sparke HELMORE LAWYERS

# Sparke Bytes

## Latest developments in technology, privacy, AI, spam and cyber

SEP 2025 QUARTERLY

# CONTENTS



# FINAL REPORT IN THE DIGITAL PLATFORMS INQUIRY CHARTS THE WAY FORWARD ON PROTECTING CONSUMERS AND SMALL BUSINESSES FROM HARM IN DIGITAL MARKETS

Authors: Hamish Fraser (Partner) and Nick Christiansen (Partner)

On 23 June 2025, the ACCC published its tenth and the final report following a comprehensive five-year investigation into Digital Platforms.

With over 400 pages, the final report has a considerable amount of information to digest. In this article, we highlight some of the key findings and recommendations that could impact Australian businesses.

## The lead-up to the final report - eight years and three inquiries

Since 2017, and across three inquiries, the ACCC has published fourteen reports and made thirty-five separate recommendations.

The reports from the Inquiry are a treasure trove of deep analysis into the changing nature of the way Australians engage with the digital world and comparisons with overseas trends and developments.

The reviews have already led or contributed to significant legislative reform in Australia, particularly in the digital economy, including:

- Strengthening the unfair contracts regime
- The Scams Prevention Framework Act, and
- The ongoing overhaul of the Australian Privacy regime.

## Conclusion of the Digital Platform Services Inquiry

This final report focuses on lessons for Australia from overseas digital platforms competition regimes, developing trends in online marketplaces, and competition issues in cloud computing and generative AI.

It also highlights the extraordinary growth in digital platform services with:

- 99% of adults using connected devices
- 94% of people over fourteen years of age own a smartphone and
- Almost 40% of Australians wear a device connected to the internet.

### New digital competition regime and mandatory service-specific codes

Digital platforms are a concern for the ACCC because of their capacity to control access to digital markets for consumers, developers, and small businesses. This control can lead to competition and consumer harms, such as increased price, reduced quality and choice, and restricted access to inputs and markets.

The ACCC has observed conduct by powerful digital platforms that distorts competition. Key issues include denial of interoperability and impeding switching, self-preferencing and tying, restricting access to key inputs, and exclusivity agreements.

Examining the regulatory frameworks implemented in the European Union, United Kingdom, Germany, and Japan targeting digital markets, the ACCC has reiterated the need for a new digital competition regime in Australia. This regime would address the slow pace of enforcement action against anti-competitive conduct in digital platform markets, the difficulty addressing continuing competitive harms, and the limited remedies available under existing competition laws.

The new digital competition regime proposed by the Australian Government in December 2024 would designate certain digital platforms with a critical position in the Australian economy – beginning with app marketplaces and ad tech services. The platforms would subject to a range of broad and service-specific obligations targeting anti-competitive conduct, enforceable by the ACCC.

The ACCC also reiterated its support for the introduction of mandatory service-specific codes of conduct. The codes would require designated digital platforms to comply with obligations targeting anti-competitive self-preferencing and tying, exclusive pre-installation, impediments to switching and interoperability, exclusivity, and other anti-competitive behaviours.

### Tackling unfair trading practices in digital markets

With the growth in digital platform services comes significant risk of increased competition and consumer harms, which undermine confidence and trust necessary for a well-functioning marketplace. These issues include:

- Undisclosed 'influencer' sponsorships
- Exploitative marketing and sales strategies, particularly those using consumer data, including subscription traps, drip pricing, and hidden fees
- Interface design strategies that impede consumer choice
- The use of AI-generated outputs to shape consumer behaviours and prevent informed decision-making
- Business practices designed to limit, discourage, or prevent the exercise of consumer rights and making it difficult for consumers to cancel services or to obtain remedies
- Various unfair contracting practices designed to have consumers agree to unfavourable contract terms.

The existing consumer protection laws are not considered adequate to fully address these harms, and the ACCC has again pressed for the introduction of an economy wide unfair trading practices prohibition.

Additionally, the ACCC has reiterated the need for mandatory minimum internal dispute resolution standards and an independent external dispute resolution body to address consumer and small business complaints relating to digital platform services, a suggestion that has strong support from Australian consumers. Existing dispute resolution processes on digital platforms are widely seen as inadequate, leaving to obvious consumer harms.

**Emerging competition issues: cloud computing and generative AI**

The report recognises the dynamic nature of digital platform services and, in that context, the need for continued scrutiny and monitoring of emerging technologies and their effects in other markets. The report focuses particularly on emerging competition issues arising from cloud computing and generative artificial intelligence.

Competition risks from cloud computing include:

- Significant barriers to entry and expansion within the cloud computing infrastructure market, given the significant upfront investment costs, the economies of scale and scope of the large incumbent cloud providers, and network effects from those providers existing software and hardware products.
- Barriers to switching and interoperability between cloud infrastructure services providers, including high egress fees, including the effect of those barriers on new providers in the market.
- Concentration of cloud computing services in existing large digital platforms that are vertically integrated across the cloud stack, with the risk of potentially anti-competitive bundling and tying of services. Where cloud providers also offer generative AI products and services, there is a related risk of them bundling, tying, or self-preferencing their own products over those of competitors.
- Information asymmetries between cloud computing service providers and customers.

The potential competitive harms include increased costs to consumers and businesses and reduced innovation in generative AI technologies.

