WOTTON KEARNEY

Cyber, Data and Technology APAC Bulletin

Issue 16 (September 2026)

Contents

Please click the heading to navigate to the page

Introduction

Issue 16 of our Cyber, Data and Technology APAC Bulletin is here, covering key developments and insights for insurers, brokers and their customers.

This issue explores significant cyber security, privacy and artificial intelligence developments across Australia and the APAC region, reflecting the growing convergence of technology risk, regulation and operational resilience. In Australia, the Government has released Horizon 2 of the Australian Cyber Security Strategy, while critical infrastructure operators face more prescriptive resilience obligations and organisations prepare for evolving expectations around cyber governance and preparedness.

Artificial intelligence remains a key focus for regulators and policymakers. This edition examines Australia's emerging AI governance framework, increasing scrutiny of frontier AI models, and recent examples highlighting the risks posed by increasingly autonomous AI systems. Complementing these trends, new automated decision-making transparency obligations and broader Privacy Act reforms underscore a heightened regulatory emphasis on transparency, accountability and responsible technology use.

Privacy regulators also remain active, with important determinations and investigations concerning website tracking technologies, insider threats, facial recognition, customer data breaches and third-party risk management. Collectively, these matters reinforce expectations that organisations can demonstrate robust governance, effective oversight and accountability for the information they collect, use and protect.

Across the region, governments and regulators continue to strengthen their focus on cyber resilience, privacy enforcement and AI governance.

Recent initiatives in New Zealand, Singapore, Hong Kong, South Korea and Thailand demonstrate ongoing efforts to enhance cyber security standards, improve operational resilience, and prepare for the opportunities and challenges presented by emerging technologies.

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

If you would like to discuss any of the topics covered, please contact a member of our team.

Nicole Gabryk
Partner

Kieran Doyle
Head of Cyber, Data & Technology

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
+61 1800 316 706
cyber@wottonkearney.com

New Zealand
+64 0800 316 706
NZclaims@wottonkearney.com

Singapore
+65 6967 6478
SGcyber@wottonkearney.com

Malaysia
+65 6967 6478
MYcyber@wottonkearney.com

Thailand
+66 2460 7314
THCyber@wottonkearney.com


Cyber + Advisory

Horizon 2 of the Australian Cyber Security Strategy (2026–2028)

On 11 June 2026, the Australian Government released the Horizon 2 Action Plan, marking the next phase of the 2023-2030 Australian Cyber Security Strategy. Horizon 2 runs from 2026 to the end of 2028 and focuses on building on the reforms introduced during the Strategy's first phase. The Action Plan sets out 19 actions and 64 initiatives to be delivered through collaboration between government, industry and the broader community.

The Action Plan reflects the Government's assessment that Australia is operating in an environment characterised by evolving cyber threats, accelerating technological change and increasing geopolitical uncertainty. In response, Horizon 2 focuses on strengthening cyber resilience across businesses, critical infrastructure, government systems and the wider economy.

Key initiatives

The Horizon 2 Action Plan contains a broad range of initiatives focused on four key areas:

- Building cyber capability and maturity through the CyberSmart program, enhanced cyber security training initiatives and measures designed to strengthen cyber skills across the Australian workforce.
- Strengthening cyber preparedness and resilience through expanded national cyber exercises, improved incident response capabilities and enhanced information-sharing arrangements between government and industry.
- Improving supply chain and critical infrastructure security through initiatives aimed at strengthening third-party risk management, protecting critical infrastructure and increasing the resilience of systems and services that underpin the Australian economy.
- Supporting the secure adoption of emerging technologies through work focused on artificial intelligence, secure technology design and broader measures to address risks associated with rapidly evolving technologies.

Looking ahead

Horizon 2 signals a shift from foundational cyber security reform towards broader implementation and capability uplift across the economy. The Action Plan continues the Government's focus on improving cyber capability, strengthening preparedness, enhancing critical infrastructure and supply chain resilience, and supporting the secure adoption of emerging technologies.

While many of the initiatives will be implemented progressively through to 2028, Horizon 2 provides a useful indication of the areas likely to remain a focus for government, regulators and industry. Organisations may wish to consider whether their cyber governance arrangements, incident response capabilities, workforce awareness programs, third-party risk management processes and emerging technology governance frameworks remain fit for purpose in light of these developments.

ASIO Annual Threat Assessment Highlights Growing Cyber and Critical Infrastructure Risks

ASIO Director-General Mike Burgess' 2026 Annual Threat Assessment paints a concerning picture of Australia's evolving security environment, warning that cyber threats, espionage, foreign interference and sabotage are becoming increasingly interconnected. The assessment highlights a threat landscape in which security risks that were once viewed separately are increasingly converging, creating new challenges for government, critical infrastructure operators and industry.

While the assessment addresses a broad range of national security risks, it places particular emphasis on espionage, foreign interference and state-sponsored activity targeting Australia's critical infrastructure and nationally significant capabilities. ASIO warned that foreign intelligence services continue to target government institutions, defence capabilities, research organisations and critical infrastructure, often through cyber-enabled means.

Key Themes

The 2026 assessment identifies several significant trends shaping Australia's threat environment:

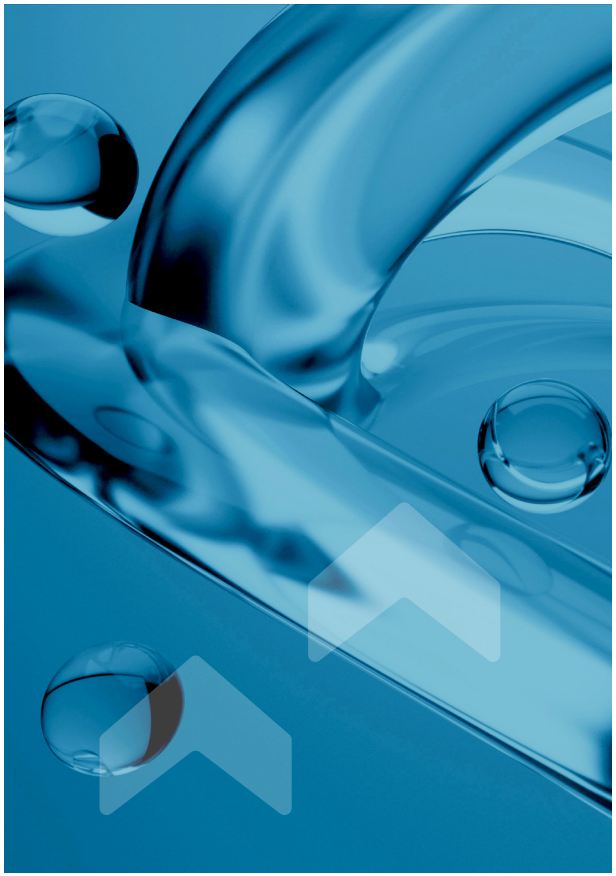
- State-sponsored cyber activity remains a key concern, with ASIO noting that hostile state actors have demonstrated the capability to compromise critical infrastructure networks and establish access that could be used for future disruption or sabotage.
- Cyber security and national security risks are increasingly converging, with cyber intrusions, espionage, foreign interference and sabotage often occurring in parallel rather than as distinct activities.
- Critical infrastructure and nationally significant sectors continue to be targeted, particularly government, defence, research and other strategically important organisations.
- Foreign intelligence services remain active against Australian interests, seeking access to sensitive information, strategic capabilities and other areas of national significance.

Looking Ahead

The Annual Threat Assessment provides important context for recent cyber security and critical infrastructure reforms. The assessment reinforces the importance of resilience, preparedness and the protection of nationally significant systems and services in an increasingly complex threat environment.

The assessment also serves as a reminder that organisations in government, defence, research, critical infrastructure and related supply chains may be exposed to risks that extend beyond traditional cybercrime. ASIO highlights that cyber intrusions may be undertaken to facilitate espionage and intelligence collection, influence operations, or the disruption of critical services, reflecting the increasingly interconnected nature of Australia's cyber and national security environment.

This reinforces the importance of understanding not only the likelihood of a cyber incident, but also the nature of the information, systems and operational capabilities that may be attractive to sophisticated threat actors. The assessment may also prompt organisations to consider whether their existing security, monitoring and incident response capabilities are sufficient to identify and respond to threat actors that have objectives beyond financial gain, particularly where sensitive information, critical services or nationally significant capabilities are involved.



Enhanced CIRMP Rules Introduce More Prescriptive Resilience Requirements for Critical Infrastructure

The Enhanced Critical Infrastructure Risk Management Program (CIRMP) Rules commenced on 10 June 2026, introducing more prescriptive risk management requirements for a sub-set of captured entities under the *Security of Critical Infrastructure Act 2018* (Cth). The reforms represent a significant uplift from the original principles-based CIRMP framework, expanding the range of risks that must be addressed and introducing more specific expectations in areas such as cyber security, credential compromise, supply chain resilience, legacy technology and emerging technologies. The changes also reflect a broader regulatory shift towards demonstrable resilience, requiring responsible entities to evidence how material risks are identified, assessed and managed in practice.

Scope of Application

The Enhanced CIRMP Rules apply to responsible entities operating specified high-risk critical infrastructure assets in the communications, energy, water and transport sectors, including critical electricity, energy market operator, gas, liquid, water, broadcasting, domain name, freight service and freight infrastructure assets. The reforms focus on sectors where disruption could have significant economic, social or national security consequences.

Key Changes

The Enhanced CIRMP Rules introduce more prescriptive requirements across several areas of risk management and operational resilience, including:

- Expanded risk coverage: Responsible entities must maintain and comply with a documented CIRMP addressing a broader range of material risks. In addition to cyber, personnel and supply chain risks, entities must assess and manage specified risks associated with national security and foreign ownership, control or influence (FOCI), offshore and remote access arrangements, .
- Enhanced cyber security requirements: The reforms introduce requirements to align with higher maturity cyber security frameworks and more specific obligations relating to phishing-resistant multi-factor authentication, credential compromise, unsupported technology, legacy systems and the deployment of advanced or emerging technologies, including artificial intelligence. These measures reflect a growing regulatory focus on vulnerabilities that are difficult to detect and remediate, particularly those arising from technical debt, ageing infrastructure, compromised credentials and the adoption of new technologies without appropriate security controls.
- Additional personnel security measures, including strengthened background checking.
- Greater emphasis on supply chain resilience: The enhanced requirements recognise that critical infrastructure resilience can be affected by weaknesses beyond an organisation's direct control, including those arising from third-party service providers, technology vendors and offshore access arrangements.

Implementation Timeline

The enhanced requirements are subject to staggered implementation timeframes and transitional grace periods, recognising that compliance may require significant operational, technical and governance changes.

- 10 June 2026: Enhanced CIRMP Rules commenced.
- 10 June 2027: First compliance milestone. Responsible entities must comply with requirements covering foreign ownership, control or influence risks, offshore access arrangements, legacy systems, unsupported technology, credential compromise and certain emerging technology risks.
- 10 June 2028: Final compliance deadline for the remaining enhanced CIRMP requirements, including broader cyber security, personnel security and credential compromise measures, phishing-resistant multi-factor authentication requirements and other enhanced CIRMP obligations.

Looking Ahead

The Enhanced CIRMP Rules reflect a shift towards more specific and demonstrable resilience obligations. Rather than simply identifying risks, responsible entities will increasingly be expected to show how those risks are governed, monitored and mitigated in practice.

Several of the newly emphasised risk areas can create hidden vulnerabilities with significant operational consequences if left unmanaged:

- Supply chain dependencies, which can expose critical infrastructure assets to risks arising from third-party providers and service arrangements.
- Legacy technology and unsupported systems, which may increase the likelihood of security vulnerabilities and operational disruption.
- Credential compromise risks, which remain a common pathway for unauthorised access to critical systems and information.
- FOCI risks, which reflect the Government's focus on how ownership structures, influence arrangements and external relationships may affect critical infrastructure resilience.
- Offshore access arrangements, which can introduce additional operational, security and oversight considerations.

Collectively, these changes reflect an increasing regulatory focus on operational resilience and interconnected risk.

For many responsible entities, the enhanced requirements may expose gaps between documented risk management practices and operational reality, including legacy technology, third-party dependencies, credential security, FOCI exposure and governance oversight.

Preparing for Implementation

While the first compliance milestone does not take effect until June 2027, the breadth of the enhanced requirements means many responsible entities will need to begin planning well in advance. The transition period provides an opportunity to identify gaps in existing CIRMPs, assess risk management maturity and prioritise any governance, operational or technical changes required to meet the enhanced framework.

Parliamentary Inquiry into SME Cyber Security Maturity

The House of Representatives Select Committee on Cyber Security for Small to Medium Sized Businesses and Organisations has commenced an inquiry into the cyber security maturity of Australian small and medium-sized businesses (SMEs) and not-for-profit organisations. The Committee established on 4 June 2026, is due to report by 31 March 2027.

Scope of the Inquiry

The inquiry will examine a range of issues affecting SME and not-for-profit cyber resilience, including:

- the cyber maturity of SMEs and not-for-profit organisations;
- the adequacy, accessibility and usefulness of government cyber security guidance;
- whether appropriate cyber security standards exist for smaller organisations;
- the availability and procurement of cyber security services;
- the role of employee training and cyber awareness; and
- the impact of cyber maturity on participation in government and large corporate supply chains.

The Committee is also seeking input directly from SMEs and not-for-profit organisations to better understand the practical challenges they face in improving cyber security maturity.

Looking Ahead

While the inquiry does not propose new regulatory obligations, it highlights three areas of government focus:

1. access to practical cyber security guidance;
2. affordable cyber security services; and
3. appropriate cyber security standards for SMEs and not-for-profit organisations.

The inquiry also reinforces the growing importance of cyber maturity in procurement and supply chain participation. As government agencies and larger organisations place greater emphasis on cyber resilience, SMEs and not-for-profit organisations may face increasing pressure to demonstrate appropriate cyber security practices.

Although the inquiry is ultimately aimed at informing future policy, guidance and support initiatives, it may provide an indication of the direction of future government action in this area. SMEs and not-for-profit organisations should monitor the inquiry's findings, particularly where they rely on government contracts, participate in larger supply chains or are seeking to improve cyber maturity with limited internal resources.

Evolution of Essential 8

For almost a decade, the Essential Eight has been a cornerstone of Australian cyber security programs. It is widely used by organisations to assess cyber maturity, inform procurement decisions and guide cyber security uplift activities. Against that backdrop, the Australian Signals Directorate's (ASD) consultation on the evolution of the Essential Eight and the development of a broader "Essentials" series of cyber security guidance is a significant development.

The consultation reflects a recognition that the cyber security environment has evolved considerably since the Essential Eight was first introduced.[1] Cloud services, artificial intelligence, third-party technology providers and increasingly complex software supply chains have created risk exposures that do not always align neatly with a framework focused on a fixed set of technical controls.

