC*, emphasising that the PPIP Act does not create civil causes of action or involve the determination of preexisting legal rights, but instead forms part of an administrative enforcement regime governing public sector conduct. The decision overturns the New South Wales Court of Appeal and provides clarity that NCAT has jurisdiction to determine privacy compensation claims, including where the claimant is a resident of another State.[48]

48. New South Wales v Wojciechowska (2025) 98 ALJR 456; [2025] HCA 27.

Privacy Beyond Compliance: A Focus on Trust and Resolution

Privacy Awareness Week 2026 comes at a moment of recalibration for Australia's privacy framework. The theme *"Trust is built here: In every privacy complaint. In every resolution"* is not simply a message about dispute handling. As the Privacy Commissioner made clear in her remarks at the Privacy Awareness launch earlier this week, it is a description of how privacy effectiveness is now being judged.

Australia is moving beyond a conception of privacy grounded primarily in formal compliance and procedural sufficiency. The emerging question is sharper and more human: does this system work for people when it matters and does it do so in a way that is fair and reasonable?

That shift has profound implications for how organisations design systems, deploy technology, respond to concerns, and ultimately earn or lose trust.

1. From Compliance to Consequence

For much of the past decade, privacy practice has focused on whether obligations were met: whether policies existed, notices were published, consent boxes were ticked. The Commissioner's remarks signal a move away from that inputbased model.

The focus is increasingly on outcomes - what individuals actually experience. Do they understand what is happening to their personal information? Do they feel they have genuine choice and control? And when something goes wrong, do they receive a meaningful response?

This outcomefocused lens aligns closely with the direction of Privacy Act reform and the Commissioner's repeated emphasis on *fairness and reasonableness* as the organising principle of modern privacy regulation. From where the Commissioner stands, agency, choice and control are not optional extras - they are inherent features of what it means for information handling to be fair and reasonable in practice.

The emphasis on complaints is telling. Complaints are no longer framed as a peripheral regulatory function or an unfortunate workload pressure. They are treated as the point at which the system reveals its true character. Every unresolved complaint, every opaque response, every delayed or defensive resolution is not just a process failure- it is a trust failure.

Seen this way, *"Trust is built here"* is not aspirational. It is diagnostic.

2. Transparency That People Can Actually See

A central plank of the Commissioner's remarks was the insistence that transparency must be specific, perceptible and intelligible, not merely present in form.

As data practices become more complex, more automated and more ambient, traditional transparency mechanisms increasingly fall short. Disclosures that exist only on paper or online, but are practically invisible to the people affected, do little to support understanding or agency.

The Commissioner's position reflects a broader regulatory evolution: transparency is no longer assessed by whether information could theoretically be found, but by whether a person encountering a technology or practice can realistically grasp what is occurring and why it matters.

This reframing is particularly significant as artificial intelligence, biometric technologies and background data collection become embedded in everyday environments. In a world where technology often obscures choice and control far more than it enables them, meaningful transparency becomes a critical safeguard and a core component of fairness and reasonableness.

The expectation is no longer that individuals will adapt to opaque systems; it is that systems must be designed to remain visible and comprehensible to individuals.

3. Understanding the Signals in Privacy Complaints

The Commissioner's reliance on data - rising complaint volumes, low satisfaction rates, and widespread disengagement from complaint mechanisms - underscores an important point: trust erosion is measurable.

These figures are not treated as incidental or cyclical. They are treated as evidence that too many organisations are failing at first instance - failing to listen, explain, remediate and resolve.

When people believe complaining will be pointless or burdensome, trust collapses quietly. When they do complain and feel unheard or dismissed, trust collapses loudly. In both cases, the regulator becomes the forum of last resort.

This reinforces the central message of this year's theme: privacy lives or dies in the resolution moment. Trust is not built through statements of principle; it is built through fair, prompt and human responses to individual concerns.

4. Agency as the Core of Privacy

The Commissioner repeatedly returned to the idea that privacy is fundamentally about agency - about enabling people to exercise meaningful control over their personal information.

This lens is increasingly shaping regulatory attention, particularly in areas where agency is most at risk:

- where personal information is reused to train AI models;
- where AI tools are introduced into sensitive settings like healthcare;
- where digital platforms demand everexpanding volumes of data; and
- where tracking technologies operate outside an individual's immediate awareness.

What links these practices is not simply innovation, but opacity. When personal data practices become passive or invisible, choice and consent are easily hollowed out.

The Commissioner's response is clear: privacy regulation must actively rebalance power and information asymmetries. That rebalancing is central to fairness and reasonableness - particularly in an AIdriven environment where decisionmaking is increasingly abstracted away from the individual.

5. Children as the Signal of Where We Are Going

Perhaps the most forwardlooking aspect of the Commissioner's remarks was the emphasis on children's privacy.

The proposed Children's Online Privacy Code is not framed as a narrow protective measure. It is framed as a model for a different way of building digital systems - one that starts with minimisation, intelligibility and genuine consent, rather than retrofitting these principles after the fact.

What is striking is the recognition of children as emerging agents. The emphasis on ageappropriate explanation, participatory consent and deletion rights reflects a belief that trust, fairness and digital literacy must be built early and visibly.

The deeper implication is this: children's privacy standards may become the proving ground for adult expectations. If systems designed for children demonstrate that strong privacy protections are compatible with usability and commercial viability, they challenge the longheld assumption that privacy must be traded off against innovation or growth.

6. Trust as National Direction

Taken together, the Commissioner's remarks describe a country at a turning point.

Australia's privacy framework is moving toward an outcomesdriven model, where laws, standards and reforms are increasingly interpreted through the lens of lived experience. Fairness and reasonableness are emerging not just as legal tests, but as measures of whether privacy law is delivering its social purpose.

Trust is not assumed. It is earned - or lost - repeatedly, through interaction.

This places a new responsibility on organisations. Privacy is no longer something demonstrated primarily to regulators, but something experienced by individuals. Investment, culture and process matter not because they look good on paper, but because they determine how an organisation responds in the moments that define trust.

Where Privacy Awareness Week Really Begins

Privacy Awareness Week is not where the work ends; it is where it should begin.

Trust is built, or broken, in everyday decisions - in how products are designed, how technologies are deployed, how complaints are handled, and how people are treated when they raise concerns.

Each of us, as designers, developers, advisors, decisionmakers and practitioners, plays a role in shaping whether privacy is experienced as protection or frustration. If fairness, reasonableness, and agency are truly to sit at the heart of Australia's privacy system, they must be embedded not just in law and policy, but in practice - one interaction, one complaint, one resolution at a time.

Technology

National Expectations and the Future Shape of AI Infrastructure Investment

What Developers and Investors Need to Know

The Australian Government has released national expectations for data centres and AI infrastructure that will materially influence how largescale digital infrastructure is assessed and prioritised.[49] The framework reflects a more coordinated policy approach to managing rapid growth in AI-driven capacity, with regulatory focus extending beyond technical feasibility to national interest, sustainability, and capability outcomes. Alignment with these expectations is now a practical factor in approval timing, sequencing, and regulatory support.

Expectation 1 - A Sharper National Interest Lens

The expectations establish a national interest lens through which future projects are likely to be assessed. Proponents are expected to demonstrate how developments contribute to economic resilience, data sovereignty, security, and longterm capability building. The emphasis reflects a policy shift towards infrastructure that delivers enduring national and community benefits alongside commercial outcomes.

Expectation 2 - Energy Transition as a Threshold Issue

Energy has emerged as a central factor in project viability. Data centres and AI compute facilities are expected to integrate with Australia's energy transition by underwriting additional renewable generation, contributing to grid infrastructure, and adopting demandmanagement mechanisms that support system stability. Projects that place pressure on existing energy systems are likely to encounter greater regulatory scrutiny.

Expectation 3 - Sustainable and Resilient Water Use

Water use is treated with comparable importance. Developers can expect close examination of cooling technologies, water sourcing, and operational resilience, particularly in waterstressed regions. Early engagement with water utilities, communities, and First Nations stakeholders is increasingly central to managing environmental risk, community confidence, and approval risk.

Expectation 4 – Investment in Australian Skills and Jobs

Workforce outcomes form a core element of the expectations. Data centre operators are expected to create fair, safe, and wellpaid jobs for Australian workers and invest in building a skilled domestic workforce. Collaboration with governments, unions, education providers, and training providers is treated as central to addressing skills gaps and establishing sustainable training pathways that support both construction and ongoing operations.

49. *New South Wales v Wojciechowska* (2025) 98 ALJR 456; [2025] HCA 27

Expectation 5 - Emphasis on Domestic Capability

The expectations place strong weight on domestic capability outcomes. Developers are encouraged to invest in Australian skills and workforce development and to support research and innovation ecosystems. Largescale compute providers are expected to contribute to local innovation, including by facilitating access to compute for Australian startups, researchers, and notforprofits, and by establishing a meaningful technical presence in Australia.

Practical Implications

The expectations are intended to guide regulatory prioritisation across Commonwealth processes and to inform coordination with state and territory decision-making. In a constrained approvals environment, projects that integrate energy, water, community, and capability considerations at an early stage are more likely to progress efficiently through approval pathways.

Taken together, the framework signals a more disciplined operating environment for AI and data centre development. Alignment with national expectations has become a defining feature of effective approval strategy and project planning, and should be treated as a first-order consideration rather than a secondary compliance step.

Against this backdrop, investors and developers of highcapacity data centres should assess proposed sites, design choices, and operating models through the lens of energy and water resilience. Early engagement with power utilities and renewable energy providers may assist in addressing grid impacts and supporting access to additional clean energy supply. Operators and anchor customers should also consider how they will contribute to domestic innovation and capability, including through collaboration with Australian startups, research institutions, and the wider innovation ecosystem.

Further developments

We expect further policy guidance and announcements as the Australian Government continues to refine its approach to data centre and AI infrastructure development, particularly in support of investment that aligns with environmental sustainability and broader social outcomes.

Tackling AI risks: Australia to stick with existing consumer protections into AI and the Australian Consumer Law

At a glance:

- In October 2025, the Australian Government concluded its review into whether Australia's existing consumer law framework adequately addresses the risks and potential harms associated with AI enabled goods and services.
- The Government's final report found that the existing consumer framework is generally well adapted to address AI risks, and a separate AI liability regime is not necessary to protect consumers.
- Australia's incremental approach to AI can be contrasted with the EU's adoption of a comprehensive regulatory framework.

Review of AI and the ACL

In October 2025, the Australian Government released the Final Report of the Review of Artificial Intelligence and the Australian Consumer Law.[50] As part of the Government's broader initiatives to support safe and responsible use of AI, the review examined whether Australia's existing consumer law framework adequately addresses the risks and potential harms associated with AI-enabled goods and services.