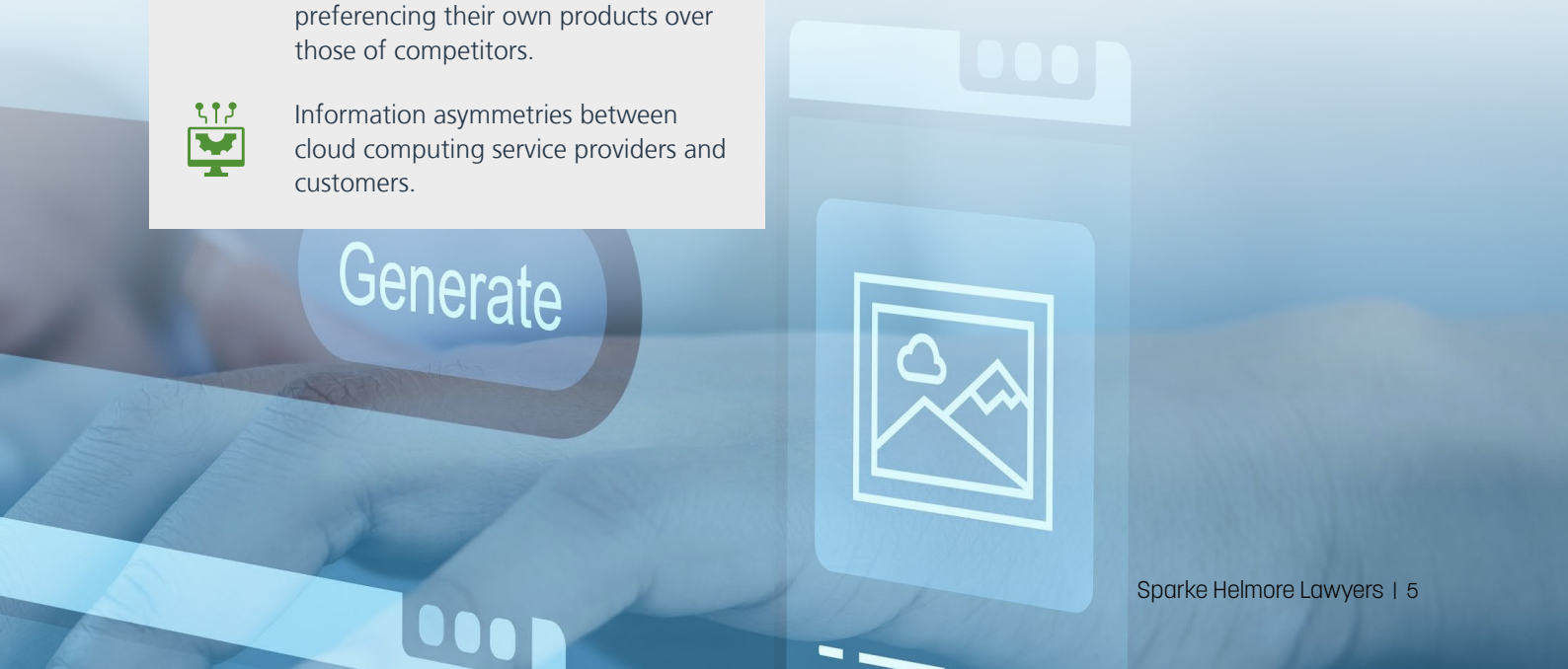
These issues give rise to two further recommendations made in the Final Report.

First, the ACCC proposes that be empowered and resourced to continue to have a monitoring function for emerging digital technologies under the proposed digital competition regime. This is intended to allow for new enforcement proposals and to inform the development and amendment of the service-specific codes.

Secondly, the ACCC proposes that the Australian Government priorities a whole-of-government approach to digital platform regulation. Since March 2023, the ACCC, the OAIC, the ACMA and the eSafety Commissioner have formed the Digital Platform Regulators Forum (DP-Reg), and the Report recommends that this be recognised as a permanent forum with adequate resources to continue to undertake information-sharing and collaboration between these regulators. These proposals are intended to ensure that digital markets are regulated in a streamlined, collaborative, holistic, and consistent way.

**Find out more**

Readers interested in the full report will find it published on the ACCC's website here and the ACCC's summary of the key findings from the final report here.



# CYBERSECURITY AS AN AFS LICENSEE OBLIGATION: ASIC'S STRONGER ENFORCEMENT APPROACH

Authors: Marianne Robinson (Special Counsel), Stephen Putnins (Partner), Robert Fraser (Associate), and Ella Sourdin Brown (Law Graduate)

*'It is not possible to reduce cybersecurity risk to zero, but it is possible to materially reduce cybersecurity risk through adequate cybersecurity documentation and controls to an acceptable level.'* Her Honour Justice Rofe in 2022.

In response to the increasingly hostile cyber landscape, the Australian Securities and Investments Commission (**ASIC**) has reminded AFS Licensees of their legal obligations to manage cyber risks – not only within their own operations but also across those of their authorised representatives. To reinforce how seriously ASIC views these obligations, it has already taken legal action against two financial services businesses in 2025 due to inadequate cybersecurity measures.

In March 2025, ASIC initiated proceedings against FIIG Securities Limited (**FIIG**), alleging that the company had failed to implement proper cyber security measures and in doing so breached multiple obligations imposed on AFS licensees by the *Corporations Act 2001* (Cth) (the **Corporations Act**). In July 2025, ASIC also initiated proceedings against Fortnum Private Wealth (**Fortnum**), alleging that Fortnum failed to adequately manage and mitigate cybersecurity risks, particularly concerning its Authorised Representatives (**AR**). These cases build on the seminal case of *ASIC v RI Advice Group Pty Ltd [2022] FCA 496* (**ASIC v RI Advice**), where the Court made a declaration that RI Advice had breached its AFS licence obligations to act efficiently and fairly due to its failure to have adequate risk management systems for managing cybersecurity risks. A brief summary of each of these cases is provided below.