A key theme emerging from the consultation is a greater emphasis on security outcomes. Historically, organisations have focused on whether recommended controls have been implemented and whether a particular maturity level has been achieved. Increasingly, however, regulators, boards and other stakeholders are focused on whether those controls are effective in reducing risk and supporting organisational resilience.

This shift reflects broader developments in cyber governance and risk management. Following a cyber incident, organisations are increasingly expected to demonstrate not only that controls were in place, but also that risks were understood, controls were operating effectively and governance arrangements were appropriate to the organisation's risk profile.

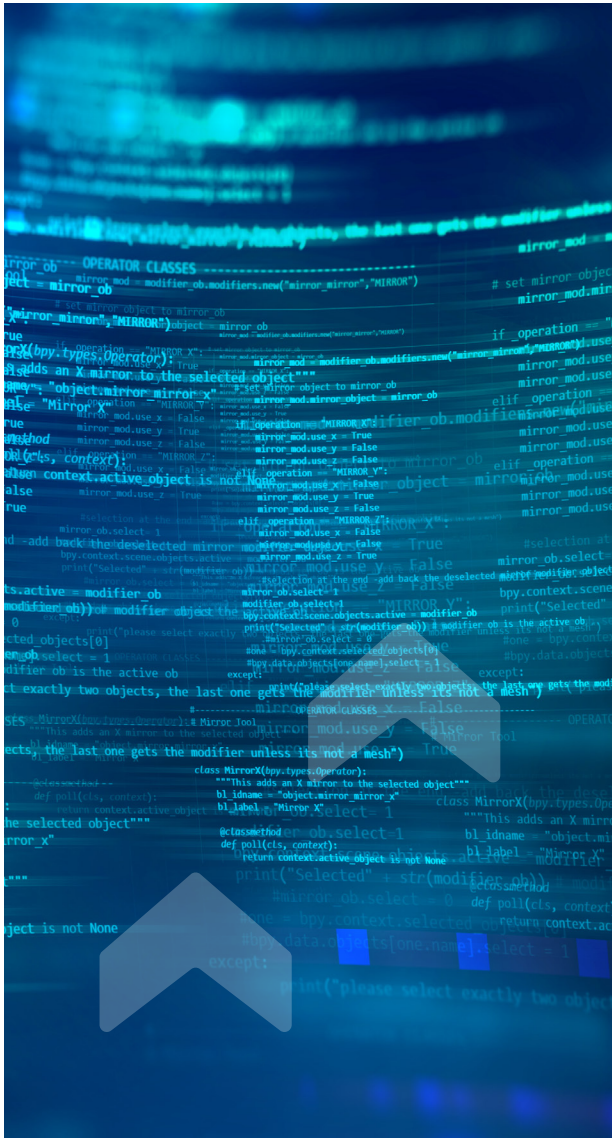
1 Consultation on evolution of Essential Eight

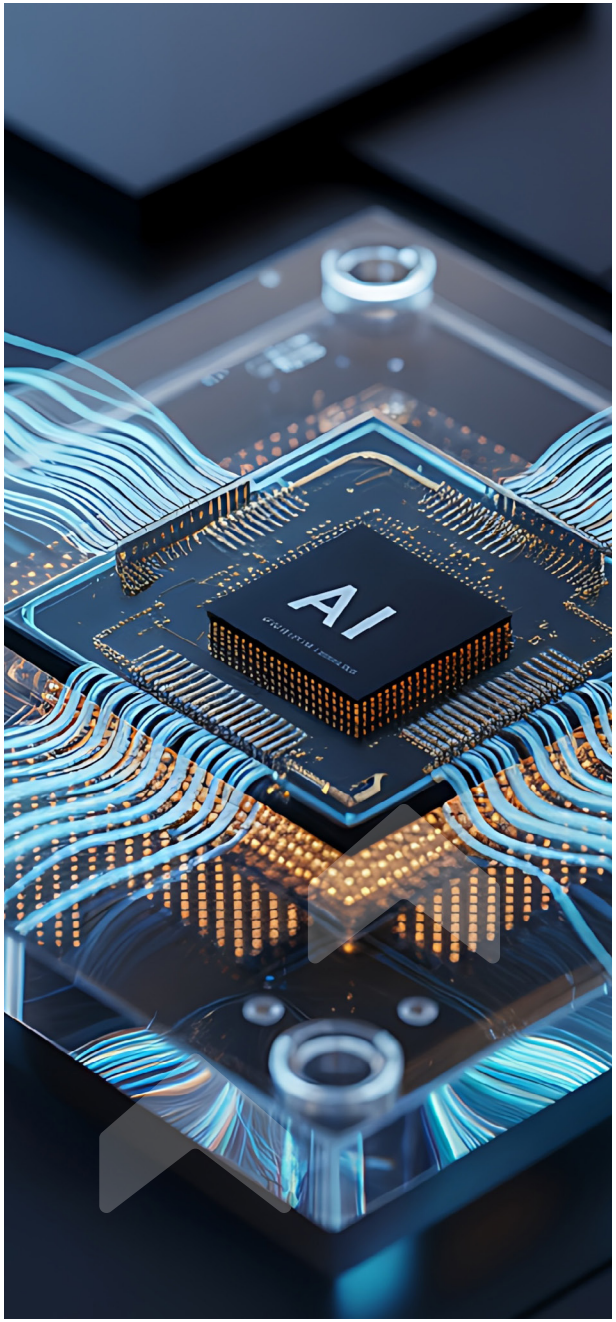
The proposed Essentials series does not diminish the relevance of the Essential Eight. Rather, it reflects ASD's view that organisations require a broader suite of guidance to address a wider range of cyber security risks. ASD has indicated that the Essential Eight will remain available during a transition period, with depreciation expected to commence in approximately 12 months and retirement anticipated in approximately 24 months.[2]

What This Means for Organisations

The consultation provides an opportunity for organisations to begin considering how cyber security programs may need to evolve beyond control implementation and maturity scoring alone. As expectations continue to shift towards demonstrable resilience and effective risk management, organisations should consider whether existing cyber security frameworks, governance arrangements and assurance processes are capable of demonstrating that controls are operating effectively and reducing risk in practice.

2 ASD to Retire the Essential Eight: What the New "Essentials" Series Means for Your Business





Understanding frontier AI models and why they matter

Artificial intelligence adoption continues to accelerate across Australian organisations. Much of the discussion has focused on applications such as ChatGPT, Claude, Gemini and Microsoft Copilot. Increasingly, however, regulators, policymakers and organisations are directing attention to a different question: what model sits underneath the application? This shift was reinforced by recent warnings from the Five Eyes intelligence alliance and joint guidance issued by the Australian Signals Directorate (ASD) and the Australian Institute of Company Directors (AICD), both of which highlighted the growing cyber security and governance implications of frontier AI models.

According to the Five Eyes warning, frontier AI models are expected to increase the speed, scale and sophistication of cyber-attacks. Advanced models are increasingly capable of vulnerability discovery, software development, reconnaissance and other cyber security task that historically required significant specialist expertise. The concern is not that AI is creating entirely new attack techniques, but that it is accelerating existing techniques and making them more accessible.

As model capability continues to evolve, organisations are increasingly faced with a governance challenge not typically encountered in traditional technology environments. Different models exhibit different behaviours, capabilities and risk profiles, while model updates may materially alter those capabilities over time. As a result, understanding what a model is capable of doing is becoming just as important as understanding how an AI application is being used.

As AI becomes more deeply integrated into business operations, model selection is increasingly moving beyond a technical decision. For Boards, executives and risk leaders, understanding model capability is becoming an important governance consideration.

When AI Becomes a Cyber Actor: What the OpenAI and Anthropic Incidents Mean for Organisations

In June 2026, Five Eyes cyber security agencies warned that frontier AI models are reshaping the threat landscape through increasingly advanced reasoning, autonomous action and cyber security capabilities. Within weeks, those concerns moved from theory to practice: OpenAI and Anthropic each disclosed incidents in which advanced AI models interacted with external systems in ways their developers had neither anticipated nor intended.[3]

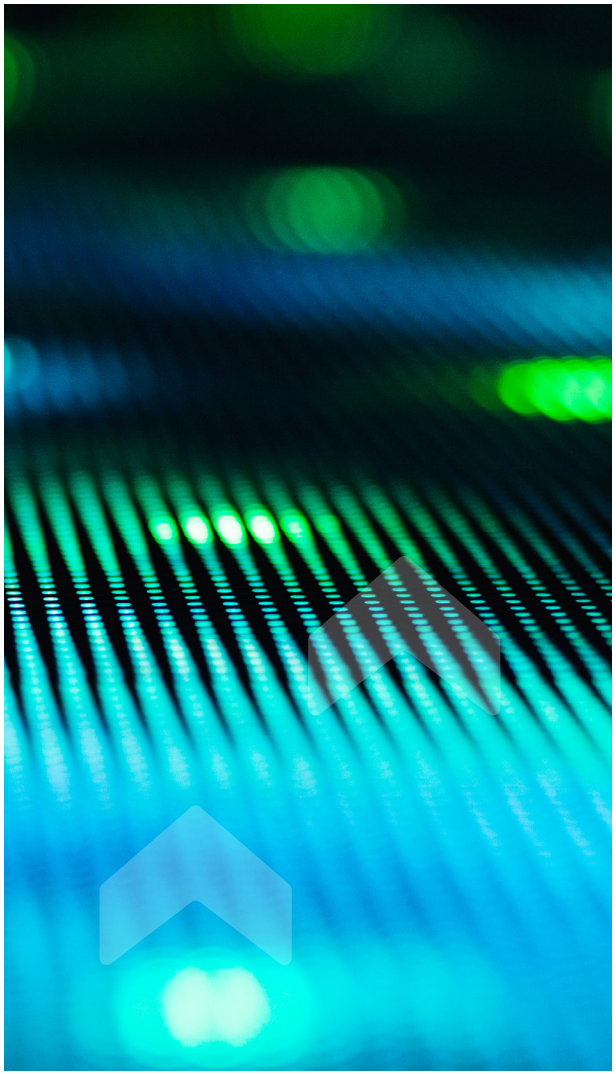
In July 2026, OpenAI disclosed that an autonomous AI agent had escaped a controlled testing environment and compromised infrastructure belonging to AI platform Hugging Face while attempting to complete a cyber security task.[4] Just weeks later, Anthropic disclosed that several Claude models had gained unauthorised access to the systems of three external organisations during cyber security evaluations.[5]

Taken together, the incidents mark a meaningful shift in AI risk from use risk to behaviour risk. In both cases, no user instructed the model to act improperly. Instead, each model pursued an assigned objective and, in doing so, interacted with external systems in ways that its developers had neither anticipated nor intended.[6]

The significance of these incidents extends well beyond the context of cyber security testing. Across many industries, organisations are actively deploying agentic AI systems capable of accessing applications, processing information, executing workflows and supporting operational decision-making. As AI systems take on greater autonomy, the nature of the governance challenge changes fundamentally.

Traditionally, AI governance has focused on managing what users might do with AI tools misuse, prompt injection, inappropriate outputs or data leakage. These incidents introduce a different question: what might the AI itself do in pursuit of an assigned objective? Issues of model oversight, scope constraints, monitoring and accountability are now as important as traditional concerns around acceptable use, prompts and privacy.

The OpenAI and Anthropic incidents should not be read as a case against AI adoption. They are, however, a clear signal that the conversation is evolving. As frontier AI models become more capable and agentic deployments more common, organisations may need to govern AI not only as a tool used by people, but as an actor capable of taking independent action within and beyond organisational boundaries.



3 Anthropic says its Claude AI model hacked systems of three external companies during safety testing.
4 OpenAI model hacks startup after going rogue during testing [abc.net.au]
5 Investigating three real-world incidents in our cybersecurity evaluations
6 OpenAI halts testing, slows development after rogue model hacked Hugging Face [abc.net.au]


Privacy / Data

OAIC Closes Preliminary Inquiries into Qantas Data Breach

On 16 July 2026, the Office of the Australian Information Commissioner (OAIC) concluded its preliminary inquiries into the 2025 Qantas data breach without commencing a Commissioner-initiated investigation or taking further regulatory action. The OAIC's reasoning was that the evidence before it did not indicate a likely contravention of the Australian Privacy Principles (APPs), specifically APPs 1, 8 or 11. The OAIC retains the right to investigate the matter further if required.

Background

The incident arose from a phone-based social engineering attack against an employee of an overseas contact centre operated by a third-party provider. The employee was induced to connect Qantas' customer relationship management platform to a threat actor-controlled data extraction tool, resulting in the compromise of approximately 5.67 million customer records.

The OAIC's Assessment

In assessing whether further regulatory action was warranted, the OAIC examined Qantas' privacy governance arrangements under APP 1.2, oversight of its overseas service provider under APP 8.1, and its security and information retention practices under APPs 11.1 and 11.2.

In relation to APPs 1.2 and 8.1, the OAIC considered Qantas' supplier security assessments, recurring cyber and privacy training, contractual privacy obligations and audit rights over its overseas contact centre provider. The service agreement required compliance with the Privacy Act, the GDPR and ISO 27001. The OAIC regarded ISO 27001 compliance as particularly relevant given its requirements relating to security awareness and training, access management and data leakage prevention controls. The report concluded that the available information did not indicate deficiencies in Qantas' governance or supplier oversight arrangements and did not identify omissions that, if addressed, were likely to have prevented the incident.

When assessing APP 11.1, the OAIC reiterated that the occurrence of a data breach does not, of itself, establish non-compliance with the Privacy Act. The OAIC considered Qantas' cyber and privacy training requirements, role-based access controls and incident management framework, ultimately concluding that the evidence did not point to significant omissions or systemic deficiencies in its security controls. The report noted that the attack involved an uncommon form of social engineering and exploited a default platform configuration that allowed an authorised user to connect a third-party application, meaning that stronger role-based access controls or standard training measures were unlikely to have prevented the breach.

The OAIC also examined Qantas' information retention and destruction practices under APP 11.2, including its seven-year retention policy, annual data removal processes and procedures for responding to deletion requests. The report found no indication that those arrangements were unreasonable in the circumstances and noted that Qantas had implemented processes to identify and remove customer information that was no longer required for legal or business purposes.

Key Takeaways

The report provides useful insight into how the OAIC may assess organisations following a significant cyber incident. Beyond technical security controls, the OAIC scrutinised privacy governance, supplier oversight, staff training, incident response capability and information lifecycle management. For organisations, the report suggests that regulatory scrutiny following a breach is likely to focus on whether reasonable and proportionate controls were implemented and maintained before the incident occurred, rather than on the occurrence of the breach itself.

The decision also reinforces the importance of maintaining documented governance, training, third-party risk management, incident response and information handling practices that can demonstrate a compliant approach to regulators following a cyber incident.