The final report found the ACL's existing principles-based, technology-neutral foundation is suitable for regulating AI markets, and that AI-related risks can be managed within the ACL through existing concepts like:

- Defective goods;
- Misleading or deceptive conduct;
- Product safety; and
- Manufacturer's liability.

This approach is intended to preserve the adaptability of the existing framework, with the expectation that more complex issues arising from AI-enabled goods and services will be clarified over time through judicial interpretation and regulatory guidance. This reflects a deliberate preference for flexibility over rigid, technology-focused regulations.

50. Australian Treasury (Cth), *Review of AI and the Australian Consumer Law* (Final Report, October 2025) < https://treasury.gov.au/sites/default/files/2025-10/p2025-702329-fr.pdf>

The final report identifies three areas where legislative clarification would improve certainty and risk allocation for new and emerging technologies such as AI:

1. Expanding the Definition of Goods

The final report recommends expressly including digital products and software-enabled goods within the statutory definition of "goods" under the ACL. At present, uncertainty persists as to whether certain AI-enabled products are properly characterised as "goods" or "services", a distinction that determines which consumer guarantees apply. This ambiguity has created scope for classification disputes, particularly where a product's functionality is delivered primarily through software. Clarifying that digital and AI-enabled products fall within the definition of goods is intended to strengthen the operation of consumer guarantees in relation to those products.

2. Amending the Definition of a Manufacturer

The final report recommends amending the current definition of a 'manufacturer' to expressly refer to manufacturers of digital products or software-enabled goods. This change is intended to address uncertainty around statutory responsibility in complex AI supply chains – where functionality may be designed by one entity, integrated by another, and supplied by a third. Clarifying that developers and integrators of digital and AI-enabled products fall within the definition of "manufacturer" is intended to provide greater certainty around liability, including obligations to indemnify suppliers and respond to safety defects.

3. Updating the 'Time of Supply' Defence

The final report recommends reframing the 'time of supply' defence to incorporate the concept of control. Under the current law, a manufacturer may avoid liability by establishing that a safety defect did not exist at the time the goods were supplied. This defence reflects an assumption that control over a product ends upon sale. AI-enabled and software-driven goods challenge that premise, as functionality and safety profiles may be materially altered through post-supply updates. Under the proposed reform, manufacturers that maintain ongoing control over a product – for example, through software updates that introduce defects – would be unable to rely on the 'time of supply' defence.

How Australia's Approach Differs from the EU

Australia's position can be contrasted with the approach adopted by the EU under the EU Artificial Intelligence Act.[51] While both jurisdictions aim to safeguard consumers and ensure trustworthy AI, they have taken different regulatory paths.

The EU has pursued a comprehensive, AI-specific regulatory framework which became operational in stages from 2025. The regime is explicitly riskbased, classifying AI systems according to the level of risk they pose to safety, fundamental rights and broader societal interests. Under this model, the EU imposes mandatory obligations before AI systems are placed on the market, particularly in highrisk domains such as biometrics, critical infrastructure, employment, education and credit. Key features of the EU's approach include:

- A formal risk classification system (unacceptable, highrisk, limitedrisk, minimalrisk);
- Prohibitions on unacceptable AI practices, such as social scoring and manipulative or exploitative AI;
- Mandatory conformity assessments and technical documentation requirements for highrisk systems; and
- Changes to the Product Liability Directive (Directive (EU) 2024/2853) to cover software, including AI systems, from 9 December 2026.

In contrast, Australia avoided a separate AI regime, and is instead introducing discrete changes into existing frameworks – such as a voluntary AI safety standard [52] and a Commonwealth Government policy for the responsible use of AI [53] – to manage AI risks. The review's recommendation to maintain a technology-neutral, principles-based enforcement model under the existing ACL framework is consistent with that approach.

Key Takeaway

The Australian Government is opting for continuity over disruption in the regulation of AI-enabled goods and services under the consumer law. Its review of the consumer law found that existing statutory protections are capable of addressing emerging risks to consumers of AI-engaged goods, although it has recommended some fairly minor changes to improve clarity in areas where digital products and evolving supply chains strain traditional definitions. Whether that approach works with the novel and rapidly evolving nature of AI remains to be seen.

51. *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence* [2024] OJ L 2024/1689 art 5.
52. Department of Industry, Science and Resources (Cth), *Voluntary AI Safety Standards* (Standard, August 2024) < https://www.industry.gov.au/publications/voluntary-ai-safety-standard>.
53. Australian Commonwealth Government, *Policy for the responsible use of AI in government version 2.0* (Web Page, 15 December 2025) < https://www.digital.gov.au/ai/ai-in-government-policy>

No privilege for the machine: US court says AI documents are not protected

At a glance:

- In February 2026, a US Court ruled that documents generated using 'Claude', a generative AI assistant, were not protected by legal privilege.
- The decision highlights the dangers of using publicly available AI tools for the purposes of obtaining legal research or advice.

Background

In November 2025, Bradley Heppner, the former chairman of US financial services company GWG Holdings Inc (**GWG**), was arrested on charges of securities fraud, wire fraud, false statements to auditors, and falsification of records. GWG filed for bankruptcy in April 2022, resulting in over US$1 billion in losses to retail investors. The defendant is set to face trial in April 2026.

As part of his arrest, the FBI seized documents and electronic devices from the defendant's home, including 31 documents prepared with the help of Anthropic's generative AI assistant, Claude. Those documents included a report outlining a defence strategy if the defendant faced criminal charges as a result of GWG's bankruptcy.

The defendant claimed legal privilege over the AI documents on the basis that he:

- Input advice received from his legal counsel into the AI tool;
- Created the AI documents for the purposes of speaking with his counsel to obtain legal advice; and
- Subsequently shared the contents of the AI documents with his counsel.

The US Government applied for a ruling that the documents were not protected by either attorney-client privilege or the 'work product doctrine', which protects materials prepared in anticipation of litigation.

US District Court's ruling

In *United States v. Heppner* (S.D.N.Y. Feb. 17, 2026), the US District Court for the Southern District of New York held the AI documents lacked at least two, if not all three, elements of the attorney-client privilege as:

- The documents were not communications between a client and his attorney;
- The documents were not confidential, not only because the defendant voluntarily communicated with a third-party AI tool, but also because Claude's privacy policy permitted disclosure of data on its inputs and outputs to third parties (including government agencies). In those circumstances, the defendant could have no reasonable expectation of confidentiality;
- The defendant did not communicate with Claude for the purposes of obtaining legal advice, because Clause cannot provide such advice. Heppner could not retroactively cloak documents with privilege by later transmitting them to counsel.

Even if the information Heppner entered into Claude attracted privilege because it originated with counsel, the Court observed that Heppner had waived that privilege by sharing the information with a third-party AI platform.

The Court also found the AI documents did not attract privilege under the work product doctrine. The Court noted the doctrine protects materials prepared by or at the behest of counsel, and depends upon the existence of a real, not

speculative, concern that the thought processes of counsel would be exposed. Neither factor was found to exist in this case, as the documents were created by Heppner of his own volition and did not reflect counsel's strategy at the time they were created.

Legal privilege in Australia

The question of whether documents generated by a third-party AI tool could attract legal professional privilege has not been tested in Australia.

Australia recognises two types of legal professional privilege:

- advice privilege, which applies to confidential communications and documents brought into existence for the dominant purpose of giving or obtaining legal advice; and
- litigation privilege, which applies to confidential communications and documents brought into existence for the dominant purpose of a client being provided with professional legal services in relation to actual or anticipated legal proceedings involving the client as a party.

In Australia, communications between a client and a third party may be privileged provided the 'dominant purpose' test is satisfied. Relevantly, however, legal professional privilege attaches only to confidential communications. In *US v. Heppner,* the court determined the AI documents were not confidential, including because Claude's privacy policy allowed for disclosure of data to third parties. It is reasonable to expect that courts in Australia may take a similar approach to confidentiality.

Australian courts have warned that AI tools trained on large language models (such as Claude and ChatGPT) are not capable of producing reliable legal research or advice[54], and recognised that uploading information or documents into a public AI tool may constitute a waiver of privilege over that material.[55] The risk of inadvertent disclosure of confidential or privileged material was also recently highlighted in the Federal Court's Practice Note on the Use of Generative AI (GPN-AI).

Takeaway

It is widely now recognised that freely available AI tools (such as Claude and ChatGPT) are not capable of producing reliable legal research or advice. The decision in *United States v. Heppner* highlights a further risk that communications with AI tools will not attract legal privilege and may be discoverable. These issues highlight the importance of using secure, private and specialised AI tools for legal tasks, with appropriately qualified legal advisors reviewing the accuracy of AI outputs.

54. *May v Costaras* [2025] NSWCA 178, [12]; *Helmold v Mariya (No 2)* [2025] FedCFamC1A 163, [6], citing Dame Victoria Sharp, President of the King's Bench Division of the High Court of Justice in *Ayinde v London Borough of Haringey* [2025] EWHV 1383 (Admin), [5]-[9].
55. *Helmold v Mariya (No 2)* [2025] FedCFamC1A 163; *Mertz v Mertz (No 3)* [2025] FedCFamC1A 222.

Much ado about crypto: High Court to consider if bitcoin is property

At a glance:

The High Court of Australia has granted special leave to appeal a decision which found bitcoin is property and capable of being the subject of the torts of conversion and detinue.

The case will be the first time the High Court has considered whether cryptocurrency is property which is capable of possession.

The decision is expected to resolve a difference in judicial opinion at the state level.

Background

In December 2013, Adam Poulton and Jeff Conrad entered into an arrangement whereby Conrad paid Poulton the sum of $10,000 to invest in cryptocurrency. Poulton used the money to acquire bitcoin on behalf of Conrad, however a dispute arose when he retained a portion of the bitcoin as a fee for his services.

Conrad brought claims against Poulton for conversion and detinue, arguing Poulton unlawfully kept and resisted his ownership of the bitcoin despite repeated demands its return.

Actions for conversion and detinue require the plaintiff to show an immediate right to possession at the time of the act of conversion. Because bitcoin is digital, therefore intangible, a question arose as to whether it is property which is capable of possession, and therefore susceptible to actions in conversion and detinue.

Procedural history

At first instance, the Magistrates Court concluded that bitcoin is property and could be the subject of claims in conversion and detinue. The Court found the software restricts access to a person in possession of a private key or PIN, and the right to hold bitcoin is definable, identifiable by third parties, capable of assumption by third parties, and sufficiently stable to satisfy the definition of property in *National Provincial Bank v Ainsworth*[56]. Conrad was awarded $50,000 in damages, with a set off of $1,500 for Poulton's reasonable fees.

Poulton appealed the decision to a single judge of the Supreme Court of Tasmania, however he did not challenge the magistrate's finding that bitcoin is property capable of possession. The appeal was dismissed.