## History of ASIC's focus on cybersecurity

In March 2015, ASIC released **Report 429 Cyber resilience: Health check**, which was a foundational report designed to assist AFS licensees to monitor their cyber risk health. In this report, ASIC emphasises the need for AFS licensees to have adequate risk management systems and resources. Importantly, Report 429 doesn't focus on broader licensing obligations but instead centres on risk and resource adequacy in the context of growing cyber threats. ASIC has recommended that AFS Licensees adopt the recommendations in the NIST Cybersecurity Framework. Since the release of Report 429, ASIC has published regular cyber readiness reports assessing the cyber resilience of market participants and licensees. These reports are based on self-assessment surveys using the NIST Framework and have revealed varying degrees of readiness across the sector.

Together, these reports have laid the groundwork for ASIC's regulatory expectations around cyber resilience, clearly signalling that cybersecurity is not only an essential part of prudent risk management, but failure to identify and manage these risks will be an AFS licence breach and expose the Licensee to substantial fines.

Significantly, these publications pre-date the decision in ASIC v RI Advice and set the stage for the current cases, demonstrating that ASIC will take enforcement action to force compliance.

In addition to commencing prosecutions against FIIG and Fortnum, ASIC has increased its focus on the need for AFS Licensees to look at cyber risk as a significant ongoing licensee obligation.

## Why is cybersecurity a priority for ASIC?

When providing financial services, AFS Licensees have access to confidential and personal information about clients, including identification documents, tax file numbers, and financial details such as bank account and credit card information. This access makes AFS Licensees likely targets for cyber-attacks and cybercrime.

## What are an AFS Licensees obligations regarding cybersecurity?

AFS Licensees are subject to a number of general licence obligations that ASIC has used to initiate proceedings for poor cybersecurity practices. An AFS Licensee has obligations imposed by the Corporations Act (**General Licence Obligations**) namely to:

- do all things necessary to ensure that the financial services covered by the licence are provided efficiently, honestly and fairly (s 912A(1)(a) of the Corporations Act)
- to have available adequate resources (including financial, technological and human resources) to provide the financial services covered by the licence and to carry out supervisory arrangements (s 912A(1)(d) of the Corporations Act)
- ensure that its representatives are adequately trained and competent to provide financial services (s 912A(1)(f) of the Corporations Act), and
- have adequate risk management systems (s 912A(1)(h) of the Corporations Act).

ASIC is using these General Licence Obligations as a basis for arguing that a failure to implement adequate cybersecurity controls is a breach of the obligations to have adequate risk management systems and to provide financial services efficiently, honestly, and fairly. By relying on these broad duties, ASIC has established that cybersecurity risk is not merely a technical issue, but a core element of an AFS Licensee's ongoing legal obligations.

In addition to the Corporations Act obligations, AFS Licensees are also subject to obligations under the *Privacy Act 1988* (Cth) (**Privacy Act**). The Privacy Act imposes general obligations related to notifiable data breaches as well as an obligation on an organisation to take reasonable steps to protect personal information it holds from misuse, interference, loss and unauthorised access or disclosure. This extends to ensuring it has adequate cybersecurity policies in place. AFS Licensees have an obligation to comply with the financial services laws, which includes the Privacy Act.

Reforms introduced since the 2019 findings of the Hayne Royal Commission mean that a failure to comply with certain AFS licensing obligations – including obligations relating to how cyber risks are addressed – may give rise to civil penalties being imposed on AFS Licensees. The cases initiated by ASIC have resulted in substantial fines.

### *ASIC v RI Advice (2022)*

In ASIC v RI Advice, the Federal Court declared that failure to implement adequate cybersecurity risk management systems could constitute a breach of General Licence Obligations under the Corporations Act. RI Advice as an AFS Licensee operated a third-party AR model, authorising independently owned corporate and individual representatives to provide services under its licence.

- Between June 2014 and May 2020, ARs under the supervision of RI Advice suffered nine cybersecurity incidents, many involving phishing, email account takeovers, ransomware attacks and compromised servers that stored sensitive retail client information.
- RI Advice admitted that it lacked adequate risk management and controls up to 15 May 2018 and was slow to act thereafter in implementing cybersecurity programs.
- Prior to May 2018, RI Advice did not have documentation, controls and risk management systems needed to adequately manage cybersecurity risk across its AR network.
- In May 2018, RI Advice implemented a number of ANZ policies that were directed to its structure and IT capabilities, but it failed to fully implement these policies until 2021.
- RI Advice admitted that it was, at all material times, required to identify the cybersecurity and cyber resilience risks faced by its ARs in the course of providing financial services under its licence, and to have in place adequate documentation, controls, and risk management systems to address those risks across its AR network.[1]

Justice Rofe, when imposing a fine of $750,000 on RI Advice, made a declaration that RI Advice contravened the obligation to have adequate risk management systems (s 912A(1)(h)) and that it failed to do all things necessary to ensure that the financial services covered by the licence were provided efficiently, honestly and fairly (s 912A(1)(a)). In doing so, Her Honour stated a number of key principles:

- that AFS Licensees are required to identify the risks that ARs face in the course of providing financial services[2]
- that AFS Licensees must have documentation, controls and risk management systems in place that were adequate to manage risk in respect of cybersecurity and cyber resilience[3]
- the public expect the holder of an AFS Licence to have adequate cybersecurity measures, although the content of the cybersecurity measures are to be assessed by reference to the reasonable person qualified in the area of cybersecurity[4]
- whether cyber risk management systems are adequate requires consideration of the risks faced by a business in respect of its operations and IT environment[5], and
- the courts will assess adequacy of any particular cyber risk management system and will require information from cybersecurity qualified experts.[6]

[1] ASIC v RI Advice, [28].
[2] ASIC v RI Advice, [28].
[3] ASIC v RI Advice, [28].
[4] ASIC v RI Advice, [49].
[5] ASIC v RI Advice, [54].
[6] ASIC v RI Advice, [55].