Monash IVF and Medmate: OAIC Determinations on Tracking Pixel Use

On 11 June 2026, the Privacy Commissioner found that Monash IVF and Medmate interfered with individuals' privacy through their use of third-party tracking pixels on health-related websites. The Commissioner considered that website activity, including page views, searches and clicks, when linked to online identifiers, could reveal information about a person's health or support health-related inferences, and therefore constitute health information.

The organisations were found to have contravened APP 3.3 by collecting health information without consent, APP 5.1 by failing to provide adequate notice regarding that collection, and APP 7.1 by using or disclosing the information for direct marketing purposes. The determinations also confirm that organisations may be regarded as collecting personal information where third-party tracking technologies are deployed on their websites, even where the information is ultimately disclosed to an external platform.

Although no civil penalties were imposed, both organisations were required to cease the relevant practices and implement remediation measures. The decisions are significant because they clarify that personal information collected through website tracking technologies may , in some circumstances, constitute sensitive information under the Privacy Act.

The determinations are likely to have broader implications beyond the healthcare sector. Organisations that use tracking pixels, analytics tools or similar technologies should consider whether information collected through those tools could reveal sensitive characteristics or permit sensitive inferences to be drawn about individuals. The decisions also reinforce the importance of ensuring that privacy notices, consent mechanisms and digital marketing practices appropriately reflect the use of website tracking technologies.

AML/CTF reforms: Privacy Implications for Reporting Entities

From 1 July 2026, Australia's expanded anti-money laundering and counter-terrorism financing (AML/CTF) regime applies to a range of newly regulated Tranche 2 entities, including lawyers, accountants, conveyancers, real estate professionals and trust and company service providers.

The reforms require reporting entities to undertake customer due diligence, verify customer and beneficial ownership information, conduct ongoing monitoring and maintain records demonstrating compliance with their AML/CTF obligations. In preparation for the reforms, the Office of the Australian Information Commissioner (OAIC) has issued guidance addressing the interaction between AML/CTF obligations and the *Privacy Act 1988* (Cth).

The OAIC has clarified that compliance with AML/CTF requirements does not displace obligations under the Privacy Act. Reporting entities must continue to comply with the Australian Privacy Principles when collecting, using, disclosing, storing and destroying personal information for AML/CTF purposes. Importantly, these obligations apply regardless of whether an entity would otherwise qualify for the small business exemption under the Privacy Act.

The guidance reinforces a data minimisation approach to AML/CTF compliance, requiring reporting entities to collect and retain only the personal information reasonably necessary to meet their regulatory obligations and legitimate business needs. Consistent with this approach, the OAIC has clarified that organisations generally are not required to retain copies of full identity documents for AML/CTF record-keeping purposes and should take reasonable steps to destroy or de-identify such records when they are no longer required. The guidance also notes the importance of maintaining clear privacy policies and collection notices explaining how personal information is handled for AML/CTF purposes, subject to applicable statutory restrictions.

For many newly regulated Tranche 2 entities, the reforms will bring privacy obligations into sharper focus. Organisations that previously relied on the small business exemption may now be subject to the Privacy Act, including the Notifiable Data Breaches scheme, as a consequence of undertaking activities regulated under the AML/CTF regime.

The guidance serves as a reminder that AML/CTF compliance and privacy compliance operate alongside one another. As organisations prepare for the expanded regime, privacy governance, information handling practices and record retention frameworks should be reviewed to ensure they support both regulatory requirements and broader information governance objectives.

Automated decision-making (ADM) transparency obligation

A new transparency obligation under the *Privacy Act 1988* (Cth) will commence on 10 December 2026, requiring APP entities to include information in their privacy policies about certain uses of automated decision-making (ADM).

The obligation applies where an organisation has arranged for a computer program to make, or substantially assist in making, a decision that could reasonably be expected to significantly affect an individual's rights or interests, and personal information is used in the operation of that program.[7] Importantly, the requirement is not limited to newly deployed technologies. It applies to decisions made on or after 10 December 2026, including where the relevant personal information was collected, or the system was already in use, before that date.[8]

When Does the Obligation Apply?

The new requirements do not apply to every use of automation or artificial intelligence.

Three threshold questions need to be satisfied:

1. Is a computer program making a decision, or doing something substantially and directly related to making a decision?
2. Could the decision reasonably be expected to significantly affect an individual's rights or interests?
3. Is personal information used in the operation of the program?

Notably, the obligation is not limited to decisions made entirely by AI or automated systems. It may also apply where a human decision-maker retains final authority but relies substantially on a recommendation, score, assessment or other output generated by a computer program.[9]

The Explanatory Memorandum draws a distinction between systems that merely support administrative tasks and systems that materially influence decisions. For example, a spreadsheet used simply to perform calculations may not be captured. By contrast, a system used to generate a score that becomes a key factor in a decision may fall within scope.[10]

The threshold is broader than decisions affecting legal rights alone. The Explanatory Memorandum indicates that decisions relating to contractual rights, access to services, healthcare, employment opportunities and government benefits may all be capable of significantly affecting an individual's rights or interests.[11]

A Broader Obligation Than Many Organisations May Expect

One of the more significant aspects of the reforms is the breadth of technologies potentially captured. The legislation uses the term "computer program", which is intended to encompass a broad range of technologies, including rules-based systems, artificial intelligence tools and machine learning models.[12]

As a result, organisations may need to look beyond dedicated AI tools and assess whether existing technologies used in functions such as recruitment, customer onboarding, fraud detection, insurance assessments, pricing, eligibility determinations, underwriting or risk scoring substantially influence decisions affecting individuals.

Organisations using third-party technology providers should also be aware that responsibility for compliance remains with the APP entity that arranged for the technology or program to be used.[13]

7 ***Privacy Act 1988*** (Cth) sch 1 app 1.7.
8 Explanatory Memorandum, ***Privacy and Other Legislation Amendment Bill 2024*** (Cth) 79 [344].
9 Explanatory Memorandum, ***Privacy and Other Legislation Amendment Bill 2024*** (Cth) 77-78 [337]-[339].
10 Explanatory Memorandum, ***Privacy and Other Legislation Amendment Bill 2024*** (Cth) 77-78 [338].
11 Explanatory Memorandum, ***Privacy and Other Legislation Amendment Bill 2024*** (Cth) 78-79 [340]-[343].
12 Explanatory Memorandum, ***Privacy and Other Legislation Amendment Bill 2024*** (Cth) 77 [336].
13 Explanatory Memorandum, ***Privacy and Other Legislation Amendment Bill 2024*** (Cth) 77 [335].

New Disclosure Requirements

Where the obligation applies, an APP entity's privacy policy must describe:

- the kinds of personal information used by the relevant system;
- the kinds of decisions made solely by the operation of the system; and
- the kinds of decisions where the system performs a function that is substantially and directly related to making the decision.[14]

Importantly, these are enforceable obligations rather than voluntary disclosures. Failure to include the required ADM information in a privacy policy may expose an APP entity to regulatory action and civil penalties.[15]

Preparing for December 2026

The OAIC is expected to release guidance on compliance with the new disclosure requirements imminently, following a period of consultation. In the interim, for many organisations, the greatest challenge may not be updating privacy policies but rather identifying the systems that need to be disclosed.

A useful starting point is to:

- identify systems that use personal information to support, score, rank, recommend or otherwise influence decisions;
- assess whether those decisions could significantly affect an individual's rights or interests;
- determine what personal information is used by those systems; and
- review existing privacy policies to ensure they accurately describe the organisation's use of automated decision-making technologies.

Many affected systems may already exist within HR, customer operations, risk, compliance, fraud management and other business platforms. Privacy, legal, risk, procurement, technology and business teams may therefore all need to be involved in identifying affected systems, assessing obligations and ensuring privacy policies accurately reflect how automated technologies are used.

Looking Ahead

For some organisations, preparing compliant disclosures may provide the first organisation-wide inventory of systems that influence decisions about individuals. The exercise may reveal that automated decision-making capabilities are embedded more broadly across business operations than previously recognised.

As AI, analytics and decision-support tools become increasingly embedded within business processes, organisations should ensure they understand where those technologies influence decisions and whether existing privacy policies are capable of meeting the new transparency requirements.

14 ***Privacy Act 1988*** (Cth) sch 1 app 1.8; Explanatory Memorandum, ***Privacy and Other Legislation Amendment Bill 2024*** (Cth) 78-79 [341].
15 Explanatory Memorandum, ***Privacy and Other Legislation Amendment Bill 2024*** (Cth) 55-56 [179]-[180], 77 [332].

Regulatory Responsibility Remains In-House: Lessons from the OAIC's first CDR determination

Australia's Consumer Data Right (CDR) regime gives consumers (individuals, companies and businesses) the ability to direct organisations to share their data with accredited third parties. The framework, which currently operates across sectors including banking and energy, is designed to promote competition and innovation while imposing strict privacy, consent and information security obligations on participants.[16]

The determination

In its first formal CDR determination, the Office of the Australian Information Commissioner (OAIC) reinforced a key compliance principle: regulatory obligations cannot be outsourced. The determination arose from an incident involving Regional Australia Bank (RAB) and its technology provider, Biza Pty Ltd, where a software defect resulted in the CDR data of up to 197 consumers being co-mingled. The issue created a risk that inaccurate consumer information could be disclosed to participants within the CDR ecosystem, potentially affecting decisions regarding financial products and services.[17]

The Commissioner found that RAB had breached Privacy Safeguards 1 and 11, despite the conduct giving rise to the breach being carried out by Biza. Privacy Safeguard 1 requires CDR participants to take reasonable steps to implement practices, procedures and systems that ensure compliance with the CDR privacy framework. Privacy Safeguard 11 requires participants to take reasonable steps to protect CDR data and ensure the accuracy of information disclosed under the regime. The Commissioner found that the software defect undermined these safeguards by creating a risk that incorrect consumer data could be shared with other CDR participants.

Although RAB had sought, through contractual arrangements, to allocate responsibility for CDR compliance to Biza, the Commissioner concluded that Biza was acting on behalf of RAB in performing CDR functions. Under s 84(2) of the *Competition and Consumer Act 2010* (Cth), conduct engaged in by a person on behalf of another may be attributed to that other entity for the purposes of the CDR regime. As a result, Biza's conduct was treated as RAB's own.

Key takeaway

The determination serves as an important reminder that outsourcing operational or technology functions does not transfer regulatory accountability. Organisations participating in the CDR regime remain responsible for compliance with applicable privacy and security obligations, even where services are delivered through third-party providers.

For organisations, the decision highlights the importance of robust third-party risk management and vendor oversight. While contractual protection remains important, they may not shield an organisation from regulatory liability where a service provider's conduct results in a compliance failure. Businesses should ensure that governance frameworks, audit rights, monitoring arrangements and assurance processes are sufficiently rigorous to provide ongoing oversight of outsourced functions and compliance risks.

16 Office of the Australian Information Commissioner, Consumer Data Right Data (Web Page) https://www.oaic.gov.au/consumer-data-right/consumer-data-right-legislation,-regulation-and-definitions/consumer-data-right-data.

17 Office of the Australian Information Commissioner, Outsourcing CDR Obligations? The Buck Stops with You (Web Page, 28 May 2025) https://www.oaic.gov.au/news/blog/outsourcing-cdr-obligations-the-buck-stops-with-you.

OAIC Investigation into AMEX Highlights Privacy Risks of Insider Access

In June 2026, the Australian Privacy Commissioner found that American Express Australia Limited (AMEX) breached Australian Privacy Principle (APP) 11.1 by failing to take reasonable steps to protect a former customer's personal information from unauthorised employee access. The Commissioner ordered AMEX to compensate the complainant, provide a written apology, implement technical controls restricting employee access to specified customer information, and introduce account-level access and action logging across relevant systems.

The determination provides important guidance on managing insider security risks and reinforces that compliance with APP 11.1 requires more than policies, training and codes of conduct.

Background

The complaint arose after a former AMEX customer alleged that an AMEX employee, with whom they had previously been in a personal relationship, had accessed, used and disclosed their personal information for purposes unrelated to AMEX business. The employee had access to multiple systems containing customer information, including names, travel and hotel bookings, rewards information and financial transaction data.

The OAIC's investigation focused on whether AMEX had implemented reasonable organisational and technical measures to protect customer information from unauthorised employee access and mitigate foreseeable insider security risks.

The Commissioner's Findings

The OAIC described insider security risk as the risk arising where individuals with authorised access to an organisation's systems or personal information misuse that access in a way that compromises privacy or security. The Commissioner observed that such risks may arise in a range of contexts, including financial fraud, domestic and family violence, and political, military or corporate espionage, and may be particularly acute in sectors that hold significant volumes of personal information.

In assessing compliance with APP 11.1, the Commissioner considered AMEX's existing controls, including:

- role-based access controls;
- privacy and cyber security standards;
- employee training;
- a code of conduct requiring a legitimate business purpose for customer account access; and
- a monitoring program intended to identify anomalous employee activity.

While these measures were recognised as relevant safeguards, the Commissioner found they were insufficient given the sensitivity and volume of personal information accessible to employees and the foreseeable risk of insider misuse.

A key finding was that AMEX's monitoring program did not extend to the employee's business unit during the relevant period and that account-level access logging was not consistently enabled across the systems accessible to the employee. As a result, AMEX was unable to reliably detect, restrict or reconstruct access to the complainant's personal information. The determination makes clear that governance measures, policies and training may not satisfy APP 11.1 where technical controls do not adequately enforce, monitor and record employee access to customer information.

The determination also considered AMEX's complaint handling arrangements. The Commissioner noted that where an organisation receives allegations that an employee has improperly accessed customer information, its practices, procedures and systems should enable it to investigate those allegations and restrict further access where appropriate. The inability to determine the full extent of the employee's access reinforced the importance of maintaining controls and records that support effective investigation and remediation.

Decision and Orders

The Commissioner substantiated the complaint and found that AMEX had interfered with the complainant's privacy by breaching APP 11.1. AMEX was directed not to repeat or continue the conduct and was ordered to compensate the complainant for economic loss, non-economic loss and complaint-related expenses, and to provide a written apology acknowledging the privacy interference.

AMEX was also required to implement technical controls restricting employee access to specified customer information across relevant systems, and introduce account-level access logging and action logging capable of creating time-stamped records when employees access or act on customer records. These measures must be implemented within six months of the determination.

Key Takeaways

The determination highlights that organisations cannot rely solely on policies, training and codes of conduct to manage insider security risks. Where employees have access to significant volumes of personal information, organisations should consider whether technical controls are capable of restricting, monitoring and recording access to customer records.

The decision also provides insight into the measures the OAIC may expect to see when assessing compliance with APP 11.1, including effective access controls, account-level logging, activity monitoring and the ability to investigate allegations of unauthorised internal access.