Decision of the Full Court

Poulton once again appealed to the Full Court of the Tasmanian Supreme Court, this time on the basis that bitcoin is intangible property and not amenable to conversion or detinue. The Full Court dismissed Poulton's appeal on both procedural and substantive grounds:

Shanahan CJ and Jago J (Estcourt J dissenting) dismissed the appeal because it relied on arguments which Poulton did not advance in his first appeal; and

the Court unanimously dismissed the appeal on substantive grounds, finding that bitcoin is property capable of possession.

Estcourt J referred with approval to the English case of AA v Persons Unknown and Ors[57], in which Bryan J found bitcoin is a form of property

56. [1965] 1 AC 1175
57. [2019] EWHC 3556

notwithstanding it is neither a chose in possession nor a chose in action. In making that finding, his Honour chose to depart from:

- the decision of the Victorian Supreme Court in *Re Blockchain*[58] that bitcoin is a chose in action, and therefore cannot be the subject of a bailment; and
- the decision of the House of Lords in *OBG Ltd v Allan*[59] that a chose in action could not be the subject of a claim for conversion,
- on the basis that this reasoning does not reflect the reality of the digital age. Estcourt and Jago JJ concluded that:

"... there is a powerful case for reconsidering the dichotomy between choses in possession and choses in action, and for recognising a third category of intangible property. Such a category in my view, would comprise property that is capable of assumption by third parties, that is rivalrous, that is capable of exclusive control, and that is susceptible of possession. As such it should be amenable to at least, the torts involved in the present case, namely, conversion and detinue."

In separate reasons, Shanahan CJ found the central premise underpinning the common law concept of possession remains control with an intent to exercise dominion. His Honour implicitly accepted that detinue and conversion are available in respect of bitcoin.

Appeal to the High Court

Poulton has been granted leave to appeal the decision to the High Court of Australia. In his appeal submissions, Poulton argues amongst other things that:

- bitcoin is simply lines in a database and does not have the characteristics of property identified in *Ainsworth*;
- bitcoin is intangible, therefore cannot be the subject of conversion (per *OBG Ltd v Allan*);
- to the extent the Full Court found there is a third category of property apart from a chose in possession or chose in action, then it went too far given the state of the authorities.

Takeaways

The High Court's decision is expected to bring clarity to the nature of proprietary rights and availability of civil remedies for crypto assets, resolving the current divergence of judicial opinion in Australia. Given the line of overseas cases on this topic, the High Court's decision will no doubt be watched with interest locally and internationally.

58. [2024] VSC 690
59. [2008] AC 1

Reinteractive Series: Procedural and Evidentiary Rulings in a Complex Technology Dispute

Introduction

The Quarter Turn Pty Ltd v Reinteractive Pty Ltd proceeding commenced on 22 January 2024 in the Federal Court of Australia (**FCA**), with Quarter Turn Pty Ltd (**Quarter Turn**) lodging an originating application and concise statement against Reinteractive Pty Ltd (**Reinteractive**), a developer of web and mobile applications.

Quarter Turn engaged Reinteractive to design a fitness marketplace application for both the web and mobile platforms (the App), under two Statements of Work. During the development phase, a dispute arose concerning alleged representations by Reinteractive about delivery timelines, and corresponding claims of breach for failure to deliver by those dates, which Quarter Turn contended were firm contractual obligations rather than estimates. Quarter Turn contended that Reinteractive did not meet the proposed timelines and asserts that no functional or launchable version of the application was delivered by the specified dates, or at all.

A series of interlocutory decisions occurred throughout the proceedings which illustrate the FCA's approach to case management in complex technology disputes. As events unfolded, Quarter Turn, sought to broaden its case by amending its pleadings to incorporate provision of technical source code and programming evidence. This expansion led to evidentiary consequences for both parties.

Application to Vacate Trial - *Quarter Turn Pty Ltd v Reinteractive Pty Ltd (No 3)* [2025] FCA 1431

On 24 October 2025, Quarter Turn lodged an interlocutory application to vacate the 7-day trial commencing 10 February 2026 (**Vacation Application**). In its submissions, Quarter Turn contended that the discovery materials provided by Reinteractive, comprising thousands of technical documents, necessitated an extended period of time for its technical expert to prepare his evidence, which would likely not be completed before the scheduled trial date.

In determining the Vacation Application, the FCA turned to the procedural history of the matter, including that:

- on 21 March 2024, an order was made for Quarter Turn to file its lay and expert evidence by 3 May 2024, which Quarter Turn failed to comply with;
- on 10 May 2024, a further order was made by consent, extending the time for the Applicant to file its lay and expert evidence to 31 May 2024. Again, Quarter Turn failed to comply with these orders;
- on 4 June 2024, the FCA ordered by consent, that Quarter Turn file its lay and expert evidence by 14 June 2024. This was a guillotine order, meaning that Quarter Turn required leave of the Court to lodge any further evidence after this date (**Guillotine Order**);
- Quarter Turn defaulted and served its evidence on 25 June 2024 in breach of the guillotine order;
- on 9 April 2025, the Applicant filed an amended originating application and amended concise statement. The amendment introduced a contractual claim based on an alleged breach of an implied term for performance of the contract within a reasonable time, or at all; and
- in May 2025, Quarter Turn informed Reinteractive for the first time that it intended to instruct Mr Michael Simonetti, to provide source code and programming evidence in relation to its claim. This was in circumstances where Quarter Turn's pleadings did not include a negligence claim such that a source code and programming expert was required to assess the reasonableness of the App delivered by Reinteractive.

Reinteractive opposed Quarter Turn's submissions and relied on the procedural history of the matter, including the Guillotine Order and late amendment of pleadings, resulting in a delayed instruction of its source code expert, Mr Simonetti. It also confirmed that the volume of discovery was a consequence of Quarter Turn's own request for eight categories of discovery, the scope of which spanned an extensive date range.

The FCA dismissed the Vacation Application, holding that Quarter Turn had already been afforded a reasonable and sufficient opportunity to adduce expert evidence and had failed to provide any cogent explanation for its delay.

The FCA emphasised the importance of early engagement especially in cases involving technical evidence in complex technology disputes and strict compliance with case management orders.

Vacating the trial dates would unfairly prejudice not only Reinteractive but other litigating parties and their respective matters at the FCA, and undermine the efficient administration of justice.

The decision underscores that parties cannot defer Court timetables by reference to the technical nature of expert evidence particularly where there has already been significant delay, late amendment to pleadings, and an evolving case theory, all of which has been induced by the vacating party itself. There must be a real and compelling justification for disrupting fixed trial dates especially on the basis that the nature and extent of the technical evidence should have least been anticipated by the party seeking to expand its pleadings and adduce this type of evidence.

Application to Set Aside Notice to Produce - *Quarter Turn Pty Ltd v Reinteractive Pty Ltd (No 2)* [2025] FCA 1389

In preparation for the Vacation Application, Reinteractive served a Notice to Produce on Quarter Turn seeking communications between Quarter Turn (and its lawyers) and the proposed technical expert, Mr Simonetti, relevant to the timing, instruction and circumstances of Mr Simonetti's engagement.

By a further interlocutory application dated 3 November 2025, Quarter Turn applied to set aside the Notice to Produce. In support of its application, Quarter Turn contended that the documents sought were irrelevant, and that they were protected by legal professional privilege.

Quarter Turn alleged that all of the documents comprised of confidential briefing materials between Quarter Turn's lawyer and its expert, created for the purpose of preparing evidence in the proceeding, in relation to Reinteractive's discovered source code materials.

The relevant issue turned on whether the communications were reasonably likely to bear on a central question in the foreshadowed Vacation Application, namely, the extent to which Quarter Turn's inability to serve expert evidence before trial was the result of its own conduct.

The FCA dismissed the application, holding that the documents sought were relevant to assessing whether Quarter Turn's procedural predicament was selfinflicted and therefore to the exercise of the FCA's discretion on Quarter Turn's Vacation Application.

The FCA also rejected the privilege claim, emphasising that legal professional privilege must be established by evidence, not merely asserted. Quarter Turn had adduced no evidence to substantiate the factual basis of its privilege claim, and the FCA was not prepared to assume that all communications with an expert attract privilege as a matter of course.

This decision reinforces the FCA's close scrutiny of parties seeking to claim privilege over expert communications, and considerations where a party insists that it is justifiable to delay a fixed trial date.

Second Security for Costs Application - *Quarter Turn Pty Ltd v Reinteractive Pty Ltd (No 4)* [2026] FCA 32

In September 2025, the FCA ordered Quarter Turn to provide $175,000 as security for Reinteractive's future costs in the proceeding. The Court recognised that Quarter Turn was impecunious, and that it was likely that Quarter Turn could not pay an adverse costs order if required. In its reasoning, the FCA emphasised that security for costs is meant to protect litigants, not punish parties, explaining that when someone brings high-value technology claims without financial means, the Court aims to balance access to justice with safeguarding litigants from costs they cannot recover.

The FCA followed the same approach in the further security for costs application brought by Reinteractive. This application flowed directly from Quarter Turn's expanded pleaded case which sought to introduce further source code and programming evidence from Mr Simonetti. Accordingly, the FCA awarded Reinteractive a further $350,000 as security for costs for the additional work required in connection with Mr Simonetti's evidence.

The FCA found that the introduction of technical evidence constituted a material change in circumstances, increasing the scope, complexity and cost of trial preparation. The FCA found that the inclusion of this stream of new technical evidence expanded the issues to be addressed at hearing, along with the necessary related preparation time.

The FCA referred to its first Security for Costs Application in which it determined that Quarter Turn is impecunious, and that the Applicant did not provide new evidence to confirm that its financial position had improved, nor did it contend that the making of a further security for costs order sought by the Respondent would stultify Quarter Turn's pursuit of the Proceeding.

The FCA accepted that those additional costs were a consequence of how Quarter Turn decided to advance its case, reinforcing that where a party's evolving technical strategy increases the burden on its opponent, the FCA will ensure appropriate costs protection.

The judgment emphasised again that security for costs serves a protective not punitive function, and that where an Applicant pursues high value technology claims without the financial capacity to meet adverse costs, the FCA will intervene to strike an appropriate balance between access to justice and fairness to litigants.

Application for Wasted Expenditure Claim - *Quarter Turn Pty Ltd v Reinteractive Pty Ltd (No 5)* [2026] FCA 102

In this proceeding, Quarter Turn's main allegations concerned Reinteractive's alleged misleading or deceptive conduct, and breach of contract with respect to works undertaken by Reinteractive on behalf of Quarter Turn. During the trial, the FCA provided reasons for Judgment to address an objection raised by Reinteractive to Quarter Turn's tendering of documents consisting of invoices between Quarter Turn and its vendors, such as Salesforce and Comet CX (**Vendors**), and bank statements recording all funds Quarter Turn incurred in the development of the website (**Wasted Expenditure Evidence**).