### *ASIC v FIIG Securities (2025)*

FIIG Securities is an AFS Licensee that offers retail and wholesale clients access to fixed income securities, bonds and managed discretionary accounts. In the course of running its business FIIG Securities collected contact details, dates of birth, identification documents (such as passports), tax file numbers, Australian Business numbers, bank account details, and assets holdings. FIIG Securities suffered a cybersecurity incident where 385 Gigabytes of confidential data was stolen in a malicious cyber-attack, impacting 18,000 clients.[7]

ASIC alleges, that FIIG's failure to have adequate risk management measures was a contravention of ss 912A(1)(h) and 912A(5A) of the Corporations Act. Unlike RI Advice, FIIG Securities did have internal policies; however ASIC alleges that FIIG Securities failed to actually implement the measures listed in these policies. ASIC alleges that this failure to adopt controls to manage and mitigate risks resulted in unreasonable exposure to cybersecurity threats. ASIC has also submitted that FIIG Securities lacked sufficient financial, technological and human resources required to ensure that these measures were in fact implemented.[8]

### *Fortnum Private Wealth (2025)*

Fortnum Private Wealth is an AFS Licensee that authorised a number of ARs. Between January 2021 and September 2022, five of Fortnum's ARs experienced cybersecurity incidents, including compromised email accounts, phishing attacks, and a significant data breach affecting approximately 9,828 clients, whose details ASIC alleges were published on the dark web.

Unlike RI Advice, Fortnum had a Cyber Policy that required all of its ARs to complete a self-assessment questionnaire regarding their cybersecurity and IT setup. ARs were also required to submit an attestation form confirming the cybersecurity measures they had implemented. The Fortum Cyber Policy indicated that Fortnum would annually review each AR to determine whether the cybersecurity strategy was effective; however, this review allegedly did not occur.

ASIC alleges that Fortnum's Policy was inadequate to address its cybersecurity risks, as the measures were vague and overly lenient. Specifically, ASIC alleges that Fortnum breached its General Licence Obligations, for the following reasons:

- The Cybersecurity Policy did not require ARs to consult Fortnum if they answered "no" or "unsure" in their Self-Assessment.
- The Cybersecurity Policy allowed ARs to consult external consultants without verifying those consultants' qualifications.
- The Cybersecurity Policy failed to mandate improvements based on negative or uncertain responses in Self-Assessments.
- The Cybersecurity Policy made key cybersecurity strategies, such as the Essential Eight, optional rather than mandatory.
- Fortnum failed to mandate a minimum level of cybersecurity training, and limited training to content related only to the April 2021 and May 2023 Policies.
- Fortnum failed to implement any cybersecurity-specific supervision or oversight systems.
- Fortnum lacked staff or consultants with cybersecurity expertise, including during the development of the April 2021 Policy.

The proceedings against Fortnum demonstrates the strong position ASIC is willing to take, especially where AFS Licensees authorise multiple ARs. The 'licensee for hire' model has always put the AFS Licensee at risk of compliance breaches, even without the need to ensure the compliance arrangements incorporate robust cybersecurity risk management. ASIC is showing that it expects robust and active supervision and management of Ars especially when there are multiple Ars. AFS Licensees are also required to provide adequate oversight of their Ars and to effectively manage the cybersecurity risks relevant to those Ars and the licensee itself.

---

[7] ASIC Sues FIIG Securities for Systemic and Prolonged Cybersecurity Failures' (Media Release, 23 July 2025) https://www.asic.gov.au/about-asic/news-centre/find-a-media-release/2025-releases/25-035mr-asic-sues-fiig-securities-for-systemic-and-prolonged-cybersecurity-failures/.

[8] Australian Securities and Investments Commission, *Concise Statement: ASIC v FIIG Securities Limited* (Concise Statement, 23 July 2025) <https://download.asic.gov.au/media/0ubnrmym/25-035mr-asic-v-fiig-securities-limited-concise-statement-sealed.pdf> .

## How does an AFS Licensee ensure it meets ASIC's expectations?

So what does an AFS Licensee need in order to ensure that it has adequate cybersecurity management systems and policies?

To ensure cybersecurity management systems and policies are adequate, AFS Licensees need to consider the guidance provided through ASIC's Statement of Claim regarding both FIIG Securities and Fortnum Private Wealth Securities. Some necessary measures include development a Cyber Incident Response Plan, implementing patch updates, establishing detection/ response programming, and conducting vulnerability scanning.

A key element in these cases is the history of cybersecurity-related incidents faced by the AFS Licensees. If an AFS Licensee has experienced multiple cybersecurity incidents, it should urgently review its policies and procedures to ensure they are sufficient. Furthermore, where an AFS Licensee authorises several ARs, that Licensee should also assess the nature and extent of cyber risk faced by those ARs and adopt appropriate oversight mechanisms and group-wide policies. If a policy is to be updated, it should be implemented swiftly.

## Where to next for AFS Licensees?

With three cybersecurity related enforcement actions now brought by ASIC, it is reasonable to assume that more enforcement proceedings are likely to follow. ASIC is not only focusing on AFS Licensees that authorise a large number of ARs but all licensees as seen with ASIC's recent action against FIIG Securities.

ASIC has already announced that enforcement against *'Licensee failures to have adequate cyber-security protections'* is one of its 2025 priorities.[9] It is now essential for AFS Licensees to implement cybersecurity controls to ensure ongoing compliance and protection against future threats.