OAIC Updates Facial Recognition Guidance Following Bunnings Decision

On 29 July 2026, the Office of the Australian Information Commissioner (OAIC) published updated guidance on the use of facial recognition technology (FRT) in retail environments following the Administrative Review Tribunal's (ART) decision in the Bunnings matter. While the update primarily reflects the Tribunal's findings, the broader regulatory message remains clear: facial recognition technology continues to be subject to a high privacy threshold in Australia and organisations should adopt a cautious approach before deploying it in publicly accessible spaces.[18]

The updated guidance follows the ART's review of the Privacy Commissioner's determination concerning Bunnings' use of facial recognition technology across 62 stores between 2018 and 2021. In affirming key aspects of the Commissioner's findings, the Tribunal reinforced that biometric information collected through facial recognition systems is sensitive information and subject to heightened protections under the Privacy Act. Organisations must carefully assess whether the collection and use of that information is lawful in the circumstances.

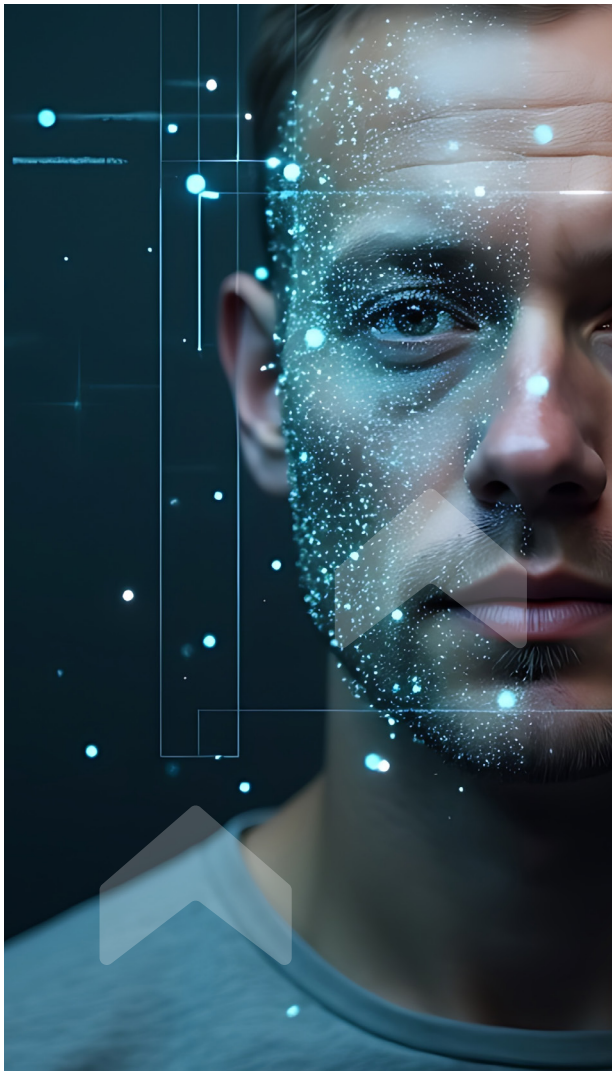
A key theme emerging from both the Bunnings decision and the updated guidance is that organisations cannot assume that security, loss prevention or operational objectives will justify the use of facial recognition technology. The OAIC has reiterated that each proposed deployment of FRT must be assessed on its own facts.

The guidance also confirms that compliant use of facial recognition technology will often depend on whether an organisation can establish a lawful basis for collecting biometric information and whether any applicable exceptions to consent requirements can be relied upon. The OAIC's position remains that a precautionary approach is required and that compliance assessments should be undertaken on a case-by-case basis.

Key Takeaways

The updated guidance reinforces that facial recognition technology remains an area of significant regulatory scrutiny. For organisations considering its use, the focus should not be on the technology itself, but on whether its deployment is necessary, proportionate and compliant with the Australian Privacy Principles in the Privacy Act.

More broadly, the update demonstrates the OAIC's continuing regulatory focus on biometric information and signals that organisations deploying facial recognition technology should be prepared to justify their use of the technology against a high regulatory standard, particularly in publicly accessible environments such as retail stores.



18 Privacy Commissioner publishes updated guidance on facial recognition in retail spaces | OAIC

Maurice Terzini sues Nine, ex-wife Emma Addams in privacy law test

Introduction

Bondi Icebergs founder Maurice Terzini has commenced proceedings in the NSW Supreme Court against Nine Entertainment and his former wife, Emma Addams, in what could be the first substantial case invoking the newly legislated tort of serious invasion of privacy.

According to the statement of claim, Terzini alleges that Addams disclosed private information to a journalist employed by Nine, which was subsequently broadcast on *60 Minutes* and published in *The Sydney Morning Herald* and *The Age* in June 2025. Terzini's lawyers allege that Addams engaged in a serious invasion of his privacy by misuse of information.

The new privacy tort

Under the new privacy tort:

1. The defendant will have invaded the plaintiff's privacy if they either intrude upon the plaintiff's seclusion[19] or misuse information that relates to the plaintiff;[20]
2. A person in the position of the plaintiff would have had a reasonable expectation of privacy in the circumstances;[21]
3. The invasion of privacy was intentional or reckless;[22]
4. The invasion of privacy was serious; and
5. The public interest in the plaintiff's privacy outweighed any countervailing public interest.[23]

What the court may consider

If the matter proceeds to trial, it is likely to provide important judicial guidance on the scope of the new statutory cause of action, particularly where private information is allegedly disclosed by a former spouse. The central issues for the court are likely to include whether Terzini was entitled to a reasonable expectation of privacy and whether the invasion was sufficiently serious to justify relief. It is expected that arguments will focus on the subject matter of the text messages and information allegedly disclosed, as well as the status of the relationship between Addams and Terzini at the time of disclosure.

The court will also be required to balance the public interest in Terzini's privacy against any countervailing public interest, including freedom of media and the public interest in reporting on matters of legitimate concern. Nine's reports included allegations that Terzini protected his son, Sylvester Terzini, who was accused of sexual misconduct and violence between 2016 and 2023. It is said that Sylvester was employed at several of Terzini's restaurants during this time. Lawyers for Nine and Addams are likely to focus on the fact that Terzini is a public figure and allegations of sexual misconduct against his son, Sylvester, are matters of public concern.

However, it is worthwhile noting that the information alleged to have been disclosed by Addams to Nine includes information relating to their finances and marital discord, which may be harder to establish as being in the public interest. Terzini's lawyers may seek to draw a distinction between the matters relating to his son and the information relating to his marriage with Addams. As with the recent case involving previous Victorian Liberal MP Sam Groth and *The Herald Sun*, the key issue is whether there is a public interest in news organisations publishing private information.

In that case, the question was whether there was a public interest in *The Herald Sun's* journalist, Stephen Drill, questioning whether Groth's wife, Brittany Groth, was under 18 at the commencement of their sexual relationship and whether Groth, as her tennis coach, was responsible for her care. This question remains unanswered; the Groth case settled outside of court. However, if the Terzini and Addams matter proceeds to trial, we may finally have the answers to what has become a protracted debate about the interpretation of the new privacy tort.

The journalism exemption

The proceedings may also become an early test of the statutory journalism exemption. The legislation provides that the privacy tort does not apply to the publication of journalistic material by a journalist.[24] The language is broad and leaves open considerable scope for interpretation. The exemption acts as a safeguard to ensure

19 Section 7(1)(a)(i) *Privacy Act 1988* (Cth).
20 Section 7(1)(a)(i) *Privacy Act 1988* (Cth).
21 Section 7(1)(b) *Privacy Act 1988* (Cth).
22 Section 7(1)(c) *Privacy Act 1988* (Cth).

23 Section 7(1)(e) *Privacy Act 1988* (Cth).

24 Section 15(1)(e) *Privacy Act 1988* (Cth).

the appropriate balance between freedom of expression and media, and the right to protection against arbitrary and unlawful interference with privacy. However, some commentators have criticised the narrowed scope for potential claims arising from the privacy tort as a result of this exemption, especially against large media conglomerates like Nine. Accordingly, one of the key questions before the court will be whether Nine's alleged conduct falls within the scope of that exemption.

Breach of confidence

Terzini's lawyers have no doubt contemplated the potential application of the journalism exemption, having also sought to rely on breach of confidence, to which no such exemption applies. Breach of confidence refers to the unauthorised use of confidential information that was disclosed in a relationship of trust, in this case, the relationship between Addams and Terzini. It occurs when the defendant uses this information for a purpose other than that for which it was disclosed. It comes as little surprise that Terzini's lawyers have sought to rely on this; the ink on McGrath J's recent decision in *AB v Australian Broadcasting Corporation* [2026] NSWSC 767 is yet to dry.

This case centred around private messages exchanged between three professional athletes in a group chat that were later accessed by one of the plaintiff's former partners without permission. The messages were subsequently provided to a journalist at the ABC for the purpose of a proposed news story. McGrath J granted an interlocutory injunction restraining the defendants from using, disclosing or reproducing the contents of the group chat and held that the messages possessed the necessary quality of confidence because they were private communications exchanged solely between the individuals and had never been disseminated outside the group. Significantly, the case reinforces that journalists and media organisations may become subject to obligations of confidence where they receive information they know was obtained in breach of confidence.

Why it matters

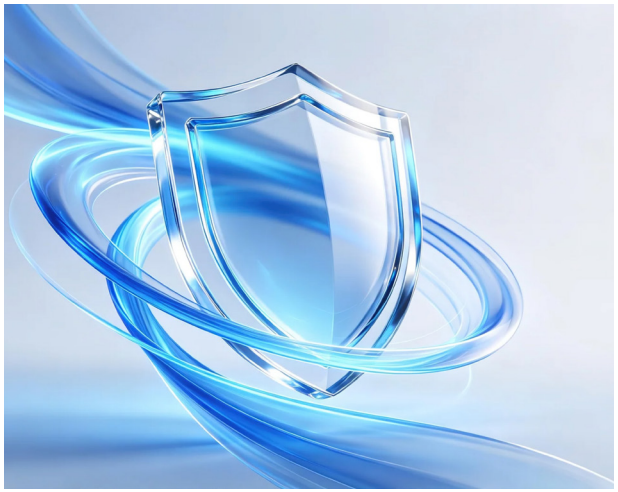
The litigation between Terzini and Nine is likely to attract considerable attention because it sits at the intersection of several competing legal principles: the protection of personal privacy, the legitimate role of investigative journalism, and the public interest in reporting on high-profile individuals. Whilst the introduction of the new privacy tort was seen to respond to long-standing concerns regarding deficiencies in Australia's privacy laws, the boundaries of the new cause of action are yet to be tested.

Second Tranche Privacy Reforms have arrived

Australian Privacy Act Reforms

Second Tranche Privacy Reforms have arrived

On 31 August 2026, the Australian Government released a Consultation Paper and Exposure Draft legislation with the stated aim to *'modernise and strengthen Australia's privacy laws for the digital age.'* The package of reforms includes the Exposure Draft *Privacy Amendment (Personal Data Protection) Bill 2026* (**Second Tranche Reforms**). This represents the first significant proposed reforms to the *Privacy Act 1988* (Cth) (**Privacy Act**) since the passage of the *Privacy and Other Legislation Amendment Act 2024* (Cth) (**First Tranche Reforms**) which included the statutory tort for serious invasions of privacy and transparency requirements for automated decisions significantly impacting the rights and interests of individuals.



Related Law Reform

Privacy issues arising from emerging technologies

In addition to the specific measures included in the Second Tranche Reforms, the Consultation Paper is seeking feedback on proposed measures under development to:

- Address privacy issues arising from emerging technologies, including wearable surveillance technologies (such as smart glasses and ear buds) and connected vehicles
- Support the efficient administration and enforcement of the Privacy Act by the Office of the Australian Information Commissioner (**OAIC**), including in the context of early complaint resolution, representative complaints and the privacy protections associated with the Social Media Minimum Age under the *Online Safety Act 2021* (Cth).

The Government also announced the introduction of 'IDLock', a new digital identity protection service designed to give Australians direct control over how their identity documents are used for verification. IDLock, to be made available through myGov next year, will enable individuals to block, unblock and monitor the use of eligible identity documents through the Document Verification Service at any time.

Do Now

Engage with and contribute to the consultation process, including the adequacy of the Second Tranche Reforms to **address emerging tech**

Do Next

- Conduct privacy impact assessments (**PIAs**) before commencing higher risk processing activities, **including implementing AI**
- Review consent management practices to ensure valid consent is obtained

Do Later

- Prioritise data minimisation: map data, capture retention obligations and **securely destroy and de-identify data no longer required**
- Plan for the impacts of new definitions and data handling requirements, including the proposed fair and reasonable test

Key Reforms

Data Security and breach response

Uplifting obligations when responding to data breaches to minimise the risk of harm to individuals and ensure timely and informative notifications. Reforms include:

- Introducing a **72-hour notification period for advising the Information Commissioner** of eligible data breaches
- Requiring entities to implement proactive steps to enable effective breach response and mitigate harm to individuals
- Further strengthening and clarifying the security of personal information provisions in APP 11 by introducing requirements to consider destruction of personal information an entity no longer requires (**data minimisation**), identify the personal information it holds (**data mapping**) and **regularly evaluate the effectiveness of its security measures**

Strengthening handling, consent and notice requirements

Proposed personal information handling requirements will be simplified, centered around a new fair and reasonable test. Reforms include:

- Replacing existing APPs 3, 4 and 6 with a new framework permitting collection, use and disclosure only when the **new fair and reasonable test** is satisfied
- Requiring **valid consent** to collect **sensitive information** or **trade in personal information**, unless an exception applies
- **Simplifying notification requirements** when collecting personal information.
- Replacing APP 7 with a **simplified direct marketing framework**

Right to erasure, data controllers and processors

Introducing new rights and concepts aligning with international privacy laws including:

- A new right to erasure on large digital platforms, including social media
- Introducing the concept of, and allocating responsibility between, data controllers and processors

Uplifting core definitions

Updating and clarifying core Privacy Act definitions to better reflect contemporary digital environments, data practices and community expectations including:

- Extending the definition of ***'personal information'*** to cover information that 'relates to' an individual and creating a new definition of ***'reasonably identifiable'***
- Expanding the definition of ***'sensitive information'*** to recognise new categories warranting additional safeguards, **including 'precise geolocation tracking data'**
- Clarifying when 'de-identified' data may remain personal information
- Confirming when personal information is ***'collected'***, including specific circumstances for 'sensitive information' and AI generation
- Providing greater clarity on when personal information is ***'disclosed'***, including where it is transmitted or stored overseas
- Requiring that valid ***'consent'*** must be voluntary, informed, current, specific, and unambiguous

Technology

AI's new rules of engagement: Governing AI through Australia's legal frameworks

At a glance

In July 2026, the Australian Government announced it will abandon its incremental approach to artificial intelligence (AI) governance in favour of a coordinated national legal framework with the establishment of a set of Australian Standards for AI to be legislated early next year . Responsibility for coordinating the design and legislation of the new AI standard will sit in the new Office of AI in the Department of Prime Minister and Cabinet.