In submitting the Wasted Expenditure Evidence the FCA relied on the 'facilitation principle', under which, the Court will not permit a plaintiff to fail entirely merely because their evidence on quantum is weak, incomplete or imprecise. Instead, the Court will do the best it can to assess damages on the available material, rather than to deny recovery altogether. Quarter Turn claimed that the wasted expenditure claim is subsumed within its claim for loss of profits, such that no election is required between the two when quantifying its loss and that as the wasted expenditure claim has always formed a part of its pleaded loss of profits claim, Reinteractive has suffered no prejudice.

Reinteractive submitted that it understood Quarter Turn's claim to allege loss and damage comprising of profits, brand value, good will and commercial opportunity only. While Reinteractive accepted that generally a wasted expenditure claim is available in a case of this nature, the objection was taken pursuant to Section 136 of the *Evidence Act 1995* (Cth), which provides the Court with a discretion to limit the use to be made of evidence if there is a danger that a particular use might be "*unfairly prejudicial to a party*". Reinteractive was not aware until this date of Quarter Turn's intention to make a wasted expenditure claim.

The FCA relevantly assessed the communications between the parties, including Quarter Turn's pleadings. The FCA made orders to only allow Reinteractive's invoices in support of Quarter Turn's wasted expenditure claim, resulting in approximately 65% of the Wasted Expenditure Evidence being rejected. In making this order, the FCA was also receptive to Reinteractive's submission that Quarter Turn has failed to plead and particularise its wasted expenditure claim.

The FCA accepted Reinteractive's evidence, stating that the prejudice identified in Reinteractive's evidence in response to Quarter Turn's claim for wasted expenditure "*is a powerful factor in favour of the exercise of discretion in the manner sought by the Respondent*". The consideration of prejudice relates to "*the extent to which the respondent would be prejudiced by the acceptance into evidence on an unlimited basis*" of the above documents. The FCA emphasised the importance of carefully exercising discretion conferred by section 136 of the *Evidence Act*, to limit the use to be made of evidence if there is a danger of unfair prejudice.

Application to Appeal Wasted Expenditure Claim Decision - *Quarter Turn Pty Ltd v Reinteractive Pty Ltd (No 6)* [2026] FCA 125

On 18 February 2026, Quarter Turn made an oral application to appeal the FCA's order dated 16 February 2026, which rejected the invoices pertaining to Quarter Turn's Vendors from its Wasted Expenditure Evidence.

Two main points were raised in Quarter Turn's oral application. Firstly, Quarter Turn submitted that the danger of unfair prejudice to Reinteractive could be ameliorated by adjourning the

proceeding to allow time for Reinteractive to adduce evidence of the kind, including evidence responding to a wasted expenditure claim. Secondly, Quarter Turn reiterated its previous submissions, that Reinteractive should have already put on evidence responsive to Quarter Turn's wasted expenditure claim.

The FCA was not convinced on both grounds. On the first ground, the FCA emphasised that Quarter Turn's proposed adjournment to allow time for Reinteractive to adduce its responsive evidence would add to the length and cost of the trial. It also recognised that the suggestion for Reinteractive to adduce evidence responding to a wasted expenditure claim was not made by Quarter Turn at the time of introducing the Wasted Expenditure Evidence. On the second ground, the FCA considered it to be "*in substance an attempt to re-present previously unsuccessful arguments*", which should not be entertained in the interests of justice.

This interlocutory decision reflects the FCA's prioritisation of the "*interests of justice*" in proceedings. The FCA emphasised the overarching purpose of litigation in section 37M(1) of the *FCA of Australia Act 1976* (Cth), in "*facilitating the just resolution of disputes according to law and as quickly, inexpensively and efficiently as possible*".

Voir dire to determine admissibility of expert quantum evidence

Prior to the experts' conclave, Reinteractive was granted the opportunity to determine the admissibility of Quarter Turn's quantum expert, Dr Brent Coker's, expert evidence in a *voir dire*.

Counsel for Reinteractive cross-examined Dr Coker on several matters, such as:

- Dr Coker's expertise and experience, which supported that Dr Coker's specialisation is better characterised as a "marketing and brand expert" based on his curriculum vitae; and
- Dr Coker was asked about key financial and quantification terms, such as a weighted average cost of capital (**WACC**) and integers of a loss calculation. In response, Dr Coker confirmed that he was not trained in, nor worked as a business valuation expert or forensic accountant;

Dr Coker provided oral evidence that he was asked "to estimate the revenue, the customer data available and the brand". In doing so, Dr Coker clarified that his expertise fit squarely with Quarter Turn's loss of opportunity claim as he was not required to estimate loss, but the value of the brand and revenue available had the project been completed on time.

At the conclusion of the voir dire, the FCA ruled that the majority of both Dr Coker's first and second reports be rejected due to lack of expertise as a valuation expert. The refusal of Dr Coker's expert reports highlights the FCA's stringent approach to determining whether an individual holds specialised knowledge "*based on training, study or experience*" to answer the evidentiary issues and to assist the Court.

CASE NOTE: Nippon Life Insurance Company of America v. OpenAI Foundation (1:26-cv-02448)

In 2026, professional services industries are confronting a rapidly evolving risk environment shaped by the widespread adoption of generative artificial intelligence. AI chatbots are now routinely used by consumers and professionals alike, raising unresolved questions around data security, privacy, information control and (critically) liability where AI systems are used to generate advice traditionally delivered by licensed professionals.

A recently filed case in the United States highlights these tensions and provides an early test of how courts may approach liability allocation in AI-assisted legal disputes. The proceedings have potential consequences not only for technology providers but also for professional indemnity and other liability insurers operating in markets increasingly exposed to AI-enabled services.

Case Background

Nippon Life is a subsidiary of Japan's Nippon Life Insurance Co., providing long-term disability insurance products in the United States.

The claimant, Graciela Dela Torre, had previously settled her long-term disability benefits claim with prejudice in January 2024, with her employer insured by Nippon Life.

The Complaint

On 4 March 2026, Nippon Life commenced proceedings in the District Court of Illinois against OpenAI Foundation and OpenAI Group PBC (together, "**OpenAI**"), seeking approximately US$10.3 million in compensatory and punitive damages.

According to the complaint, following dissatisfaction with the settlement, the claimant contacted her former attorney, who confirmed that there were no deficiencies in the documentation supporting her disability claim. Despite this advice, the claimant allegedly uploaded attorney-client correspondence to ChatGPT. The chatbot's responses reportedly validated her dissatisfaction with the settlement.

The complaint alleges that the claimant subsequently terminated her legal representation and proceeded as a selfrepresented litigant, relying substantially on ChatGPT for legal advice. In response to her prompts, ChatGPT is alleged to have generated legal arguments asserting that her former attorney had improperly pressured her into signing a blank signature page.

Nippon Life further claims that ChatGPT assisted with at least 44 court filings across two recent proceedings against Nippon Life and another insurer, including the citation of a fabricated case, which "only exists in Dela Torre's papers and the "mind" of ChatGPT".

Causes of Action

The complaint sets out three causes of action against OpenAI, framed on the basis that OpenAI is a commercial entity capable of attracting tortious liability. These include:

1. Tortious interference with a contract;
2. Abuse of process; and
3. The unlicensed practice of law

Tortious interference with a contract

Nippon Life alleges that OpenAI, through the outputs of ChatGPT, intentionally interfered with the binding settlement agreement between Nippon Life and Dela Torre. The pleaded case is that ChatGPT encouraged the claimant to breach the settlement, attempt to reopen a dismissed claim and initiate fresh proceedings asserting the same causes of action.

The complaint emphasises that ChatGPT allegedly characterised the advice of the claimant's former attorney as an attempt to "*gaslight*" her, thereby undermining confidence in the settlement and inducing repudiation of a concluded contract.

Abuse of process

The second cause of action alleges that the claimant (on ChatGPT's advice) filed frivolous motions and requests for judicial notice "*with no legitimate or proper purpose*". Nippon Life contends that the filings were designed to harass, burden and publicly defame the insurer, amounting to an abuse of the court's processes.

Importantly, the complaint seeks to attribute this conduct to OpenAI, alleging that ChatGPT materially assisted in the preparation, drafting and legal analysis underpinning these filings. OpenAI is pleaded to be a joint tortfeasor by virtue of providing legal research, advice and document drafting that facilitated the alleged abuse of process.

The unlicensed practice of law

The third (and most novel) cause of action concerns the alleged unlicensed practice of law. Nippon Life asserts that ChatGPT was "*intentionally designed*" to allow users to obtain legal research, legal analysis, legal advice and draft legal documents.

The complaint draws attention to the fact that, while ChatGPT reportedly achieved a combined score of 297 on the Uniform Bar Examination, it is not admitted to practise law in Illinois or any other US jurisdiction. The pleading raises the question of whether an AI system, and by extension its operator, can attract liability when it performs functions indistinguishable from those of licensed legal practitioners.

This claim is brought against the backdrop of changes to OpenAI's terms of use introduced in November 2025, which prohibit the provision of tailored advice requiring a professional licence (such as legal or medical advice) without appropriate involvement by a licensed professional.

Status of Proceedings

These allegations have not yet been tested at trial, and no final judgment has been delivered. Nonetheless, the pleadings themselves are notable for the breadth of liability asserted and the willingness to frame AI-generated outputs as actionable wrongs.

Implications for Professional Indemnity and Related Insurance Markets

Although still at an early stage, the proceedings have potentially significant implications for technology and professional indemnity insurers. The complaint highlights growing scrutiny on AI terms of use and "*failure to warn*" exposures, the systemic risk posed by AI hallucinations and aggregation issues, and uncertainty over whether AI-generated outputs constitute a "Professional Service" or a product failure.

The case may also influence underwriting of legal service providers, medical practitioners and other professional service providers using generative AI, as insurers assess whether reliance on AI shifts risk from individual negligence to firm-wide systemic exposure, with potential impacts on coverage scope, limits and pricing.

Advisory

NIST Publishes Draft Cyber Framework for AI (IR 8596)

The United States National Institute of Standards and Technology (NIST) released in December 2025 the initial preliminary draft of its Cybersecurity Framework Profile for Artificial Intelligence (Cyber AI Profile), published as NIST IR 8596.[60] The profile aims to address how organisations can adopt AI while addressing the risks arising from its advancements.