Our multi-disciplined team can assist with a range of services including working with clients to write and develop their cyber compliance plans, staff training for cyber risk, reviews of existing compliance policies including AR contracts and working with cyber risk experts whose technical expertise is required.

[9] ASIC enforcement priorities | ASIC

# Chantal Tipene appointed to the Information and Privacy Advisory Committee

We are delighted to announce that Chantal Tipene, Partner in our Government Public & Regulatory practice, has been appointed by the Governor of NSW to the Information and Privacy Advisory Committee (**IPAC**).

IPAC plays a key role in supporting the work of the Information Commissioner and the Privacy Commissioner in NSW. It was set up under the Privacy and Personal Information Protection Act 1998 to provide expert advice on how we manage access to information and protect privacy across the State.

IPAC's main focus is helping the Information and Privacy Commission (**IPC**) meet its legal responsibilities and strategic goals. Sometimes, the advice it gives touches on broader human rights issues—like employment, personal freedoms, and ethical concerns—especially as these relate to how information is handled.

At the heart of IPAC's work is a commitment to fairness, transparency, and accountability. These principles guide how NSW approaches information access and privacy, especially as technology and public expectations continue to evolve.

The IPAC also supports efforts to improve how the NSW public sector handles information and privacy—by building leadership, skills, and capability across government.

IPAC is made up of the Information Commissioner, the Privacy Commissioner, and up to six other members who are appointed by the Governor of NSW, based on recommendations from the Minister for Customer Service and Digital Government.

Chantal commented, 'The Committee members bring a wide range of expertise to tackle the unique challenges of our digital age, where service delivery and technology are changing rapidly.  There is no better time to have a seat at the table and I am honoured and excited to have been appointed.'

## Chantal Tipene

Partner in the Government Public & Regulatory team

# **THE CHAIN REACTION:** THIRD-PARTY BREACHES AND THE RISE OF CYBER LITIGATION

Authors: Jehan Mata (Partner), Dinah Amrad (Associate), and Maxwell Watson (Paralegal)

Recent high-profile cyber incidents involving Louis Vuitton and a major Australian airline **(Australian Airline)** have underscored the growing exposure of personal data through routine transactions. These breaches demonstrate a broader trend of sophisticated cybercrime that increasingly targets large organisations via indirect and persistent methods, often exploiting vulnerabilities in third-party systems.

## Supply chain vulnerabilities

The Louis Vuitton breach resulted in the exposure of customers' personal information including names, contact details, and purchase histories. It remains unclear how many customers were affected by the attack, as the breach stemmed from weaknesses in customer relationship management platforms rather than a direct compromise of Louis Vuitton's core infrastructure. Similarly, the Australian Airline breach involved unauthorised access to a third-party contact centre, resulting in the exposure of sensitive data belonging to 5.7 million Australians.

As cyber threats continue to evolve, vulnerabilities with supply chains and outsourced service providers are becoming increasingly critical. These risks demand stronger safeguards and oversight. The legal and operational consequences of such breaches are significant, particularly when organisations fail to implement adequate protections or maintain effective supervision of third-party vendors. Some key takeaways are as follows:

- Organisations must assess and strengthen cybersecurity across their entire supply chain, including third-party platforms and service providers.
- Failure to manage these risks can result in significant legal liability, including regulatory investigations and class actions.
- The growing number of data breach cases has prompted calls for reform. For example, the new serious invasions of privacy tort of privacy, which allows individuals to seek compensation for serious invasions of privacy, even in the absence of a breach of existing legislation.
- Breaches can disrupt business operations, damage reputations, and erode customer trust.
- Cyber insurance and robust vendor management frameworks are essential tools for mitigating exposure and ensuring rapid response to incidents.

This topic was previously addressed in greater detail in our earlier edition, accessible via the following link: Sparke Bytes - June 2025: Sparke Helmore.

## Legal action and regulatory scrutiny

In just three major cyber incidents involving major local companies namely Optus, Medibank, and most recently the Australian Airline, more than 25 million customer accounts have been exposed. This trend highlights the growing scale and impact of data breaches in Australia.

The Australian Airline data breach has prompted a class action filed in July 2025 by Maurice Blackburn, alleging breaches of the *Privacy Act 1988* (Cth). This case marks the latest development in Australia's expanding cyber litigation landscape. While details continue to emerge, the action reflects a rising trend of affected individuals seeking collective legal redress. The claim seeks compensation for those impacted and raises broader concerns about the Australian Airline's data governance and privacy practices.

The Medibank data breach class action is ongoing and stems from the 2022 Medibank incident. The Federal Court has recently ruled on privilege claims concerning investigation reports related to this breach. The class action is being funded by Omni Bridgeway on a no-win, no-fee basis, with Slater and Gordon representing the affected individuals. The case is still developing, with key procedural issues yet to be resolved.

The Optus data breach class action, also arising from a 2022 incident, involves the exposure of personal data belonging to nearly 10 million customers. This matter remains active, along with regulatory proceedings initiated by the Office of the Australian Information Commissioner.

Together, these actions highlight the multifaceted legal consequences of large-scale data breaches.

## Key takeaways

### For businesses

The recent breaches demonstrate the urgent need for improved cybersecurity practices across all sectors. Businesses should actively assess cybersecurity frameworks and data protection strategies, ensuring that third party vendors are subject to stringent contractual obligations. Cyber insurance is an essential safeguard to ensure rapid and effective breach response.

### For insurers

Insurers should closely monitor developments in privacy law and supply chain risk. As regulatory scrutiny intensifies, insurers must refine their understanding of risk and ensure that policy wording adequately addresses indirect exposures.

### For underwriters

The increasing frequency of third-party breaches highlights the need for underwriters to evaluate how insureds manage vendor relationships and data governance.