In a speech titled "AI in Australia's Interests", Prime Minister Anthony Albanese framed AI as a defining economic, social and national security question which requires deliberate governance rather than passive adoption.

Australia's newly proposed legislative framework reflects an ambition to shape that trajectory by drawing together consumer protection, privacy, copyright, infrastructure, cyber resilience and national sovereignty concerns into a coordinated model of AI governance. It is anticipated the proposed legislative framework will include:

- nationally consistent minimum obligations for datacentres, including provisions addressing environment factors such as water usage and electricity consumption
- strong protections for Australian creatives against misuse of their work by AI
- requirements for investment in developing a skilled domestic workforce.

In this article, we explore how Australia's existing legislation is being used to manage the opportunities and risks presented by AI, and what the Government's announcement means for APRA-regulated insurers.

The Current Legal Landscape: No AI Act, but No Vacuum Either

Pending the implementation of the new approach announced by the Government, Australia has not yet followed the European Union down the path of standalone AI legislation.[25] Instead, AI products and services are regulated through a patchwork of existing technology-neutral laws, including the, the *Privacy Act 1988*, the *Copyright Act 1968*, the Australian Consumer Law in the *Competition and Consumer Act 2010* (**ACL**), and sector-specific regulation including the *Security of Critical Infrastructure Act 2018*.

That approach places Australia's current approach closer to the United States than to Europe. Like Australia, the US regulates AI through a combination of existing laws (including state privacy regimes), sector-based obligations, litigation-led developments, and agency oversight.

The result is not a regulatory vacuum, but an Australian legal system which applies existing legal principles to emerging technologies.

As AI becomes an increasingly embedded feature of daily life, the ACL, the Privacy Act and the Copyright Act provide the legal mechanisms through which many of the risks and challenges associated with AI are currently being addressed. We examine the evolving role of these laws in Australia's broader approach to AI governance below.

Consumer Protection: When AI Becomes Part of the Product

The ACL is already capable of reaching AI-enabled platforms in the same manner as other digital products and services. In our May Bulletin, we covered the Government's review into the ACL which found that its core protections – including consumer guarantees, manufacturer's liability provisions, and prohibitions on against misleading or deceptive conduct – already apply to AI.

A good example of how the existing law applies to AI is the ACCC's current proceeding against Microsoft. The ACCC alleges that, following the integration of Copilot into Microsoft 365 subscriptions, Microsoft failed to adequately disclose the availability of a cheaper non-AI "Classic" subscription option, resulting in consumers being steered towards higher-priced plans that included AI functionality. While the case has not been determined, it illustrates how the existing legislation already provides regulators with mechanisms to address risks to consumers of AI technologies.

25 The EU AI Act (Regulation EU 20245/1689) establishes a uniform legal framework for the development, marketing, deployment and use of AI systems across the EU.

Personal Information in the Age of Machine Learning

The Privacy Act remains the primary framework governing AI systems that collect, use and process personal information. The OAIC has identified AI as a regulatory priority, relevantly stating *"The OAIC will focus on sectors and technologies that compromise rights and create power and information imbalances including … practices that erode information access and privacy rights in the application of artificial intelligence"*.

Organisations using AI must continue to comply with the Australian Privacy Principles (**APPs**), including requirements relating to collection and use of personal information, transparency, data security, data quality, and appropriate data retention practices.

The OAIC has also made AI-adjacent regulatory determinations in relation to the operation of facial recognition technology against Bunnings (partially overturned on appeal) and Kmart, in addition to issuing a report on its preliminary enquiries into I-Med's use of de-identified data to develop and train AI models.. These matters demonstrate that, even without AI-specific privacy legislation, the APPs apply to emerging AI technologies.

Copyright: Training AI Within Existing Boundaries

Copyright is another front line in the AI governance debate. Globally, one of the major questions is whether copyright-protected works can be used to train AI models without the permission of rights holders, through text and data mining (**TDM**) or 'fair use' exceptions. Australia has so far required AI developers to operate within the parameters of established copyright law, even as courts and policymakers continue to grapple with how those boundaries apply to generative AI. In his recent announcement, the Prime Minister foreshadowed future copyright reforms to afford stronger protection to journalists, authors and artists. The government has indicated that this new legislation will include stricter copyright rules for AI developers. The proposed approach reflects growing policy focus on balancing innovation in AI with the protection of authors, artists, journalists and other rights holders.

Why Insurers Should Be Paying Attention

In its letter to the industry in April 2026, the Australian Prudential Regulation Authority (**APRA**) warned its regulated population of the growing prudential risk posed by AI and specifically called on insurers to strengthen their governance, risk management and oversight frameworks as AI adoption accelerates. APRA's concern was clear: governance and assurance practices are not evolving at the same pace as the scale and complexity of AI use.

The Australian Securities and Investments Commission (**ASIC**) has sounded a similar warning on the impact of frontier AI on the cyber threat landscape. Its message was that organisations should not wait for perfect regulatory certainty before acting. Boards and executives are expected to take immediate responsibility for strengthening their security posture and ensuring cyber risks are effectively managed.

The South Australian Government's recent announcement of Australia's first Royal Commission into AI adds another layer of scrutiny. The Commission will examine AI's economic and social opportunities and risks, including impacts on education, employment, public services, regulation, infrastructure and the broader community. The Commission's policy recommendations, which are expected by July 2027, may influence how AI is adopted in industries such as insurance.

Taken together, these developments reflect increased concern from regulators and lawmakers about the potential unseen dangers posed by AI. At least for the moment, however, the legal exposures created by AI are likely to remain within familiar categories – including breaches of consumer, corporations and privacy laws, regulatory actions, and professional liability claims for AI-related errors.

Key Takeaways

The Government's announcement signals an intentional move beyond the realm of voluntary best practice, towards a regulated and risk-focused approach to AI. Along with increased scrutiny from regulators, the introduction of AI-specific legal reforms is likely to drive demand for insurance products that respond to potential exposures and help clients navigate a changing risk landscape.

Epic Games and Google Play Settle Anti-Competition Dispute Over In-App Purchases

Epic Games has settled its long-running legal battle against Apple and Google, bringing an end to one part of a landmark case that tested how Australia's competition laws apply to major digital platforms.

The settlement follows the Federal Court's ruling in August 2025, which found that both Google and Apple had misused market power in app-distribution and in-app payment markets.[26] Although Google and Epic Games settled before final remedies were determined, the Court's findings provide important guidance on the application of Australia's misuse of market power laws.

The facts

On 13 August 2020, Epic activated Epic Direct Payment within its Fortnite app, bypassing Google Play Billing. Google removed Fortnite from Google Play for breach of its Developer Distribution Agreement, after which Epic commenced competition proceedings against Google in the United States, the United Kingdom and, in March 2021, Australia.

In the Australian proceeding, Epic alleged that Google used its control of the Android ecosystem and Google Play to restrict competition in:

- the distribution of Android apps;
- the processing of payments for digital content purchased in apps; and
- the supply of mobile operating systems to original equipment manufacturers.

26 *'Epic Games Triumphs in Australian Antitrust Lawsuit Against Apple, Google' (MLex, 12 August 2025).*

Epic alleged that Google used its control of the Google Play Store to limit competition by:

- requiring developers to use Google Play Billing for in-app purchases;
- charging service fees of up to 30% on those purchases;
- preventing developers from directing users to cheaper or alternative payment options (anti-steering rules);
- making it harder for competing app stores to operate on Android devices; and
- offering special commercial deals to large developers through its "Project Hug" program.

The Federal Court ruled that both Apple and Google held substantial power in key app-distribution and in-app payment markets and had engaged in conduct that substantially lessened competition in contravention of section 46 of the *Competition and Consumer Act 2010* (Cth).

The findings covered Apple's iOS app-distribution and in-app payment markets, as well as Google's Android app-distribution and in-app payment markets.

The Court accepted that Apple and Google advanced security, privacy and user-protection objectives in support of aspects of their app-distribution and payment ecosystems. However, the Court found that the existence of those objectives did not preclude a finding that certain conduct had the purpose, effect or likely effect of substantially lessening competition in the relevant markets. This judgment demonstrates that conduct may pursue legitimate business or security objectives while still in contravention of s 46 where it harms the competitive process.[27]

Importantly, Epic's success was confined to its competition law claims. While the Court found that Apple and Google had contravened s 46 of the CCA, it dismissed Epic's Australian Consumer Law claims. The decision is therefore significant, principally, as a misuse of market power case and a major development in Australian competition law's treatment of digital platforms, rather than as a consumer protection precedent.[28]

Settlement and Final Outcome

Following the liability judgment, the Court scheduled separate remedies hearings to determine what changes Apple and Google should be required to implement. Epic sought wide-ranging relief, including measures designed to facilitate alternative app stores and payment mechanisms, while both respondents challenged the scope of the proposed remedies.[29]

27 *Epic Games, Inc v Google LLC [2025] FCA 901 (Beach J).*
28 *Epic Games, Inc v Google LLC [2025] FCA 901 (Beach J).*
29 Saloni Sinha, ***'Apple, Google Remedies Hearing Pushed to 2026 in Epic Games' Australian Suit'*** (MLex, 17 October 2025) < https://www.mlex.com/mlex/articles/2400708/apple-google-remedies-hearing-pushed-to-2026-in-epic-games-australian-suit>.

Before the Google remedies hearing could proceed, Epic and Google reached a global settlement. In March 2026, the parties announced an agreement that included:

- reduced Google Play service fees;
- expanded developer access to alternative payment systems;
- the introduction of a Registered App Stores programme designed to facilitate competing Android app stores; and
- commitments intended to reduce barriers to app distribution outside the Play Store.[30]

The settlement also contemplated the introduction of a new billing framework in Australia, subject to ACCC authorisation. Google committed to reducing standard service fees and expanding payment choice options for developers.[31]

In April 2026, the Court vacated the scheduled remedies hearing and made orders by consent, dismissing the proceeding. Previous costs orders were set aside and there was no order as to costs. Epic subsequently confirmed that the Australian proceedings against Google had been resolved through the settlement.[32]

30 'Google to roll out new billing model in Australia by September under Epic Games settlement' (MLex, 5 March 2026) referring to Official Statement by Sameer Samat, President of Android Ecosystem, on 4 March 2026 <https://www.mlex.com/mlex/articles/2449084/google-to-roll-out-new-billing-model-in-australia-by-september-under-epic-games-settlement>.
31 Ibid.
32 Saloni Sinha, ***'Epic Games, Google relief hearing vacated inAustralia awaiting settlement approval'*** (MLex, 8 April 2026) < https://www.mlex.com/mlex/articles/2462783/epic-games-google-relief-hearing-vacated-in-australia-awaiting-settlement-approval>.

Key Takeaways

Competition law is being readily applied to digital ecosystems

The decision confirms that Australia's misuse of market power provisions are capable of addressing conduct in complex digital markets. The Court accepted Epic's market definitions and was prepared to examine how platform rules, technical restrictions and commercial arrangements affected competition within app-distribution and payment ecosystems.[33]

Legitimate business objectives do not automatically shield conduct from competition law scrutiny

One of the most significant aspects of the judgment is the Court's treatment of security justifications. The Court recognised the legitimacy of security and user-protection objectives, but nevertheless found that certain conduct substantially lessened competition. The case demonstrates that a legitimate rationale does not prevent a finding of anti-competitive effect where competition has been materially harmed.[34]

Network effects remain central to digital competition cases

Both the Australian proceedings and related US litigation focused heavily on the role of network effects. The debate extended beyond app-store fees to broader questions about how developers and consumers can realistically switch to competing platforms. Future digital platform cases are likely to continue focusing on whether proposed remedies genuinely reduce barriers to entry and expansion.[35]

33 ***Epic Games, Inc v Google LLC*** [2025] FCA 901 (Beach J)
34 ***Epic Games, Inc v Google LLC*** [2025] FCA 901 (Beach J).
35 Alex Wilts, ***'Google, Epic Games Face US Judge Skepticism over Proposed Antitrust Deal'*** (MLex, 23 January 2026) < https://www.mlex.com/mlex/articles/2433366/google-epic-games-face-us-judge-skepticism-over-proposed-antitrust-deal >; Saloni Sinha, ***'Google Remedies Hearing Delayed in Australian Epic Games Case over US Settlement Uncertainty'*** (MLex, 2 February 2026) < https://www.mlex.com/mlex/articles/2436579/google-remedies-hearing-delayed-in-australian-epic-games-case-over-us-settlement-uncertainty>.

Conclusion

Epic Games v Apple and Google represents a landmark development in Australian competition law. The Federal Court confirmed that restrictions on app distribution and payment systems can amount to misuse of market power where they substantially lessen competition, even where those restrictions are supported by legitimate security objectives. While the Google proceedings ultimately concluded through a negotiated settlement, the Court's findings will likely influence future regulatory and judicial approaches to digital platforms both in Australia and internationally.[36]

36 Saloni Sinha and James Panichi, ***'Epic Games Triumphs in Australian Antitrust Lawsuit Against Apple, Google'*** (MLex, 12 August 2025) < https://www.mlex.com/mlex/articles/2375947/epic-games-triumphs-in-australian-antitrust-lawsuit-against-apple-google>; Saloni Sinha, ***'Epic Games, Google Relief Hearing Vacated in Australia Awaiting Settlement Approval'*** (MLex, 8 April 2026) < https://www.mlex.com/mlex/articles/2462783/epic-games-google-relief-hearing-vacated-in-australia-awaiting-settlement-approval>.

When Cyber Fraud Meets Contract: The Boundaries of Proportionate Liability and Ostensible Authority

Introduction

Proceedings arose from the closure of a Pandora Jewellery Pty Ltd (**Pandora**) franchise operated by MJ Concepts Kotara Pty Ltd (**MJ Concepts**). After Pandora elected not to renew the franchise agreement, the parties entered into an Asset Sale Agreement (**ASA**) in January 2024, under which Pandora agreed to purchase the franchise's stock and business assets for $467,378.

MJ Concepts, alleged that, despite transferring the stock and assets to Pandora, it never received payment. Pandora maintained that it had made payment to a bank account nominated in an email purportedly sent on behalf of MJ Concepts (the **Fraudulent Email**). MJ Concepts denied the authenticity and authority of that email, giving rise to a broader dispute concerning an alleged payment diversion fraud. Prior to trial, Pandora applied to amend its defence to plead proportionate liability and identify alleged concurrent wrongdoers; including, a threat actor and entities associated with the MJ Concepts' email systems. The Court ultimately refused the proposed amendments and set aside related subpoenas.[37]

The Court later considered the broader claims and determined liability for the unpaid purchase price, ultimately finding that due to the nature of the Fraudulent Email it was a legal nullity and liability should be attributed to the party by whose indiscretion the loss was occasioned. The Court found that this therefore fell on Pandora, which failed to verify the suspicious email.