The preliminary draft offers guidelines for using the NIST Cybersecurity Framework (CSF 2.0) to accelerate the secure adoption of AI,[61] and extends existing standards by mapping AI-specific risks and controls to familiar CSF functions, categories, and outcomes. NIST envisions that the NIST CSF, NIST AI Risk Management Framework, and the Cyber AI Profile be used together.[62] The Cyber AI profile organises guidance around three overlapping focus areas:

- *Secure* (protecting AI system components by managing cyber challenges when integrating AI into organisational infrastructure.).
- *Defend* (leveraging AI to enhance cybersecurity operations).
- *Thwart* (building resilience against AI-enabled attack vectors such as deepfakes, AI-generated phishing, and adversarial manipulation of models).

The preliminary draft integrates AI-specific considerations across all six core functions of the NIST CSF 2.0 (Govern, Identify, Protect, Detect, Respond, and Recover), with sample considerations provided for each of the three Focus Areas. Each consideration is assigned a proposed priority level: High (1), Moderate (2), or Foundational (3), intended to guide organisations on where to focus first and to support structured planning toward their cybersecurity objectives.[63]

The profile addresses the growing cyber risk caused by the development of AI. The ACSC warns that AI allows threat actors to scale phishing, data analysis, and impersonation activity more efficiently than ever before, with AI-enabled cyber-attacks rising 47% in 2025 globally.[64] In April this year, Anthropic released information regarding Claude Mythos Preview. In a short period, Mythos identified thousands of critical zero-day vulnerabilities across major operating systems and browsers, including flaws that had gone undetected for up to 27 years, and demonstrated the ability to chain exploits autonomously without human direction. As Anthropic noted, it is only a matter of time before similar capabilities proliferate more broadly.[65] Days later, OpenAI unveiled GPT-5.4-Cyber, a variant of its flagship model specifically optimised for defensive cybersecurity use cases. Together, these developments signal a rapid convergence of advanced AI capability and cybersecurity, that organisations can no longer treat as a distant concern.

While NIST standards are not mandatory in Australia, the NIST CSF 2.0 is widely adopted, with Australian organisations increasingly integrating it alongside other frameworks such as Essential 8 or regulatory specific frameworks. NIST plans to develop an initial public draft for release in 2026, with the final profile expected to include expanded mappings to the NIST AI Risk Management Framework.

It's important to note however, that while frameworks such as the Cyber AI Profile are a necessary starting point, effective cyber management of AI requires organisations to go further. At its core, AI risk management must focus on the underlying data assets and systems that AI touches. Organisations also need to recognise that they face three distinct AI risk profiles simultaneously:

- Shadow AI: unsanctioned tools adopted outside of formal processes.
- Basic AI Users: staff using low or no-code tools and chat interfaces.
- Advanced AI Users: developers and agentic AI deployments with deeper system integration and broader access.

The Cyber AI Profile provides a strong lens through which to identify and prioritise controls, but it must be contextualised to each organisation's specific environment, data assets and risk appetite before it can be operationalised effectively.

Lastly, this space is evolving rapidly, and AI cyber risks and controls frameworks will need to be agile and dynamic to move with speed.

60. Cybersecurity Framework Profile for Artificial Intelligence
61. Draft NIST Guidelines Rethink Cybersecurity for the AI Era | NIST
62. KPMG - NIST Draft Cybersecurity Framework for AI
63. New Guidance from NIST Demonstrates How Organizations Can Use AI for Cybersecurity: Stinson LLP Law Firm
64. ASD Cyber Threat Report 2025 Insights | CyberPulse
65. Anthropic Project Glasswing

INC Ransom Affiliate Model Enabling Targeting of Critical Networks

The Australian Cyber Security Centre (ACSC), Kingdom of Tonga's CERT Tonga, and New Zealand's National Cyber Security Centre (NCSC) have jointly issued an advisory outlining the activity of ransomware group INC Ransom and its affiliate network, and the threat their operations pose to networks hosted in Australia, New Zealand, and the Pacific island states.[66]

INC Ransom is a Russian-based, financially motivated cybercriminal group that operates a Ransomware-as-a-Service (RaaS) model, in which core operators develop and maintain the ransomware platform and lease it to affiliates who carry out intrusions in exchange for a share of ransom proceeds. INC Ransom and its affiliates have been increasingly observed targeting Australia, New Zealand, and the Pacific island states since early 2025, having previously focused on the United States and United Kingdom.

Affiliates obtain initial access through spear-phishing campaigns, exploitation of unpatched internet-facing systems, and the use of valid credentials purchased from initial access brokers. After gaining a foothold, they create new privileged accounts, move laterally within networks, compress and exfiltrate data using legitimate tools, and then encrypt systems.[67] Between 1 July 2024 and 31 December 2025, the ACSC responded to 11 reported INC Ransom incidents in Australia, predominantly affecting professional services and health care organisations, with data exfiltration of personally identifiable and medical information observed in some cases. The group employs double-extortion tactics, threatening to publish stolen data on its dedicated leak site if demands are not met. The RaaS model has lowered the barrier to entry for a broad range of threat actors and enabled affiliates to target critical infrastructure - with minimal technical skill of their own.[68]

The ACSC has recommended that organisations prioritise regular backups, harden remote access, implement phishing-resistant MFA, maintain vulnerability management, restrict network traffic and control privileged access.

66. INC Ransom Affiliate Model Enabling Targeting of Critical Networks | Cyber.gov.au
67. Authorities warn of INC Ransom impact on regional networks | Insurance Business
68. INC Ransom's Franchise Model Is Putting Critical Infrastructure On The Chopping Block - The Cyber Express

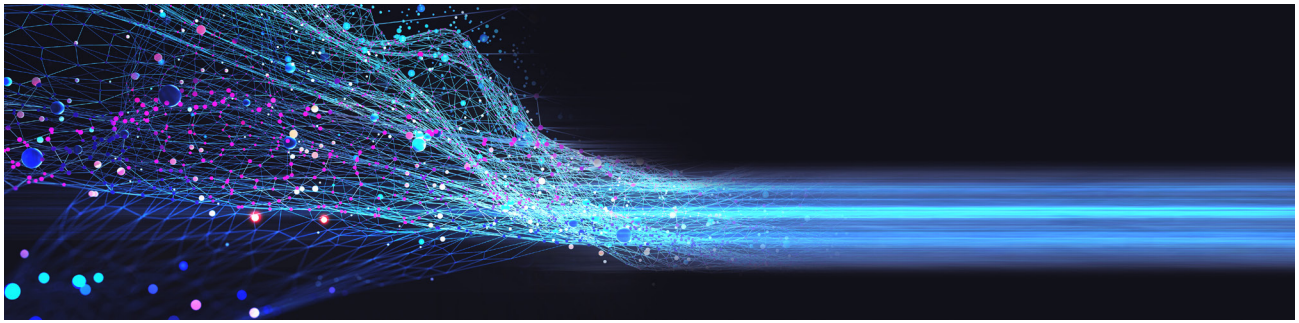
New Zealand

The New Zealand National Cyber Security Strategy

Following a series of high-profile incidents the New Zealand Government released New Zealand's first Cyber Security Strategy for 2026-2030 in February this year. The strategy is supported by the Cyber Security Action Plan 2026-2027, which sets out more immediate, granular objectives.

As you might expect, the Strategy sets out the prominent and growing risk that cybercrime and data risks pose to New Zealand, and the associated concern from the public. The Strategy and Action Plan then go on to set out four main areas of focus to immediately improve New Zealand cyber risk posture:

- **Understand** – The NCSC is tasked with establishing a single point for cyber incident reporting to improve data quality and access to assistance. The NCSC is also tasked with providing operators of critical infrastructure with support and guidance.
- **Prevent and Prepare** – Perhaps most notably in the entire Action Plan – the Ministry of Justice is tasked with providing advice on options to *"incentivise the protection of personal information from cyber threats, such as introducing a civil pecuniary penalty regime to the Privacy Act 2020."* DPMC will develop options to improve the cyber security of critical infrastructure, including through public consultation on regulatory proposals. Higher and more consistent security standards are to be embedded in digital procurement and design across Government, and the mandate of the Government Chief Digital Officer is to be expanded.



- **Respond** – As well as considering a potential civil penalty regime for the Privacy Act 2020, the MoJ is also tasked with advising on a new offence targeted at individuals who view, possess or disseminate personal information when they are aware it has been obtained illegally. DPMC and the PSC are tasked with managing public service use of high-risk, vendors, services and products. DPMC is also tasked with updating regulatory powers enable the security sectors use of cyber capabilities and tools.
- **Partner** – NCSC is tasked with deepening collaboration with the cyber security industry, as well as bolstering regional engagement across the Pacific.

The Strategy and Action Plan outline a range of potential bold initiatives that could fundamentally shift the cyber and data risks environment in New Zealand. Some of these initiatives are already underway. The first round of consultation for regulation or critical national infrastructure cyber security regulation is already complete.

Other changes may take more time but will have a very real impact on the risk posed by malicious cyber incidents in particular. The directive that MoJ consider potential changes to the Privacy Act 2020 aligns with the Office of the Privacy Commissioner's own push for change, particularly in the area of civil penalties. The adoption of an "access" type of offence will also directly address the continued need to obtain injunctions against "persons unknown" in ransomware scenarios (the topic of another article in this quarter's bulletin).

The WK cyber, data and technology team will be keeping a close eye on developments as they unfold. If you have any questions about the Strategy or Action Plan, or developments in cyber and data risks more generally, please reach out to a member of our team.

New OPC Guidance Signals Rising Expectations for Children's Privacy Protection

Strengthening privacy protections for children has been one of the Office of the Privacy Commissioner's core strategic priorities since it launched the Children's Privacy Project in 2023. As part of the project, on 11 March 2026 the OPC released new 289-page privacy guidance for the education sector.

The guidance is intended for those working with learners and covers 16 topics. Highlights include:

Commentary on the interaction between the Privacy Act 2020, other relevant legislation (the Education and Training Act 2020, Public Records Act 2005, Oranga Tamariki Act 1989, and Family Violence Act 2018), and relevant codes such as the Teachers Code of Professional Responsibility.

Guidance on common privacy topics, such as transparency and notice requirement for learners and parents, including age appropriate notification, and managing common privacy issues such as access requests, accuracy, and security considerations in an education context.

Guidance on managing privacy incidents, including development of privacy incident management plans and maintaining privacy incident registers.

Risk management of new digital technologies in education contexts.

The guidance complements existing OPC guidance for children's privacy relating to children's privacy, including information sharing, photographing and filming children and young people, best practice when responding to requests for a child or young person's personal information, and how to help children, young people and their parents protect their privacy while exploring the online world.

This guidance is likely to be treated not only as best practice but, increasingly, as a de facto standard. This projection is reinforced by the OPC's decision to issue a Compliance Notice to Oranga Tamariki in May 2025. The Notice was issued following a series of privacy breaches relating to the storage, security and unauthorised disclosure of personal information that have caused serious harm to children. Over time, it will become less defensible for organisations to maintain privacy governance frameworks that do not align with the guidance.