# THINKING OF GETTING LEGAL ADVICE FROM AN AI ASSISTANT? THINK AGAIN.

Authors: Jason Kwan (Partner) and Ella Sourdin Brown (Law Graduate)

As Artificial Intelligence (**AI**) tools become more accessible, there is the temptation to use publicly available models such as ChatGPT or Google Gemini to seek legal advice. After all, how does it differ from consulting a conventional search engine when searching for an answer or a steer in the right direction?

Unfortunately, using AI as your legal assistant comes with numerous pitfalls you should consider. This is especially the case if you are entering confidential, personal or other commercially sensitive information into the tool. In this article, we explore some of the key risks, including potential inaccuracies, breach of confidentiality, waivers of legal professional privilege and privacy concerns.

## The 'Hallucination' problem

Large language models (such as ChatGPT, Google Gemini and Perplexity AI) are examples of generative AI known for their ability to instantaneously produce large amounts of sophisticated text from minimal prompts. Generative AI operates in a similar way to predictive text, generating responses based on patterns and predictions on what text is statistically likely to follow, rather than verified facts.

This may lead to 'Hallucinations' which occur when AI models produce inaccurate, misleading or sometimes entirely fabricated results. This may include false cases, incorrect legal principles, or even non-existent laws. There are growing numbers of cases of lawyers (even experienced ones) being caught out misusing AI. When using AI for legal research you almost need to work back from the answer in order to validate its accuracy and the sources relied upon.

## AI and the duty of confidentiality

When seeking legal advice, you are usually doing so because a specific set of facts has given rise to a legal issue - facts that you might be tempted to use to prompt the AI.

However, when you are interacting with an AI model, you are not necessarily interacting with someone who is bound by and who you can rely on to observe obligations of confidentiality in the same way as a colleague or a legal advisor would be. Instead, you are engaging with software or an application that may not be able to reliably distinguish between confidential and non-confidential information, increasing the risk of unintended disclosures. Behind that software or application sits a technology vendor that may or may not be technically and contractually restricted in their ability to access information entered into the AI model and that may use the information to further train or improve the model.

Although, some platforms offer deletion features, these are often limited due to the "black box" nature of AI (and may only involve the deletion of chat history or account information). Much like the human brain, once information is absorbed by the AI, it becomes deeply embedded and difficult, if not impossible, to fully erase. This is especially the case if the data has been used to train the model.

There is also the risk that any data you input into an AI model could be disclosed under certain legal circumstances, such as a court order. Recently in the United States, the Federal Court ordered 400 million chat logs (including deleted chat logs) to be disclosed to the court as part of discovery in a case brought by the New York Times against Open AI.[10]

It is best to assume that feeding an AI model with information is akin to putting it in the public domain. Waiving legal professional privilege

[10] Bankston, K. (2025, June 25). In ChatGPT case, order to retain all chats threatens user privacy. Center for Democracy and Technology. Retrieved from https://cdt.org/insights/in-chatgpt-case-order-to-retain-all-chats-threatens-user-privacy/

## Waiving legal professional privilege

Legal professional privilege protects confidential communications and documents between a lawyer and their client from mandatory disclosure. Such communications or documents must be made for the dominant purpose of providing legal advice or professional legal services or for use in current or anticipated litigation. Legal professional privilege also applies to in-house lawyers who must show the document was brought into existence in the course of the performance of the lawyer's professional role. The rationale for legal professional privilege is that clients must be able to communicate openly and freely with their lawyer.

However, privileged communications must remain confidential. Privilege can be waived by the client by acting in a way inconsistent with preserving the confidence of a communication. This might include where the client discloses the information into a publicly available AI model.

The Victorian Legal Services Board has issued a statement saying that lawyers cannot safely enter confidential, sensitive or privileged client information into public AI chatbots/copilots (like ChatGPT), or any other public tools. If lawyers use commercial AI tools with any client information, they need to carefully review contractual terms to ensure the information will be kept secure.[11]

## Providing personal information to an AI model?

Specific privacy concerns arise when entering personal information (i.e. information that can identify an individual such as names, addresses, phone numbers, dates of birth or various health related information) into an AI model.

Under the *Privacy Act 1988* (Cth), personal information may only be used and disclosed for the purpose for which it was collected (primary purpose) or for a secondary purpose if the individual has consented or would reasonably expect the use or disclosure for the secondary purpose and that secondary purpose is related to the primary purpose. Consent may therefore need to be obtained before disclosing personal information to an AI model, especially where the personal information is used for training purposes.

In addition, an organisation may need to ensure that sufficient contractual protections are in place with the AI vendor if personal information is transferred outside of Australia. Likewise, organisations should conduct adequate due diligence to ensure the security of the AI product, including an assessment of security measures implemented by the vendor to protect against threats and cyberattacks.

As a matter of best practice, the OAIC recommends that organisations do not enter personal information, and particularly sensitive information, into publicly available generative AI tools, due to the significant and complex privacy risks involved.

## Conclusion

So, the next time you consider getting legal advice from your AI assistant, think again. Or at least, think about what information you are disclosing, who you are really disclosing it to and what risks you might be exposing yourself to.