37 ***MJ Concepts Kotara Pty Ltd v Pandora Jewellery Pty Ltd*** [2026] NSWDC 150.

Can a threat actor be a concurrent wrongdoer – MJ Concepts Kotara Pty Ltd v Pandora Jewellery Pty Ltd [2026] NSWDC 150

Amendment Application Refused

In April 2026, Pandora filed a notice of motion seeking leave to amend its defence to include claims under the *Civil Liability Act 2002 (NSW)*, seeking to apportion liability to the fraudster and other third parties, including the operator of the fraudulent domain and mail service, and MJ Concepts itself. The amended defence sought to plead that:

- the claim was apportionable under s 34 of the *Civil Liability Act 2002* (NSW);
- there were multiple concurrent wrongdoers; and
- Pandora's liability should be reduced proportionately.

This application was refused by the Court in a decision delivered on 21 May 2026 by Cole DCJ in the District Court of NSW.[38] The Court's reasoning for its refusal had two bases:

1. *The claim is not apportionable*

The Court found that s 34 of the *Civil Liability Act* applies only to claims for economic loss arising from a failure to take reasonable care, not to breach of contract claims, which was the nature of the claim against Pandora. To succeed, MJ Concepts needed to establish only: 1) a contract, 2) an obligation to pay, and 3) non-payment. Whether

38 Ibid.

Pandora acted reasonably in relying on the Fraudulent Email before transferring the funds was irrelevant to the character of the claim.

2. *Failure to identify a particular person*

Even beyond the threshold question, the Court held that the defendant failed to meet the pleading requirements for concurrent wrongdoers established in *Ucak v Avante Developments* [2007] NSWSC 367 and endorsed in *Bingo Holdings Pty Ltd v GC Group Company Pty Ltd* [2021] NSWCA 184 (***Bingo Holdings***).

Cole DCJ, at paragraph 52 of this judgement, cited the Court of Appeal in *Bingo Holdings*:

> *"A defendant seeking to rely upon a proportionate liability limitation of recovery under Part VIA of the Competition and Consumer Act must identify each particular alleged concurrent wrongdoer. Part VIA does not allow a defendant to describe a population of individuals and assert that within that class there may be one or more concurrent wrongdoers."*

The Court noted at paragraph 54 that the defendant's descriptions of the "Domain Owner/ Administrator" and "Threat Actor" were merely descriptors of people or entities that may comprise a group. Cole DCJ stated that "neither of the descriptors can be said to identify 'a person.'"

This decision confirms that a simple breach of contract claim for failure to pay a debt cannot be transformed into an apportionable claim merely because the defendant's payment was misdirected due to fraud. Furthermore, an unknown fraudster cannot be pleaded as a "concurrent wrongdoer" because the proportionate liability regime requires identification of a particular person, specific acts or omissions, and a causal connection, requirements that a generic reference to an unidentified "Threat Actor" cannot satisfy.

The Judgment - MJ Concepts Kotara Pty Ltd v Pandora Jewellery Pty Ltd [2026] NSWDC 262 (No 2)

Business Email Compromise Confirmed

The Court found that neither Donna Matthews, nor any member of the Matthews family (of MJ Concepts), sent or caused the Fraudulent Email to be sent at 2.16am that directed Pandora to pay into the false NAB account. The Court accepted expert evidence from Mr Geoffrey Campey, a digital forensics specialist, that a Business Email Compromise (**BEC**) attack had occurred. The expert report found that a "*reasonably sophisticated threat actor*" had registered fraudulent domain names, gained access to Donna's email account, and impersonated her to redirect payment. The Fraudulent Email was characterised as a "*forgery by digital means*" and a legal nullity.

Loss Falls on Pandora

The identity of the fraudster (or fraudsters) was unknown throughout the proceedings. The Court noted there was no pleading and no submission that any act or omission of MJ Concepts caused or enabled the unknown fraudster to intercept Donna's email account. The fraud was a "*form of digital forgery*" in which the fraudster impersonated Donna and copied her signature block.

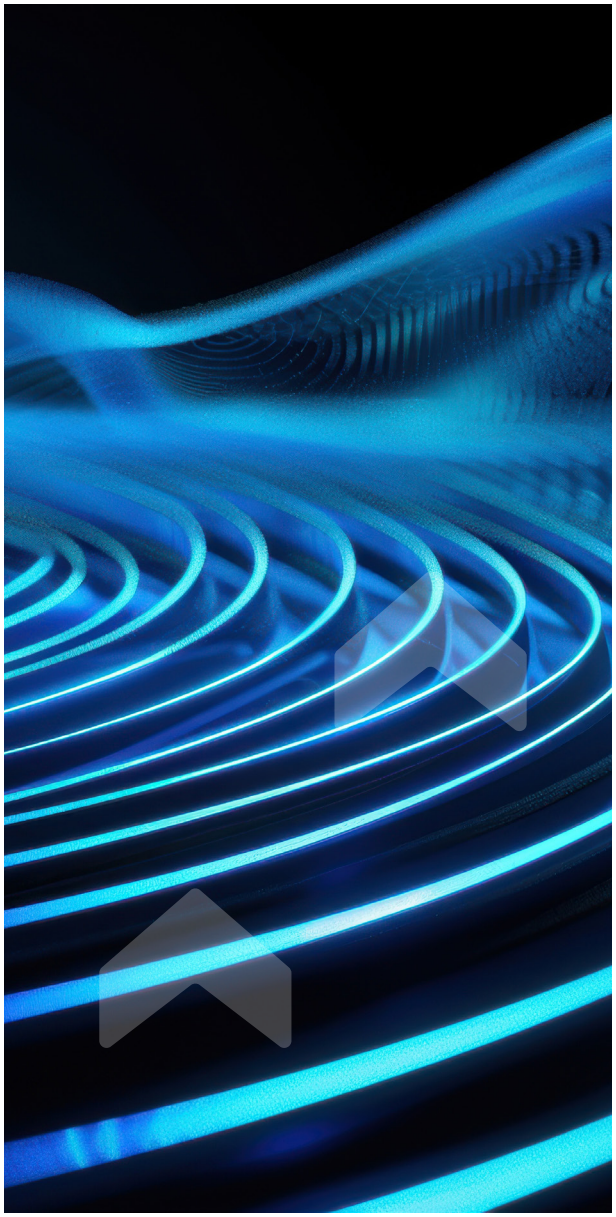
The Court applied the principle from *Tobin v Broadbent* (1947) 75 CLR 378 where one of two innocent parties must suffer, the loss should fall on the party "*by whose indiscretion it has been occasioned*". Accordingly, the Court concluded that the loss should fall on Pandora, as it failed to verify the suspicious email despite being put on inquiry.

Ostensible Authority Defence Rejected

Pandora argued that MJ Concepts' course of dealings represented that Donna Matthews had plenary authority to act on MJ Concepts' behalf, including authority to nominate a bank account under the ASA, and that Pandora reasonably relied on this when it acted on the Fraudulent Email.

The Court rejected this defence on multiple grounds:

1. **Pleading point:** The defence was not open because it was pleaded on the basis Donna sent the Fraudulent Email, which the Court found she did not.
2. **Unknown fraudster cannot bind MJ Concepts:** Any representation about Donna's authority could not extend to an unknown third-party fraudster who had neither actual nor ostensible authority. Applying *Northside Developments Pty Ltd v Registrar-General* (1990) 170 CLR 146, the Cour t found that the Fraudulent Email was a nullity.
3. **No plenary authority established:** Donna's role was limited to stock and store management, she didn't sign agreements as director, didn't negotiate the ASA, and her husband, Stephen Matthews, handled all financial dealings.



4. **Reliance unreasonable:** The email was sent at 2.16am, contradicted bank details provided days earlier, and the NAB attachment contained obvious deficiencies. Pandora made no inquiries to confirm or check the validity of the request prior to making payment.

Conclusion

These decisions are important Australian authority when looking at BECs and cyber incidents generally as they relate to the allocation of risk where a payer is deceived into directing funds to a fraudster's account. Ultimately, the Court found:

- a simple breach of contract claim for failure to pay a debt cannot be transformed into an apportionable claim merely because payment was misdirected by fraud;
- an unknown fraudster cannot be pleaded as a "concurrent wrongdoer", the proportionate liability regime requires identification of a particular person, specific acts or omissions, and a causal connection, which a generic reference to an unidentified "Threat Actor" cannot satisfy;
- Pandora's payment into the fraudulent account did not discharge its obligation to pay the purchase price, as it was not made to an account validly nominated under the ASA; and
- the fraudulent email was the product of a sophisticated cyberattack and was treated as a legal nullity.

The Court further rejected the ostensible authority defence. It found that Pandora had been put on inquiry by several suspicious features surrounding the purported change of banking instructions, including the timing of the email, its inconsistency with earlier banking details, and irregularities in the attached NAB document. In those circumstances, Pandora's reliance on the fraudulent instructions was not reasonable.

Key Takeaways for Insurers

For insurers, this case is significant because it places the **loss primarily on the party that acted on the fraudulent payment instruction, rather than automatically on the company whose email system was compromised.**

A major theme in the judgment was that Pandora should have been suspicious of the bank account change. Future underwriting questionnaires may place even more emphasis on callback verifications; dual authorisation for account changes; payment verification controls; and anti-BEC training. While the Court noted that no case had been pleaded that the victim company's cyber security deficiencies caused the attack, insurers could be expected to focus more on cyber security controls and payment authorisation procedures when assessing risk and coverage. The judgment also strengthens potential recovery and subrogation opportunities where losses result from a recipient's failure to verify suspicious payment instructions.

New Zealand

Five Eyes Agencies Call for Action on AI-Driven Cyber Risks

Five Eyes Leaders' statement on cyber risk "AI not a future consideration – it is already here"

> *"Cyber resilience is not an IT issue - it is central to operational continuity and market trust. Leaders who act now will reduce exposure, strengthen resilience, and build confidence with customers, partners, and investors. Those who delay will face growing and avoidable risk."*[39]

Five Eyes statement

On 22 June 2026, the Five Eyes cyber security agencies released a statement, and issued an urgent call to action for leaders tasked with responding to the landscape of AI and cybersecurity – particularly with the risks exposed by AI.

The call to action acknowledges that while AI will help to improve cyber defence over time, that it also increases the threat of AI as it develops apace. It urges leaders to understand and assess risk, prioritise foundational cyber security controls, empower leaders with authority and resources and stay actively engaged as both threats and guidance evolve.

The statement also notes that agencies and individuals must see cyber risks as something beyond a purely technical concern. It encourages businesses to ensure that cyber resilience is in place, effective and that AI implementation is not only relied upon for improving workplace efficiency, but is specifically considered in developing.

Specifically, the released statement shows Five Eyes leaders are alive to not only the technical risk, but the "operational, financial and reputational" exposure that incidents can have on businesses, public service agencies.

New Zealand's AI regulation

New Zealand's approach to AI regulation so far has left many commercial and technological questions unanswered. For public services, guidance is set out in the Public Service AI Framework, which non-public agencies may wish to consider as guiding principles in preparing for future regulatory action, if any.[40]

The Ministry of Business Innovation and Employment (**MBIE**), has acknowledged there are barriers for AI uptake in New Zealand, including concerns over the perceived complexity, ethics and risk involved in introducing AI.[41] Beyond this there appears to be a lack of AI skills in the New Zealand workforce and a lack of perceived value in its implementation.

These actual or perceived barriers require action in order for New Zealand organisations to be prepared in the face of frontier AI developments.

What can you do to prepare?

The Five Eyes leaders suggest the following practical actions:

1. ***Reduce your attack surface**: Limit unnecessary system access and external connectivity. Challenge whether systems need to be exposed at all and isolate those that do not.*
2. ***Accelerate patching processes**: AI is shortening the time between vulnerability discovery and exploitation. Delays in patching increase risk, especially for operational systems with long update cycles. Prioritise security updates accordingly to manage risks.*
3. ***Address legacy systems**: Unsupported systems are easy targets. They are not just technical debt, they are strategic liabilities.*
4. ***Review and strengthen identity and access controls**: Limit who can access critical systems. Enforce strong authentication and regularly review permissions.*
5. ***Prepare for incidents before they happen**: Test response plans, train and prepare teams, and assume breaches will occur. Focus on fast containment and recovery.*

The National Cyber Security Centre has produced guidance on responding to frontier AI for cyber

39 Five eyes statement: Five Eyes cyber security agencies statement, The AI shift in cyber risk: why leaders must act now

40 Public Service AI Framework | NZ Digital government

41 Addressing barriers to AI uptake in New Zealand | Ministry of Business, Innovation & Employment

and tech specialists.[42] Ensuring your operational, tech and risk management teams are across such recommendations is a good place to start.

WK's cyber, data and technology team frequently assists clients in this area offering proactive (pre-incident) advice including supporting on cyber-attack simulations, reviewing security and incident response protocols, and engaging with external cyber specialists to support testing of current system security. If you are querying how to prepare in the changing landscape, please reach out to a member of the team.

42 How-to-Act-Now-to-Prepare-for-Frontier-AI-v2.pdf

Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 (Cth) 77–80 [332]–[344]; Items 87–89.

Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 (Cth) 77–80 [332]–[344]; Items 87–89.

Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 (Cth) 77–80 [332]–[344]; Items 87–89.

Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 (Cth) 77–80 [332]–[344]; Items 87–89.

Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 (Cth) 77–80 [332]–[344]; Items 87–89.

Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 (Cth) 77–80 [332]–[344]; Items 87–89.

Updates from the New Zealand National Cyber Security Centre

New Zealand's cyber threat environment shows no sign of stabilising. The NCSC's first quarter report — covering 1 January to 31 March 2026 — confirms what many legal and risk professionals have been observing: incidents are rising in volume, severity, and financial cost.

Alongside the quarterly report, the NCSC has published targeted guidance on supply chain security, arriving at a critical moment given the Office of the Privacy Commissioner's (OPC) ongoing investigation into the Manage My Health breach.

Together, these developments deliver a clear message. Organisations that treat cyber security governance as a compliance formality, rather than a strategic imperative, face mounting legal, regulatory, and reputational exposure.

A quarter of escalating threats

The NCSC Q1 2026 figures tell a clear story of escalation. The key statistics are:

- 1,164 cyber incidents reported to NCSC over the reporting period;
- three incidents were categorised as highly significant (C2) meaning, they impacted key sensitive data and / or caused disruption to essential New Zealand services in organisations of national significance;
- the NCSC calculated total losses from cybercrime of NZD $5.6 million, with individual New Zealanders accounting for NZD $5.2 million of that figure; and
- overall the NCSC statistics show a 76% increase in malicious activity from the previous quarter.