Looking under the hood - the Manage My Health Inquiry

On 30 December 2025, the patient portal platform Manage My Health suffered a third-party cyber breach, resulting in the exfiltration of patient health information and data stored on the platform. Following the breach, both the Ministry of Health and the Office of the Privacy Commissioner announced that they would be conducting inquiries into the breach. While both inquiries are in their early stages, they are a timely reminder of the steps the Government and OPC might look to take in the wake of a prominent cyber or data incident.

The material purpose of both inquiries is largely the same - to assess the cause of the incident, review the adequacy of the data protections that were in place at the time of the breach, Manage My Health's and Health New Zealand's response to the incident, and to recommend any improvements required to prevent similar incidents.

In the case of the OPC, the inquiry is a good reminder of the various powers the Commissioner has under the Privacy Act. Under part 5, sub part 2 of the Act the OPC can initiate investigations on its own account. In doing so the OPC has the power to regulate is own procedure in an investigation, summon persons and request information, and refer unresolved complaints to the Director of Human Rights Proceedings.

As New Zealand's privacy regulator, the OPC has a public assurance function and may make public comment on privacy issues that are of serious concern to the public. As set out in the relevant Terms of Reference for the MMH inquiry, the OPC anticipates issuing reports following the completion of each stage of the inquiry. The findings will be used to improve processes and systems to help prevent similar incidents and/or reduce the impact as a result of such incidents.

While the Privacy Commissioner does not have the power to charge or issue fines to Manage My Health or any associated agencies, the inquiry has scoped in compliance with the Privacy Act 2020 and the Health Information Privacy Code 2020. As a result, the findings from the inquiry, and any referral to the Director of Human Rights Proceedings, will no doubt be of great interest to privacy and data risk professionals.

Injunctions against persons unknown, the new norm in ransomware attacks

The first quarter of 2026 saw a spate of applications for injunctions against "persons unknown" in the New Zealand High Court following several public ransomware attacks and data leak threats. Prominent examples include the Manage My Health[69] and Neighbourly[70] incidents.

The Office of the Privacy Commissioner has long commended the use of injunctions in the context of cyber incidents and privacy breaches. But what are they? How do you get one? And what are the pros and cons of obtaining this kind of injunctive relief?

Injunctions against "persons unknown"

Injunctions against "persons unknown" are applications for orders restraining individuals from interacting with or publishing information stolen or leaked in cyber incidents and data breaches.

Because the wrongdoers' identities are unknown at the time of the breach, these injunctions are framed broadly to capture anyone acting unlawfully with the data in question. This includes the activities of not just the attackers, but third parties who may look to interact with the information.

The importance of such broad orders was made clear following the ransomware attack against the Waikato District Health Board in 2021, following which various media outlets accessed and reported on the content of leaked data, resulting in further invasions of individuals' privacy.[71]

How are orders obtained?

Orders are obtained via application to the High Court. Recent prominent examples include *Neighbourly Ltd v Unknown defendants* [2026] NZHC 1 and *Manage My Health Ltd v Unknown Defendants* [2026] NZHC 2.

In practice, seeking injunctive relief of this nature involves filing formal proceedings and an associated application for injunctive relief. The application will then need to satisfy the usual requirements for injunctive relief: that there is a serious question to be tried; that the balance of convenience lies in favour of an injunction; and that granting of an injunction is in the interest of justice. The available precedent shows that these requirements will typically be made out in ransomware and cyber incident scenarios, provided sufficiently detailed supporting evidence is supplied. Causes of action in breach of confidence and breach of privacy are typically easily supported, and there are compelling reasons to restrict access to leaked information as far as possible (particularly if the victim organisation is the subject of an extorsion).

What are the pros and cons of seeking an injunction against "persons unknown"?

The advantages of seeking orders of this nature are clear. While threat actors and other malicious third parties may pay injunctions of this nature little mind, orders are typically effective against media and publicly identifiable third parties.

Reporting on cyber incidents comes from an increasingly broad group – extending from professional mainstream media through to bloggers and interested cyber security professionals with a social media account. Injunctions against "persons unknown" are a helpful tool for addressing the entire media spectrum. Obtaining an injunction also sends a positive message to stakeholders and impacted individuals that the subject of an attack or data breach is taking all possible steps in response.

In saying that, parties should also be realistic about the limitations of injunctions against "persons unknown" and the associated draw backs. As noted, there is little evidence that threat actors and malicious third parties pay heed to this kind of injunctive relief. Applications also run the risk of exposing further information about an incident then may be desirable. By their very nature the applications require supporting evidence of the nature and extent of the incident. While Court files can sometimes be sealed, judgements are typically public, and media and members of the public can apply to have access to documents filed in support. The decision to apply for an injunction in the first place can be a delicate balancing act.

WK's cyber, data and technology team has considerable experience obtaining and advising on injunctive relief, including seeking injunctions against "persons unknown" in cyber and data incidents. If you have further queries on this topic, please reach out to a member of the team.

69. MMH Cyber Breach Update March 15 2026 | Manage My Health
70. Q&A regarding Neighbourly data breach 03/01/2025 – Neighbourly
71. Seven Complainants and Radio New Zealand Ltd - 2021-090 (14 September 2022)

Singapore

European Union (EU) - Singapore Digital Trade Agreement entered into force on 1 February 2026

The EU-Singapore Digital Trade Agreement (**DTA**) officially came into force on 1 February 2026, setting the bar for the standard of transparency required for cross-border digital transactions. Building on from:

i. the EU–Singapore Digital Partnership and the Digital Trade Principles that Singapore and the EU entered into on 1 February 2023; and

ii. the longstanding free trade arrangements (by way of the Partnership and Cooperation Agreement and Free Trade Agreement (**FTA**) between Singapore and the EU since 2018;

As the EU's first standalone bilateral digital trade agreement, it reflects the strategic importance of digital trade between the EU and Singapore. Several provisions in the DTA supersede those in the FTA, positioning it as the primary framework governing EU–Singapore digital trade.

What the agreement covers

The DTA establishes a framework to facilitate cross-border digital transactions, promote paperless trade and enhance online consumer safety and trust vis-a-vis consumer data protection and trust through improving access to safety and redress mechanisms. A key objective is to provide legal certainty for businesses (e.g. removing data localisation requirements), while addressing barriers to digital commerce.

Digital trade refers to digital transactions, that is, commerce (i.e. trade in both goods and services) enabled by electronic means and digital technologies (e.g. telecommunications, and other information and communication technologies). Examples include goods and services ordered and delivered digitally, or goods and services ordered digitally and delivered physically, and related permutations. Digital trade also invites consideration of issues such as cross border data transfer and the use of technology in the production and distribution process.

Key provisions

- Article 5 – Cross Border Data Flows
  - Article 5 sets out certain measures which the Partiers should not adopt so that the cross-border transfer of data is not prohibited or restricted.
  - Parties have agreed to keep the implementation of this provision under review and assess its functioning within three years of the effective date of the DTA (i.e. by 31 January 2029).
  - Parties have agreed not to hamper the transfer of data across jurisdictions such that digital trade may flow more freely by generally permitting data transfer from Singapore to EU and vice versa, as well as the storage or processing of data in EU/ Singapore territory.
  - To this end, parties will:
    - not require the use of computing facilities or network elements in EU/ Singapore's territory for processing of data, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of that party;
    - not require the localisation of data in EU/ Singapore's territory for storage or processing;
    - not make the cross-border transfer of data contingent upon use of computing facilities or network elements in EU/ Singapore's territory or upon localisation requirements in that party's territory
- Article 6 – Personal Data Protection
  - Article 6 of the DTA recognises that individuals have a right to privacy and that high and enforceable data protection standards contribute to trust in the digital economy.
  - Each party must maintain a legal framework protecting personal data, and should publish guidance on how individuals can pursue remedies and how enterprises can comply with legal requirements
  - Parties will explore convergence between their respective data protection regimes to facilitate cross-border data flows (e.g. the recognition of regulatory outcomes, broader international frameworks, or joint guidance on the utilisation of common cross-border data transfer mechanism).

- Article 22 – Cybersecurity
  - Recognising that cybersecurity threats undermine digital trade, Article 22 of the DTA prescribes that the EU and Singapore should adopt a risk-based approach by:
    - building their national cybersecurity incident response capabilities;
    - collaborating to identify, mitigate and protect against cybersecurity risks (e.g. malicious intrusions or dissemination of malicious code that affect electronic networks), detect cybersecurity events, expeditiously respond to and recover from cybersecurity incidents, and share information to develop greater awareness;
    - encouraging enterprises to adopt risk management best practices.
- Article 13 – Unsolicited commercial electronic messages
  - Article 13 deals with unsolicited electronic commercial messages, which the Do Not Call (**DNC**) Provisions under the Singapore Personal Data Protection (Do Not Call Registry) Regulations 2013 lend themselves to. Essentially, the Regulations protect consumer privacy by preventing unsolicited communications. They contain a prohibition against organisations sending marketing messages to telephone numbers of individuals registered in the DNC Registry.

Singapore and Australia renew Memorandum of Understanding (MOU) to enhance Cyber Security Cooperation

Singapore and Australia have renewed their bilateral cybersecurity cooperation agreement, reinforcing a partnership that now spans nearly a decade.

Singapore and Australia first signed an MOU on cybersecurity collaboration in 2017, which was renewed in 2020. The 2026 renewal recognises the need for continued cooperation, and in fact an enhancement of the same. The renewed MOU expands the scope of cooperation to include information exchange on cybersecurity incidents and threats, sharing of regulatory, policy and operational developments, risk management and mutual recognition of cybersecurity labelling and certification schemes.

There will also be more joint cybersecurity exercises (generally focussing on the protection of critical information infrastructure), training and education and sharing of best practices. The aim is to promote innovation, trade, and investment, as well as regional confidence-building and capacity-building measures.

Singapore and Australia have also entered into an MOU concerning Enhanced Defence Cooperation in October 2025 which addresses cyber defence collaboration.

The renewal carries broader strategic significance as both countries have been tightening their domestic cybersecurity frameworks – Singapore through amendments to its Cybersecurity Act 2018 and the new Cyber Trust Mark certification mandates, and Australia through its 2023-2030 Cyber Security Strategy. The MOU creates a channel to align these efforts and share learnings across jurisdictions, particularly as both nations grapple with similar risks of threat actors targeting critical information infrastructure.

Enhancing Cybersecurity standards for key stakeholders in the cybersecurity domain

In March 2026, the Cybersecurity Agency (**CSA**) announced new mandatory cybersecurity certification requirements for Critical Information Infrastructure Owners (**CIIOs**), auditors conducting CII audits and licensed cybersecurity providers to meet Cyber Trust Mark (**CTM**) certification requirements. The move is aimed at raising baseline national cybersecurity standards and addressing supply chain risks.