[11] Victorian Legal Services Board and Commissioner, Statement on the Use of Artificial Intelligence in Australian Legal Practice (Web Page, 6 December 2024) https://www.lsbc.vic.gov.au/news-updates/news/statement-use-artificial-intelligence-australian-legal-practice

# **AI IN THE SUPPLY CHAIN:** THE WEAKEST LINK FOR CORPORATE DATA PRIVACY

Authors: Jason Kwan (Partner), Stefanie Constance (Associate) and Nicholas Chan (Associate)

Artificial intelligence (**AI**) is increasingly being integrated into supply chain operations, from procurement and forecasting to logistics and vendor management.[12] AI models are often trained on vast datasets, which may include personal information, to function effectively. Global supply chain leaders such as Amazon, Nestle and Unilever[13] are already experimenting with AI in their internal business processes, although large-scale deployment is still limited.[14]

While the benefits in terms of operational efficiencies gained from AI are clear, the associated risks are equally stark. Regulators have warned that supply chain partners may represent the 'weakest link in data protection[15], stressing that organisations must 'pass on their obligations… in any contract with third parties'.[16] Smaller suppliers are increasingly becoming prime targets for threat actors, serving as an entry point into larger organisations.[17] Recent incidents have demonstrated that a breach at a vendor, even one not central to an organisation's supply chain, or AI provider can quickly escalate to expose sensitive customer or employee data on a much larger scale.[18]

This concern is underscored by ASIC's **Cyber Pulse Survey 2023**, which found that 44% of small organisations do not conduct risk assessments on their third-party vendors.[19] For larger corporates who rely heavily on third-party vendors, this creates a double vulnerability. They face direct cyber threats and may also be exposed through supply chain partners that fail to meet even baseline risk management practices.[20] In an environment where threat actors deliberately target the weakest link, vulnerabilities in a third-party vendor's controls can become an entry point for breaches that ultimately compromise the data of much larger organisations.[21]

## Legal obligations and accountability

Australian privacy laws make it clear that an organisation cannot outsource its privacy obligations. Under the *Privacy Act 1988* (Cth) (**Privacy Act**) entities remain responsible for protecting personal information, even if that information is held or handled by a supplier.

In practice, if an Australian company engages an AI analytics provider and shares personal information with it, the company is still deemed to "hold" that information where it retains possession or control over that information and must take reasonable steps to protect the information from misuse, interference and loss. Therefore, a company may be in breach of Australian Privacy Principles even where the unauthorised access or disclosure of information is due to the third party supplier's failure.

---

[12] Oracle, Benefits of AI in Supply Chain (Web Page, Oracle, 11 January 2024) https://www.oracle.com/scm/ai-supply-chain

[13] Cem Dilmegani and Sıla Ermut, Top 13 Supply Chain AI Use Cases with Examples in 2025 (Web Page, AIMultiple, 12 June 2025) https://research.aimultiple.com/supply-chain-ai/.

[14] The Hackett Group, Supply Chain AI Adoption Rising Amid Economic Pressures (Media Release, 4 April 2025) https://www.thehackettgroup.com/the-hackett-group-supply-chain-ai-adoption-rising-amid-economic-pressures/.

[15] The Guardian, "Third-Party Providers a Customer Data Weak Spot, Australian Privacy Commissioner Says" (6 May 2024) https://www.theguardian.com/australia-news/article/2024/may/06/third-party-providers-a-customer-data-weak-spot-australian-privacy-commissioner-says.

[16] Ibid.

[17] Nick Martindale, "The Risks of Supply Chain Cyberattacks on Your Organisation" (Information Age, 3 February 2025) https://www.information-age.com/the-risks-of-supply-chain-cyberattacks-on-your-organisation-123514230/ accessed 14 August 2025.

[18] Cyber Management Alliance, Snowflake, Ticketmaster & Santander Breaches: A Live Timeline (Cybersecurity Blog, 5 June 2024) https://www.cm-alliance.com/cybersecurity-blog/snowflake-ticketmaster-santander-breaches-a-live-timeline accessed 14 August 2025.

[19] Australian Securities and Investments Commission, "Report 776: Spotlight on Cyber – Findings and Insights from the Cyber Pulse Survey 2023" (13 November 2023) 6 https://asic.gov.au/regulatory-resources/find-a-document/reports/rep-776-spotlight-on-cyber-findings-and-insights-from-the-cyber-pulse-survey-2023/.

[20] Aon, AI-Driven Cyber Attacks and Supply Chain Vulnerabilities Escalate Risk Landscape in Australia (Web Page, Aon, 31 July 2025) https://www.aon.com.au/australia/newsroom-2025/ai-cyber-attacks-supply-chain-risk-report

[21] evo, Supply Chain Attacks: Infiltrating Organizations Through the Backdoor (Blog Post, 28 August 2024) https://www.devo.com/blog/supply-chain-attacks-infiltrating-organizations-through-the-backdoor.

The Office of the Australian Information Commissioner (**OAIC**) has reinforced this position stating after a series of multi-party breaches that outsourcing data processing 'does not negate an organisation's privacy and notification obligations.'[22] If personal information is compromised, the original organisation is still required to notify affected individuals and the OAIC under the Notifiable Data Breaches scheme, regardless of where the incident occurred.[23]

These obligations extend beyond Australia's borders. AI vendors are frequently located overseas meaning Australian companies often disclose data internationally. Under APP 8, before disclosing personal information offshore, organisations must take reasonable steps to ensure the recipient will handle the information consistently with the APPs. Limited exceptions apply where informed consent is obtained from the individual or if the data is disclosed to a recipient in a jurisdiction with substantially similar privacy protections.[24]

### Practical steps for organisations

Given the heightened risks associated with the use of AI, organisations should prioritise governance around AI in the supply chain. Practical measures include:

1. **Enhanced due diligence.** Ask suppliers whether they (and potentially other third parties in their extended supply chain) use AI in providing their services, where data is stored, how it is handled, and whether personal information is retained or used to train AI models. Conduct privacy impact assessments before engaging high-risk AI vendors. Continue to monitor vendors on an ongoing basis to identify material changes.
2. **AI-specific clauses.** Require suppliers to disclose AI use, restrict the use of personal information from being used for training without consent, and require prompt notification of data breaches. Contracts should also provide audit rights, address retention and destruction of data and allow termination for unauthorised AI use.
3. **Cross-border safeguards.** Confirm where AI vendors store and how they handle personal information. If disclosure offshore is involved, ensure contracts require compliance with the APPs or that the vendor is bound by substantially similar privacy standards.
4. **Data minimisation.** Share only the personal information necessary for the service and prefer anonymised or de-identified data where possible. Sensitive information should not be entered into public AI tools.
5. **Ongoing monitoring.** Build AI vendor oversight into risk management frameworks. Require periodic security reports, review certifications and test incident response plans involving key suppliers.