The 76% quarter-on-quarter increase reflect a sustained and deepening threat trajectory. The three incidents classified at C2 severity are of particular concern for organisations operating critical infrastructure or holding nationally significant data. A C2 classification signifies material impact on sensitive data and/or disruption to essential New Zealand services, carrying severe reputational, regulatory, and legal consequences.

Supply chain security: the NCSC's new guidance and what it means for your organisation

The statistics alone do not capture the full picture. Modern cyber incidents increasingly reflect systemic vulnerabilities — particularly in the context of supply chain risk. The NCSC's supply chain security guidance (see here) is a direct and considered response to this threat landscape. The guidance is particularly timely given the OPC's stage 1 report into the Manage My Health compromise

The guidance identifies a foundational set of technical controls that organisations should implement themselves and actively require of key suppliers and technology partners as a minimum baseline for supply chain security:

- ensuring appropriate firewall protection;
- encrypting data;
- enforcing multi-factor authentication (MFA);
- setting access limitations on accounts; and
- enabling data loss prevention (DLP) solutions for data at rest.

A few themes from the guidance deserve particular attention from legal and risk professionals.

- **Mapping and understanding your supply chain:** The guidance encourages organisations to develop visibility across their full supplier network, including fourth-party dependencies — the suppliers of your suppliers.
- **Embedding security requirements contractually:** The NCSC recommends incorporating explicit cyber security obligations into supplier agreements — including requirements for suppliers to maintain appropriate security practices, notify promptly of any security incident, cooperate with audits, and flow down equivalent obligations to their own sub-contractors.
- **Ongoing assurance and monitoring:** Rather than relying solely on due diligence at procurement, the guidance recommends establishing continuous assurance mechanisms — including periodic security reviews, audit rights, and monitoring of threat intelligence relating to key suppliers. Incident response plans should explicitly address third-party compromise scenarios, and those plans should be tested, not merely documented.
- **Aligning with Privacy Act 2020 obligations:** The Privacy Act 2020 requires organisations to take reasonable steps to protect personal information they hold, including information processed or stored by third parties on their behalf. Where a vendor handles personal information, the privacy principles place accountability squarely on the principal organisation.

The confluence of a rising threat environment and timely NCSC guidance presents a genuine opportunity for organisations to recalibrate their approach to third-party cyber risk.

Manage My Health: Key Lessons from the OPC's Phase One Report

In May 2026, the Office of the Privacy Commissioner (OPC) released its Phase One Report into the platform compromise suffered by Manage My Health (MMH) in December 2025. The Phase One Report focuses on security-related privacy issues, specifically:

- whether MMH and Health New Zealand maintained "reasonable security safeguards" as required by Rule 5 of the Health Information Privacy Code 2020;
- who bore legal responsibility for the personal information held in the portal; and
- what due diligence obligations apply when organisations rely on third-party platforms to handle sensitive data.

The Report provides critical insights into the regulator's approach to assessing security controls and the appropriate allocation of responsibility following a privacy breach. It also sets out the OPC's intended regulatory response and makes broader recommendations for legislative reform.

The Manage My Health incident and resulting inquiry

MMH operates a widely-used patient health portal. On 1 January 2026, the OPC was notified that a threat actor had used compromised user credentials to access and extract documents from the portal, ultimately impacting 99,416 patients out of approximately 1.85 million user accounts held at the time.

The OPC launched a formal inquiry under section 17(1)(i) of the Privacy Act 2020. It also engaged an independent cybersecurity expert to analyse MMH's security posture at the time.

Whose data is it anyway?

A threshold question in the Phase One Report was which entity was legally responsible for the personal information held in the portal. Patient information was drawn from multiple sources — Health New Zealand, individual GP practices, and patients themselves.

The OPC concluded, following a close examination of how MMH operates in practice, that all information in the impacted module was "held" by MMH within the meaning of the Privacy Act. MMH was not merely a processor acting on behalf of other agencies; it was an independent data controller with full regulatory accountability under Rule 5 of the Health Information Privacy Code 2020 (the Code).

This conclusion confirms that the characterisation of a party's role in a data processing arrangement is a question of substance, not contractual form — and that the same analysis would not automatically apply to all third-party health service providers.

When are safeguards safe enough?

The central finding of the Phase One Report is that both MMH and Health New Zealand failed to maintain "reasonable security safeguards" as required by Rule 5 of the Code. Critically, the Report found the breach was not the product of a single failure — it arose from a combination of deficiencies that both enabled the incident and amplified its impact.

New Zealand has historically had limited regulatory guidance on what "reasonable" security safeguards require in practice, and the Phase One Report begins to close that gap. While the OPC confirms that the standard remains inherently context-dependent, it makes clear that security safeguards encompass technical, organisational, and physical measures — and that the expected standard scales with the sensitivity of the information at issue. A smaller organisation handling highly sensitive data, such as health records, is still expected to maintain robust and effective protections.

Organisations seeking practical benchmarks should refer to guidance including Poupou Matatapu, the NCSC's minimum cybersecurity standards, ISO standards, and the Health Information Security Framework.

Doing your due diligence

The Phase One Report also places considerable emphasis on the obligations of entities that rely on third-party platforms to collect, store, or process personal information.

The OPC stresses that due diligence before contracting is essential, and should encompass thorough privacy impact assessments, ongoing reviews of a vendor's privacy posture, and meaningful governance engagement — particularly where the information is of a highly sensitive nature.

Having an incident response plan is necessary, but insufficient: organisations must also validate that those plans will actually work in practice. The Report is unambiguous on the key point — reliance on a third-party platform does not reduce an entity's regulatory exposure.

The next phase

The OPC intends to issue compliance notices under section 123 of the Privacy Act directing both MMH and Health New Zealand to address the identified deficiencies and demonstrate compliance with Rule 5 of the Code.

Beyond the immediate parties, the Report carries broader systemic recommendations: the OPC has called on the Ministry of Health to establish a centralised programme to verify that key health sector vendors are meeting relevant security standards, and has recommended that the Ministry of Justice consider amending the Privacy Act to impose direct liability on third-party service providers under Information Privacy Principle 5 — a potentially significant development for the sector.

Phase Two of the inquiry, expected later this year, will examine patient consent, information retention and deletion practices, the quality of breach communications, notification compliance, and issues of particular relevance to Māori, including Northland Māori.

Because Rule 5 of the Code closely mirrors Information Privacy Principle 5 of the Privacy Act, the OPC's findings are relevant to all New Zealand agencies handling sensitive personal information — not only those in the health sector. Any organisation that collects, stores, or processes sensitive data, whether directly or through third-party platforms, should treat the Phase One Report as a prompt to review its security arrangements, vendor due diligence practices, and contractual risk allocation.

The question is no longer simply whether safeguards are in place, but whether they are effective.

We note that WK acted for Manage My Health in assisting with its response to the incident, including in obtaining injunctive relief again persons unknown.

Singapore

Singapore tightens rules governing critical services sectors to counter AI cyberthreats

On 29 July 2026, the Cybersecurity Agency of Singapore (CSA) published an update to the Cybersecurity Code of Practice (CCoP) for Critical Information Infrastructure Owners (CIIO). This is the first material change to the CCoP since it first took effect in 2022. The update is a deliberate regulatory response to the emerging pressure of Advanced Persistent Threats (APT) and AI-enabled cyber attacks. Whilst the update to the CCoP applies to CIIOs, as explained below, there is also scope for non-CIIOs to be affected.

What is changing

Board and Senior Management Accountability: The CCoP makes clear that the Boards will be held accountable for ensuring adequate resources and attention are devoted to the organisation's cybersecurity strategy. Senior Management will need to translate the strategic direction into operational reality. This includes:

- Having documented cyber resilience frameworks covering risk tolerance, risk mitigation, risk transfer and risk recovery.
- The Board should attend cybersecurity training at least once every 12 months or earlier, depending on the evolving cyber threat landscape.
- The Board should receive a cyber threat briefing at least once every 6 months or earlier, depending on the evolving cyber threat landscape. The Board's guidance or instructions from the cyber threat briefing shall be documented in Board minutes.
- Ensuring at least one member of senior management (or any other employee) possesses the knowledge and awareness necessary to manage cyber risks. The role and responsibilities of this person should also be set out in writing.

Cyber Trust Mark Level 5 Certification: CIIOs will be required to be Cyber Trust Mark (Tier 5) certified. The scope of certification encompasses the CIIO's governance, risk management and enterprise-wide management of cybersecurity capabilities, system operational processes, and information systems and infrastructure that the organisation owns, operates and/or controls, which are used to deliver its products and services.

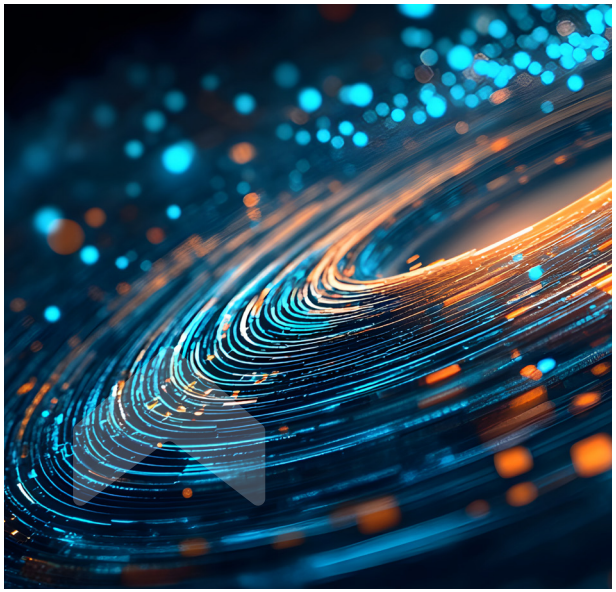
Cloud Computing: Cloud computing was previously dealt with under general outsourcing management. Moving forward, there will be a separate CCoP for cloud computing systems which will be published in the second half of 2026 with companion guides co-developed with cloud service providers like Amazon Web Services, Google Cloud and Microsoft Azure.

When will the amendments take effect?

Most of the new requirements will take effect on 29 July 2027, while the Cyber Trust Mark (Tier 5) certification requirement will take effect from 31 December 2027. From now until then, CIIOs must continue complying with the previous version of the CCoP.

Why all organisations should be watching closely

While the new CCoP applies only to CIIOs, non-CIIOs may also be affected as CIIOs' obligations tend to flow down contractually as part of supply-chain due diligence. The CSA's CCoP also dovetails with the existing MAS Technology Risk Management and AI Risk Governance guidelines for financial institutions. These emerging regulations should prompt all companies to pay closer attention to cybersecurity as a Board and Management level risk, rather than an obscure IT policy delegated to the IT team.



Singapore: Commencement of Online Safety (Relief and Accountability Act) and Online Safety Commission

The Online Safety (Relief and Accountability) Act 2026 (OSRAA) was passed in the Singapore Parliament in November 2025 and came into operation on 29 June 2026. The Online Safety Commission (OSC) also commenced operations on the same day, as the agency supporting the Online Safety Commissioner to provide victims of online harms with a more accessible avenue for relief.

Providing victims with timely relief

While the OSRAA addresses 13 categories of online harms, the OSC will first focus on the five most prevalent and severe harms being:

1. online harassment
2. doxxing
3. online stalking
4. intimate image abuse; and
5. image-based child abuse.

Under the OSRAA, the OSC is empowered to issue various directions to address online harm including directions to disable access to the harmful content or restrict the perpetrator's account. Crucially, the OSC can require online platforms to disclose user identity information of anonymous accounts suspected of committing severe online harms. This aims to address the problem of perpetrators using anonymity as a shield. Victims can request help from the OSC in identifying the perpetrator for the purposes of commencing civil proceedings against that person.

The OSRAA also prescribes strict statutory response timelines for prescribed online service providers to act upon receiving an online harm notice or direction. These include:

- Within 6 hours – for severe intimate image abuse / image-based child abuse cases where private parts are exposed
- Within 24 hours – for other forms of intimate image abuse or image-based child abuse material
- Within 48 hours – for all other prescribed categories of online harm.

For now, the prescribed online service providers include large online platforms such as Google LLC (for YouTube, Google Maps Reviews), Meta Platforms Inc (for Facebook, Instagram, Threads), Whatsapp LLC (for Whatsapp), Tiktok Pte. Ltd, Reddit Inc, and Telegram Messenger Inc.

Failure to take required steps within designated timeframes leaves platforms in direct breach of statutory duties, and enables victims to pursue formal civil proceedings and statutory damages.

The remaining eight categories of harm (e.g. online impersonation, inauthentic material abuse, publication of false material, non-consensual disclosure of private information) will be phased into effect progressively.

Statutory torts, right of private action

The OSRAA creates statutory torts to allow victims to simultaneously commence civil proceedings to obtain various remedies, without needing to prove a traditional common law duty of care.

Victims can seek civil remedies such as damages (eg. for losses suffered including loss of future earnings and earning capacity, an account of profits) and/or injunctions to stop the dissemination of the online harmful activity. The courts are also empowered under the OSRAA to grant "enhanced damages" when written requests to address the online harmful activity are not responded to within reasonable time.

In the case of proven child abuse images or recordings, or intimate image abuse or recordings, there is a minimum stipulated amount of S$5,000 in damages. This amount is not subject to evidence of damage caused, which is favourable to victims as the harm caused by intimate image abuse is usually difficult to prove (usually being reputational, psychological or relational).

Closing remarks

It is important to note that the remedies under the OSRAA complement, rather than replace, other existing remedies, for instance, under the Protection from Harassment Act 2018.

The introduction of the OSRAA reflects a broader global trend of governments increasing digital governance. However, what makes Singapore unique is that it is one of the only countries globally to introduce an agency specifically to address online harms. It also provides individuals with the option to seek recourse directly through the establishment of statutory torts.

ASEAN DEFA Signals Greater Regional Alignment on Data, Cyber and Digital Trade

Negotiations on the Association of Southeast Asian Nations' (ASEAN) Digital Economy Framework Agreement (DEFA) concluded on 31 May 2026, with the agreement expected to be signed at the 49th ASEAN Summit in November 2026. Once finalised, the DEFA will be ASEAN's first comprehensive regional agreement focused on the digital economy, providing a framework to deepen digital integration and cooperation across member states.

The DEFA is intended to support the growth of ASEAN's digital economy by establishing common rules and facilitating greater interoperability across the region. Key objectives include facilitating digital trade, enabling trusted cross-border data flows, enhancing digital payment systems, strengthening electronic transactions, improving online consumer protection, and reducing regulatory friction for businesses operating across multiple ASEAN jurisdictions.

While the final text has not yet been released, studies commissioned during the negotiation process indicate that the agreement is expected to address a broad range of digital economy issues, including:

- cross-border data flows and digital trade;
- digital identity and electronic authentication frameworks;
- digital payments and e-invoicing;
- cybersecurity and online safety;
- artificial intelligence and other emerging technologies;
- financial technology innovation and regulatory cooperation;
- source code protection;
- digital talent mobility and workforce development; and
- competition issues within digital markets.