From February 2026, CSA has discontinued its CTM programme named Cyber Trust (2022) which certifies an organisation for meeting classical cybersecurity standards and instead rolled out an enhanced Cyber Trust (2025) to address newer risks in cloud security, operational technology security and artificial intelligence security in addition to cybersecurity. This is now in effect.

Who is affected and by when

- CII auditors are to obtain the CTM certification by 31 December 2026.
- Licensed cybersecurity service providers (covering penetration testing and managed SOC monitoring) must obtain the CTM Level 3 (Promoter tier) by 31 December 2026.
- Licensed cybersecurity service providers who provide penetration testing (**PT**) and managed security operations centre monitoring (**MSOC**) services are to hold a CTM Tier 3 certification by 31 December 2026.
- CIIOs are required to obtain the CTM Tier 5 certification (the highest tier) by 31 December 2027 for non-CII systems under its control.

Why this matters

The timing of these requirements is no coincidence – it follows a series of regulatory and real-world developments that have shifted how Singapore views cyber risk. On the threat front, Singapore's telecommunication infrastructure was subject to recent attacks by UNC3886, a sophisticated state-linked espionage group. An increasing number of incidents caused by advanced persistent threats have also been a cause of concern. These heightened cybersecurity standards follow amendments to the Cybersecurity Act 2018 last year to strengthen incident reporting requirements for CIIs.

Taken together, the CTM certification mandate is best understood as the structural complement to enhanced incident reporting obligations. UNC3886 demonstrates sophisticated tactics such as "living off the land" techniques that exploit legitimate tools and blend into normal network activity, making them nearly invisible to organisations without strong detection and monitoring capabilities.

The CTM requirements are designed to close this gap, ensuring that key stakeholders in the cybersecurity domain maintain the depth of security practice needed to surface these threats before they propagate.

Singapore Reveals State-Linked Cyber Espionage Campaign Against Telecoms Sector

Cyber incidents today may carry national, operational, regulatory and contractual consequences even where no personal data is compromised. National risk may exist even without breaches that are reportable to the Personal Data Protection Commission in Singapore.

On 9 February 2026, Singapore's Cyber Security Agency (**CSA**) and the Infocomm Media Development Authority (**IMDA**) confirmed that all four major Singaporean telecommunications providers, Singtel, StarHub, M1 and Simba Telecom, which are critical information infrastructure (**CII**) owners, had been targeted in a sophisticated espionage campaign attributed to the cyber threat group UNC3886[72]. These incidents triggered the country's largest coordinated cyber security response to date.[73]

According to the CSA, advanced persistent threat group UNC3886 gained access to the telecom systems during a coordinated campaign which was "deliberate, targeted and well-planned."[74] While the intrusions did not result in service disruptions or the compromise of personal customer data, investigators found that the group was able to exfiltrate a limited amount of network-related technical information intended to support longterm espionage objectives.

The threat actor campaign prompted a largescale government response titled '*Operation Cyber Guardian'* which CSA and IMDA described as "Singapore's largest coordinated cyber incident response effort"[75]. The operation ran for more than 11 months and involved over 100 cyber defenders from multiple agencies working alongside telecom providers to contain the threat, remove persistent access and strengthen network defences.

Security researchers and government officials have linked the threat actor group UNC3886 to Chinanexus cyber espionage activity targeting strategic sectors globally, including telecommunications, defence and technology.[76] CSA said UNC3886 demonstrated "deep capabilities"[77] typical of advanced persistent threats. The Singaporean authorities warned that the telecom infrastructure still remains a target for statebacked actors given its importance to national security and economic stability, and cautioned that despite the successful containment of this campaign, further attempts to access their critical networks could still occur.[78] The government framed the risk as extending to essential services such as banking, healthcare and transport, which are CII sectors regulated by the CSA.

UNC3886 is known for:

- Zero-day exploitation (Fortinet firewalls, VMware vCenter / ESXi);
- Virtualisation-layer compromise; and
- Rootkits and long-term persistence, not smash-and-grab ransomware.

This means standard and traditional tooling which focuses on endpoint level visibility may be inadequate since UNC3886 would deliberately attack below this layer. The scope of "reasonable security measures" will have to be expanded to take this into account.

The UNC3886 incident marks a shift in Singapore from cyber incidents as compliance events to cyber operations as national-security risks. Although not all high-impact cyber incidents involve personal data, private and public organisations alike should give due regard to spanning data protection, cybersecurity regulation, and board-level risk governance collectively, instead of treating them as silos.

72. Largest Multi-Agency Cyber Operation Mounted to Counter Threat Posed by Advanced Persistent Threat (APT) Actor UNC3886 to Singapore's Telecommunications Sector | Cyber Security Agency of Singapore; Singapore says cyber espionage group targeted telco infrastructure | Reuters
73. Largest Cyber Operation Mounted to Counter UNC3886's Threat | IMDA; China-Linked UNC3886 Targets Singapore Telecom Sector in Cyber Espionage Campaign
74. Singapore's four major telcos came under attack by cyber espionage group UNC3886 - The Business Times
75. Largest Cyber Operation Mounted to Counter UNC3886's Threat | IMDA; Largest Multi-Agency Cyber Operation Mounted to Counter Threat Posed by Advanced Persistent Threat (APT) Actor UNC3886 to Singapore's Telecommunications Sector | Cyber Security Agency of Singapore
76. Singapore mounts largest ever cyber operation to oust APT actor | Computer Weekly
77. Largest Multi-Agency Cyber Operation Mounted to Counter Threat Posed by Advanced Persistent Threat (APT) Actor UNC3886 to Singapore's Telecommunications Sector | Cyber Security Agency of Singapore
78. Singapore says cyber espionage group targeted telco infrastructure | Reuters

MAS launches AI Risk Management Toolkit for Financial Institutions

On 20 March 2026, the Monetary Authority of Singapore (**MAS**) published an AI Risk Management Toolkit for the financial services sector as part of a broader industry initiative known as Project MindForge led by MAS. Project MindForge was created in 2023 to promote the adoption and responsible use of AI among financial institutions.

MAS has been building up to this for some time, starting with the issuance of the 14 Principles to Promote Fairness, Ethics, Accountability and Transparency for responsible AI use in the financial services sector (**FEAT**) back in 2018, followed by the Veritas Initiative to operationalise those principles between 2020 to 2023.

The Toolkit contains (a) an Executive Handbook; (b) an Operationalisation Handbook; and (c) Implementation Examples. It aims to address governance and risk management for all types of AI including traditional AI, Generative AI and Agentic AI.

At its core, the Operationalisation Handbook structures around four main areas:

1. **Oversight** (i.e. establishing clear roles and responsibilities for AI supervision);
2. **AI Risk Management** (i.e. defining and establishing frameworks for effective AI identification, risk materiality assessment, AI inventorisation, policies and procedures);
3. **AI Lifecycle Management** (i.e. implementation of controls covering the entire lifecycle of AI use); and
4. **Enablers** (i.e., development of organization capabilities, infrastructure and resources to enable ongoing responsible AI use and risk management).

The Operationalisation Handbook (in line with MAS' initial paper on AI Model Risk Management in 2024, the consultation paper proposed by MAS on AI Risk Management Guidelines in late 2025 and the MAS Technology Risk Management Guidelines from 2021) also makes clear that the Board and Senior Management are primarily responsible for ensuring effective AI-related policies, procedures and standards.

The Toolkit will be periodically updated. MAS will also establish an AI risk management workgroup under MAS' Financial AI Builder programme (also known as Buildfin.ai) to develop implementation resources, facilitate knowledge sharing and build capabilities and frameworks for managing emerging AI risks.

The Toolkit is designed as a practical, operational guidance for financial institutions. When the MAS AI Risk Management Guidelines are published in due course, they will represent supervisory standards expected of financial institutions (although not technically binding).

Infocomm Media Development Authority (IMDA) Model AI Governance Framework for Agentic Artificial Intelligence (AI)

On 22 January 2026, Singapore's IMDA launched the world's first governance framework specifically designed for agentic AI i.e. AI systems capable of autonomous planning, reasoning and action. The Model AI Governance Framework (**MGF**) is targeted at organisations looking to deploy agentic AI, whether through developing AI agents in-house or via third-party agentic solutions.

Unlike traditional AI or generative AI, agentic AI can reason and take actions on behalf of users. This comes with a new set of risks as the increased autonomy of agentic AI also means more challenges in accountability and possible unauthorised actions (e.g. processing a non-intended payment, releasing sensitive personal information). This is known as "process hallucination" where the agent executes a wrong sequence of actions, or claims to complete a step it never performed.

The MGF outlines four core dimensions:

1. **Assess and mitigate risks upfront**: Determine suitable use cases for agentic AI deployment and design choices to mitigate the risks upfront.
2. **Make humans meaningfully accountable**: Establish chains of accountability within and outside the organisation across the agent value chain and lifecycle, and adopt measures to enable meaningful human oversight (e.g. requiring human approval at significant checkpoints).
3. **Implement technical controls and processes**: Implement technical controls during design and development stage, test agents for safety and security pre-deployment, and when deploying them, perform a gradual roll out and continuous monitoring in production.
4. **Enable end-user responsibility**: Provide sufficient information to end users to promote trust and enable responsible use (e.g. information on the agent's capabilities and contact points for escalation in the event of malfunction, education on the proper use and oversight of agents).

The MGF does not sit alone as it is only one part of the growing body of local and regional governance instruments relating to AI. While compliance with the MGF is not mandatory, it does present a set of best practices that organisations deploying agentic AI are encouraged to adopt.


Thailand

Cyber-incidents emerge as top Thailand's top business risk for 2026

At a glance:

Cyber incidents are now the number one business risk in Thailand for 2026, according to the Allianz Risk Barometer 2026.

The risk is amplified by AI-enabled attack methods and increasing dependence on third-party service providers.

Enforcement of Thailand's Personal Data Protection Act (**PDPA**) has entered a more assertive phase, with the Personal Data Protection Committee (**PDPC**) actively imposing fines on both data controllers and processors following cyber incidents.

Rise of cyber risk

According to the Allianz Risk Barometer cyber-incidents are the leading business risk in Thailand for 2026, rising four places to be cited by 37% of Thai respondents, up from 21% the previous year. This ranking reflects what many organisations have experienced firsthand. Attacks on Thai businesses and public institutions have increased markedly in both frequency and sophistication, with government agencies, financial institutions, and critical infrastructure emerging as prime targets. While phishing and social engineering remain the most prevalent entry points, the growing deployment of artificial intelligence by threat actors is giving rise to attacks that are faster to execute, harder to detect, and more difficult to contain once underway.