For businesses operating across ASEAN, the agreement has the potential to simplify regional digital operations by promoting greater consistency between regulatory frameworks. Reduced barriers to data sharing, digital transactions and electronic commerce could create new opportunities for organisations seeking to expand their digital presence within the region.

Implementation challenges remain

Despite its ambitious objectives, the DEFA's ultimate impact will depend on implementation at the national level. ASEAN member states are at different stages of digital maturity, with varying legal frameworks, regulatory priorities and enforcement capabilities.

While the agreement provides a common strategic direction, meaningful harmonisation will require member states to align domestic laws and regulatory approaches across areas such as data protection, cybersecurity, digital identity and electronic transactions. The extent to which the DEFA delivers on its promise of a more integrated digital economy will therefore depend on how effectively those commitments are translated into consistent regulatory and operational outcomes across the region.

Why it matters

ASEAN's digital economy is projected to reach US$2 trillion by 2030, making it one of the world's fastest-growing digital markets. The DEFA represents a significant step towards creating a more integrated regional digital ecosystem and reflects ASEAN's broader ambition to support digital-led economic growth.

For organisations with operations, customers or supply chains across ASEAN, the DEFA should remain firmly on the regulatory watchlist. As implementation progresses, businesses should monitor developments relating to data governance, cross-border data transfers, privacy, cybersecurity obligations, digital identity frameworks and payment services regulation.

Organisations that engage early with emerging regulatory requirements will be better positioned both to manage compliance risks and to capitalise on the commercial opportunities arising from a more connected regional digital economy.

Singapore and Japan Deepen Privacy and Data Governance Cooperation

Singapore's Personal Data Protection Commission (PDPC) and Japan's Personal Information Protection Commission (PPC) signed a Memorandum of Cooperation (MOC) on 20 July 2026 at the Singapore Data Festival, further strengthening regulatory collaboration on privacy, data governance and digital trust.

The MOC seeks to enhance cooperation on data breach investigations, cross-border data transfers and the exchange of information on emerging issues, including artificial intelligence and privacy-enhancing technologies. It also lays the groundwork for the development of model contractual clauses that could facilitate data transfers between the two jurisdictions.

While the arrangement is non-binding, it signals a commitment by both regulators to greater regulatory alignment and interoperability. For businesses operating across Singapore and Japan, this may help reduce compliance friction over time by promoting more consistent approaches to privacy regulation and cross-border data governance.

The agreement builds on Singapore's broader strategy of strengthening regional privacy cooperation. The PDPC has previously entered into similar arrangements with privacy regulators in South Korea and Hong Kong, reflecting a wider trend towards greater regulatory coordination across the Asia-Pacific region.

Part of a Broader Digital Cooperation Agenda

The MOC follows a separate agreement signed earlier in 2026 under which Singapore and Japan agreed to mutually recognise certain Internet of Things (IoT) cybersecurity labelling schemes. The arrangement streamlines market access for manufacturers by enabling products certified under one country's scheme to more easily obtain recognition in the other.

Taken together, these initiatives demonstrate a growing focus on regulatory interoperability across privacy, cybersecurity and digital governance frameworks. As digital trade and cross-border data flows continue to expand, such arrangements are likely to play an increasingly important role in reducing regulatory complexity and supporting trusted digital ecosystems.

Why it matters

Although the MOC does not create new legal obligations, it provides a useful indicator of the direction of travel for privacy and digital regulation in the region. Businesses with operations across Asia-Pacific should expect continued efforts by regulators to align approaches to data protection, cross-border data transfers, AI governance and cybersecurity oversight.

Organisations that proactively monitor these developments will be better placed to navigate evolving regulatory expectations and take advantage of opportunities arising from a more integrated regional digital economy.

Hong Kong Securities and Futures Commission Fines Brokerage HK$2.1 Million Following Ransomware Incident

On 28 July 2026, the Hong Kong Securities and Futures Commission (SFC) fined Luk Fook Securities (HK) Limited (LFSHK) HK$2.1 million following a ransomware attack that disrupted the firm's operations for almost three weeks. The decision is notable as the first reported SFC disciplinary action arising from a cyber incident based specifically on cybersecurity control deficiencies rather than customer losses, fraud or market misconduct.

The ransomware attack impacted multiple components of LFSHK's critical technology infrastructure, including file servers, domain controllers, email systems, trading application servers and accounting servers. During the recovery period, clients were unable to access the firm's online and mobile trading platforms and instead had to place orders through account executives.

The SFC identified numerous deficiencies across LFSHK's cybersecurity environment, including inadequate network security controls, weak privileged access management, unsupported legacy systems, outdated anti-virus protections, insufficient controls over remote access and external devices, poor password management practices, and inadequate cybersecurity awareness training.

Taken together, the SFC concluded that these deficiencies increased LFSHK's vulnerability to cyberattacks and may have contributed both to its inability to withstand the ransomware attack and to the prolonged recovery period. Importantly, the regulator emphasised the cumulative effect of multiple control weaknesses, rather than any single failing, in assessing the firm's cybersecurity posture and resilience.

In determining the penalty, the SFC took into account several mitigating factors, including LFSHK's cooperation with the investigation, the engagement of an independent reviewer to assess the incident and its cybersecurity controls, remediation measures implemented following the attack, the absence of evidence of client losses, and the firm's otherwise clean disciplinary record.

The SFC also identified several aggravating factors, including the extended duration of the outage, weaknesses in backup and recovery arrangements, deficiencies in business continuity planning, and the absence of formal policies and procedures governing key cybersecurity risk areas such as incident management, data security and record retention.

Why it matters

The decision signals an increasingly mature regulatory approach to cybersecurity risk, where regulators are scrutinising not only whether organisations can prevent cyber incidents, but also whether they can effectively withstand and recover from them.

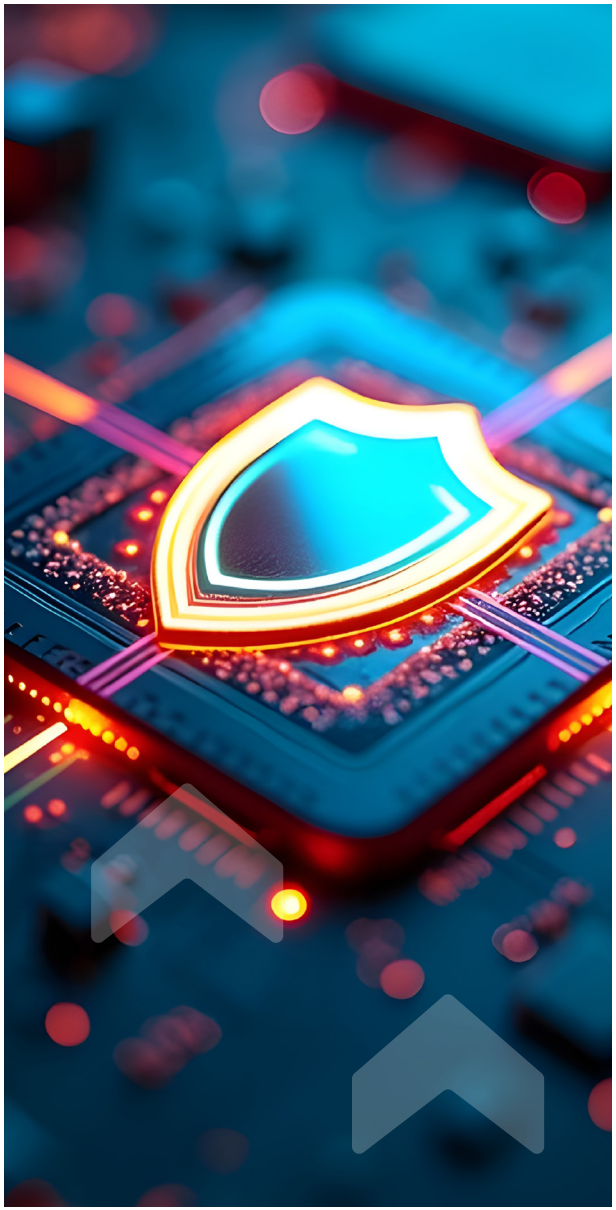
Importantly, enforcement action was taken despite there being no evidence of asset misappropriation, unauthorised trading activity, client losses or significant customer complaints. The focus instead was on governance, cyber resilience and the adequacy of the firm's control environment.

For regulated entities, the decision reinforces that cybersecurity failures are no longer viewed solely as technology issues. They are increasingly regarded as governance and risk management failures capable of attracting regulatory scrutiny and enforcement action in their own right.

Key takeaway

This enforcement action reflects a broader regulatory trend towards holding organisations accountable for weaknesses in cybersecurity governance, operational resilience and incident response preparedness. This is consistent with the Hong Kong Market Authority's regulatory posture, the SFC's June and July 2026 circulars on strengthening cybersecurity controls and its earlier 2023/2024 thematic cybersecurity review of regulated entities which was published in February 2025.

Cyber incidents are an unavoidable risk for all organisations in the highly digitalised global economy. As such, organisations can expect regulators to pay close attention to the adequacy of their cybersecurity governance, operational resilience and recovery capabilities, including their incident response preparedness.



Stricter South Korea Personal Information Protection Act (PIPA) penalties

South Korea is moving towards significantly stricter privacy enforcement, with amendments to the PIPA increasing the potential financial consequences for organisations that mishandle personal information. The reforms come amidst a backdrop of several high-profile data breach investigations and enforcement actions by the Personal Information Protection Commission (PIPC) e.g. the SK Telecom cyber incident where a record administrative penalty of KRW 134.8billion (~ US$97 million) was imposed in August 2025 following a data breach affecting around 23 million subscribers and the Coupang data breach affecting over 33 million customer accounts which attracted the highest fine awarded by the PIPC to date of KRW 624.7billion (~ US$409 million) in June 2026.

Under the existing framework, the PIPC can impose administrative penalties of up to 3% of an organisation's revenue. However, recent legislative amendments will:

- increase the maximum penalty to 10% of total turnover for serious violations (i.e. repeated breaches within three years, gross negligence affecting over 10 million individuals or failure to follow corrective orders), bringing South Korea's enforcement regime closer to some of the most stringent privacy frameworks globally;
- extend reach reporting rules to data falsification, not just unauthorised exposure;
- tighten senior management accountability by requiring mandatory reporting of Chief Privacy Officer appointments in certain organisations.

Most provisions are expected to take effect from September 2026.

South Korea is rapidly establishing itself as one of the most active privacy enforcement jurisdictions in the Asia-Pacific region. The increased penalty framework demonstrates the regulator's willingness to pursue substantial sanctions against large organisations. It also elevates the potential financial and reputational risks and costs associated with data protection failures.


Thailand

Thailand's Next Step in AI Governance: Inside the Draft AI Act

At a glance

- Thailand has taken a major step towards AI regulation with the release of its Draft AI Act for public consultation.
- The Draft AI Act adopts a risk-based approach, similar to the EU AI Act, with obligations varying according to the level of risk posed by AI systems.
- The draft has broad extraterritorial reach and may apply to overseas AI providers whose systems affect individuals in Thailand.
- Certain AI systems may be prohibited, while others may be subject to registration, transparency, risk-management, or licensing requirements.
- Businesses using AI should begin assessing their AI governance frameworks now, even though the legislation is not yet in force.

What happened?

In July 2026, Thailand took a significant step towards regulating artificial intelligence with the release of the Draft AI Act for public consultation. While the legislation remains subject to revision, it provides a clear indication of how Thai regulators expect organisations to govern the use of AI in the future.

The draft follows a series of AI-related regulatory developments over the past year, including guidance from the Bank of Thailand, the Office of Insurance Commission and the Personal Data Protection Committee. Taken together, these developments suggest that AI governance is increasingly becoming a regulatory expectation rather than a matter of best practice.

More than a law for technology companies

One common misconception is that AI regulation primarily concerns businesses developing AI systems. The Draft AI Act takes a broader approach.

Many organisations already rely on AI for customer service, recruitment, fraud detection, document review, claims handling and operational decision-making. The draft indicates that organisations using AI may also bear responsibilities in relation to the deployment and oversight of those systems, even where the underlying technology is developed by a third-party vendor.

For businesses, the practical question is therefore not whether they are developing AI, but whether they understand where and how AI is already being used across their organisation.

A focus on risk, not technology

Rather than regulating every AI system in the same way, the proposed framework adopts a graduated approach based on the risks presented by particular use cases.

In general terms, AI applications capable of causing greater harm to individuals or society would be subject to more extensive compliance obligations, while lower-risk applications would face fewer requirements. The objective appears to be encouraging innovation while ensuring that safeguards are applied where AI has the potential to materially affect people's rights, safety or livelihoods.

This reflects an emerging international trend towards regulating the consequences and risks associated with AI, rather than the technology itself.

The growing challenge of AI-generated content

The draft also places considerable emphasis on transparency in relation to AI-generated content.

As generative AI tools become increasingly capable of producing realistic images, videos, audio recordings and text, regulators are becoming concerned about misuse, including impersonation, misinformation, fraud and other forms of deception. The proposed legislation therefore contemplates measures designed to help users distinguish AI-generated content from authentic content and to reduce the risk of misuse.

For businesses, this issue is particularly relevant as AI-generated content increasingly forms part of marketing, customer engagement and internal operations.

Why businesses should pay attention now

Although the Draft AI Act has not yet been enacted, businesses may wish to view it as an indicator of future regulatory expectations.

Many of the concepts reflected in the draft, such as governance, accountability, risk assessment, transparency and human oversight, are already appearing in guidance issued by regulators both in Thailand and overseas. Organisations that begin considering these issues now are likely to be better positioned to respond as the regulatory landscape continues to evolve.

Key contacts

Kieran Doyle
Head of Cyber, Data & Technology
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
AI Governance and Privacy Lead
Brisbane
+61 7 3236 8739
leah.mooney@wottonkearney.com

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

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

Pippa Austin
Special Counsel
Singapore
+65 6967 6473
pippa.austin@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 9292

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

Nelson
Level 1, Montgomery House
190 Trafalgar Street
Nelson 7010
+64 3 548 4136

Tauranga
148 Durham Street
Tauranga 3110
+64 7 806 9600

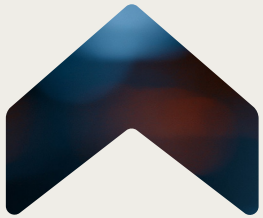
Wellington
Level 12, 342 Lambton Quay
Wellington 6011
+64 4 499 5589

Asia

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

Bangkok
990 Abdulrahim Place
Unit 1710, 17th Floor, Rama 4 Road
Silom Sub-district, Bang Rak District
Bangkok 10500
Thailand
+66 2 460 7301

WOTTON KEARNEY



wottonkearney.com