Third-party issue

A consistent feature of significant cyber incidents in Thailand is that the point of compromise often lies outside the affected organisation's own systems. Instead, breaches frequently originate through third-party vendors or service providers that process personal data on the organisation's behalf.

This mirrors patterns observed in prior largescale incidents, including the massemail service provider breach in November 2025. In that case, attackers gained access to a platform shared by multiple corporate clients, exposing recipient data and facilitating widescale phishing campaigns, even though the clients' internal systems were not directly compromised. From a legal perspective, however, regulatory exposure remained firmly with those clients as data controllers.

Under the PDPA, an organisation's responsibility for personal data does not end at its own perimeter. Data controllers remain accountable for the adequacy of security measures implemented by their data processors. Selecting vendors based on cost or convenience, without meaningful assessment of their security posture, has emerged as a common weakness identified in PDPC investigations.

PDPA enforcement: a harder line

The PDPC's regulatory posture has shifted materially over the past year. In August 2025, the PDPC announced eight administrative fines across five noncompliance cases, bringing total fines imposed since PDPA enforcement commenced to more than THB 21.5 million. Both public and private sector entities were fined, and the cases reveal several consistent themes.

In at least one matter, the service provider acting as data processor received a higher fine than the organisation that engaged it. This reflects a clear regulatory signal that processorside failures are independently actionable and not merely derivative of controller liability. Organisations that failed to notify the PDPC or affected individuals in a timely manner faced increased penalties, as did those operating without robust data processing agreements.

The enforcement pattern is consistent. Weak contractual frameworks, inadequate or poorly

articulated security obligations on processors, and delayed or uncoordinated breach responses are the recurring issues driving regulatory action. The practical implication is that data processing agreements are no longer a formal compliance artefact; their quality now directly affects regulatory risk exposure.

What companies in Thailand should do

The Allianz findings, read alongside the PDPC's recent enforcement record, highlight three priority areas for organisations operating in Thailand.

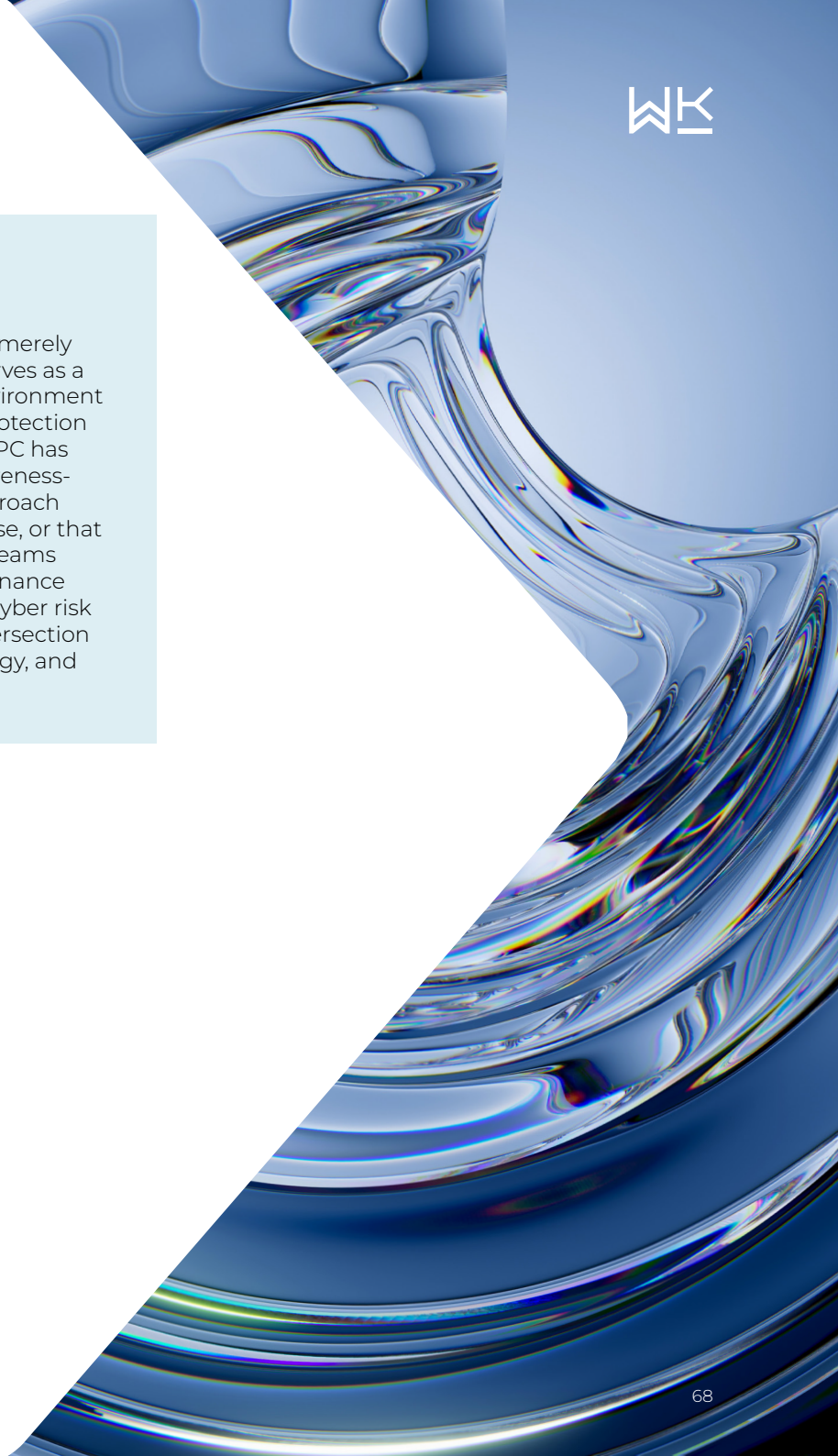
Vendor due diligence. Before engaging any service provider that processes personal data, organisations should assess the provider's security controls in substance, not merely rely on contractual warranties. This includes reviewing authentication mechanisms, access controls, breach notification procedures, and alignment with relevant security standards.

Contractual protection. Data processing agreements should extend well beyond boilerplate clauses. They should incorporate specific security standards by reference to Article 40 of the PDPA, provide audit and oversight rights, and impose clear notification obligations that enable controllers to meet their own 72-hour PDPC reporting requirements.

Incident response readiness. PDPC enforcement makes clear that postincident conduct matters. Organisations that respond promptly, coordinate remediation efforts effectively, and communicate transparently with regulators and affected individuals are materially better positioned than those that delay or underdisclose.

Looking ahead

The rise of cyber-incidents to the top of Thailand's business risk rankings is not merely a data point for risk managers but it serves as a signal that the legal and regulatory environment surrounding cyber security and data protection in Thailand is maturing rapidly. The PDPC has moved decisively beyond its initial awareness-building phase. Organisations that approach PDPA compliance as a one-time exercise, or that delegate responsibility for it to their IT teams without corresponding legal and governance frameworks are increasingly exposed. Cyber risk in Thailand now sits squarely at the intersection of technology, law, and corporate strategy, and needs to be managed accordingly.



EU, Thailand and Japan Advance Maritime Cyber Security Cooperation

The European Union, Thailand and Japan have taken further steps to strengthen maritime cyber security cooperation, hosting a regional seminar in Bangkok focused on improving the cyber resilience of global maritime supply chains. The discussions reflected growing concern about cyber risks affecting ports, vessels, navigation systems and associated digital infrastructure, and the potential for such vulnerabilities to disrupt international trade and critical sea lanes. Participants emphasised the need for coordinated incident response, improved information sharing and closer publicprivate collaboration to address increasingly sophisticated cyber threats in the maritime sector. The initiative underscores the strategic importance attached by the EU and its regional partners to cyber resilience as a core element of maritime security and supply chain stability in the IndoPacific.[79]

79. European External Action Service, 'EU-Thailand-Japan Regional Seminar Explores How to Strengthen Cyber Resilience of Maritime Supply Chains' (Press Release, 25 March 2026) <https://www.eeas.europa.eu/delegations/thailand/eu-thailand-japan-regional-seminar-explores-how-strengthen-cyber-resilience-maritime-supply-chains_en>.

Key contacts

Kieran Doyle
Partner
Sydney
+61 2 8273 9828
kieran.doyle@wottonkearney.com

Nicole Gabryk
Partner
Sydney
+61 2 9064 1811
nicole.gabryk@wottonkearney.com

Stephen Morrissey
Partner
Sydney
+61 2 8273 9817
stephen.morrissey@wottonkearney.com

Christy Mellifont
Partner
Melbourne
+61 3 9604 7921
christy.mellifont@wottonkearney.com

Lana Remedi
Partner
Sydney
+61 2 7240 2060
lana.remedi@wottonkearney.com

Leah Mooney
Brisbane
+61 7 3236 8739
leah.mooney@wottonkearney.com

Joseph Fitzgerald
Partner
Wellington
+64 27 285 5010
joseph.fitzgerald@wottonkearney.com

Pippa Austin
Special Counsel
Singapore
+65 6967 6473
pippa.austin@wottonkearney.com

Sorawat Wongkaweepairot
Partner
Bangkok
+66 2 460 7308
sorawat.wongkaweepairot@wottonkearney.com

Australia

Adelaide

Level 1, 25 Grenfell Street
Adelaide, SA 5000
+61 8 8473 8000

Brisbane

Level 21, 71 Eagle Street
Brisbane, QLD 4000
+61 7 3236 8700

Canberra

Level 6, 121 Marcus Clarke Street
Canberra, ACT 2601
+61 2 5114 2300

Hobart

Level 6, Reserve Bank
111 Macquarie Street
Hobart, TAS 7000
+61 3 6108 9000

Melbourne

Level 30, 500 Bourke Street
Melbourne, VIC 3000
+61 3 9604 7900

Perth

Level 49, 108 St Georges Terrace
Perth, WA 6000
+61 8 9222 6900

Sydney

Level 9, Grosvenor Place
225 George Street
Sydney, NSW 2000
+61 2 8273 9900

New Zealand

Auckland

Level 8, 21 Queen Street
Auckland 1010
+64 9 377 1854

Christchurch

203/237 High Street
Christchurch 8011
+64 3 667 4003

Tauranga

148 Durham Street
Tauranga 3110
+64 7 806 9600

Wellington

Level 12, 342 Lambton Quay
Wellington 6011
+64 4 499 5589

Asia

Singapore

138 Market Street
07-03, CapitaGreen
Singapore, 048946
+65 6967 6460

Thailand

990 Abdulrahim Place
Unit 1710, 17th Floor, Rama 4 Road
Silom Sub-district, Bang Rak District
Bangkok 10500
+66 2460 7301

WOTTON KEARNEY

wottonkearney.com