## Conclusion

As businesses increasingly adopt AI across their supply chains, privacy obligations do not diminish, they intensify. Smaller vendors and overseas AI providers can quickly become the entry point for major breaches. Australian Regulators have made it clear that organisations remain accountable for how their suppliers handle data, meaning that boards can no longer ignore third-party and AI-specific risks. By identifying AI in the supply chain as a potential weak link and strengthening contractual governance and due diligence practices accordingly, organisations can better protect personal information.

[22] Office of the Australian Information Commissioner, Guide to Securing Personal Information (5 June 2018) https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/guide-to-securing-personal-information.
[23] Ibid.
[24] *Privacy Act 1988* (Cth) s 16C.

# A NEW APPROACH TO PRIVACY GOVERNANCE: THE PRODUCTIVITY COMMISSIONER'S RECOMMENDATION FOR AN OUTCOMES-BASED PRIVACY REGULATION

Authors: Hamish Fraser (Partner) and Jasmine Thai (Lawyer)

The average productivity growth in Australia over the decade to 2020 was the slowest in 60 years.[25] To address this slowdown and reverse the trend the Australian Government has tasked the Productivity Commissioner (**PC**) to produce five inquiries into key policy areas the Government should focus on.

On 5 August 2025, the PC released an interim report on one of these five inquiries, specifically addressing actionable recommendations related to Harnessing Data and Digital Technology (**Interim Report**).

Technology is a key driver for innovation, efficiency, and growth in the economy. However, alongside the opportunities and benefits it provides, there are also potential risks that must be considered. It is therefore not surprising that one of the five PC inquiries focuses on technology and the balancing exercise Government needs to perform regarding privacy regulation. The balance is necessary to ensure consumer trust with appropriate guardrails in place while not stifling the innovation or adoption of emerging technologies.

The Interim Report delivered seven draft recommendations for consultation, focusing on four key areas in technology. This article specifically examines the third key area: 'supporting safe data access and use through an alternative compliance pathway for privacy.'

The PC have provided two recommendations in relation to the *Privacy Act 1988* (Cth) (**Privacy Act**), being:

1. **amend** the Privacy Act to create for an **alternative compliance pathway** for entities to comply with their obligations by meeting criteria that is outcome based as opposed to controls-based rules (**recommendation 3.1**), and
2. **do not amend** the Privacy Act to introduce **a right to erasure (recommendation 3.2).**

## Recommendation 3.1: Alternative Compliance Pathway

**The first recommendation the PC has proposed is an alternative compliance pathway.** This would allow flexibility for businesses to choose the most appropriate and effective ways to protect the privacy of its customers in a way that is targeted and fit for purpose.

The PC has commented that certain requirements under the Privacy Act are focused on specific controls - such as certain mandated procedures like consent, notification, and disclosure requirements - that result in a 'tick-box' exercise, failing to adequately meet the protections the Privacy Act intends to achieve.

For example, APP 1 requires entities to have an up-to-date privacy policy and specifies what information needs to be included. However, the PC suggests that the overload of information does not achieve its intended result of informing consumers. the ACCC found that '*If Australian consumers were to read all of the privacy policies they encounter in full, it would take nearly 46 hours every month*.'[26]

[25] Treasury, Intergenerational Report 2023, Australia's future to 2063, pg. 81 Intergenerational Report 2023

[26] Productivity Commissioner, 2025, Interim Report: Harnessing data and digital technology, pg. 57 Interim Report - Harnessing data and digital technology - Productivity Commission

The PC is therefore advocating flexibility for businesses to have the discretion to meet regulatory requirements that effectively caters to their specific customers and business needs. Privacy protections can vary significantly among different business models; what a small and medium business enterprise considers for privacy protections differs from a well-known corporation. The PC argues that there is no 'one size fits all' solution, so the privacy laws should be flexible to reflect these differences.

The PC is consulting on what an alternative compliance pathway might look like and has provided two potential frameworks:

1. outcomes-based obligations could be framed as a defence so if entities are not compliant with certain requirements, they are still able to rely on the defence to show they have achieved the intended privacy protections, or
2. establishing an alternative compliance pathway that is focused on outcome-based requirements.

This approach differs from the recommendations put forward for tranche 2 reforms of the Privacy Act, which introduced a 'fair and reasonable test'. The fair and reasonable test adds to businesses' current obligations and the PC argues that its recommendation does the opposite, offering a reduction in business obligations.

However, measuring what a successful outcome-based model is and enforcing it may present challenges. Some suggestions the PC has provided include:

a. an obligation on businesses to have the **best interest** of its the customers in relation to privacy
b. **having regard** to a consumer's **best interest** when making privacy decisions, or
c. or imposing a **duty of care** to take reasonable steps to mitigate future harms.

The PC's recommendation encourages the Government to explore alternative pathways that achieve effective privacy outcomes for consumers while simultaneously reducing unnecessary burdens on businesses.

### Recommendation 3.2: Right to Erasure

The PC has recommended against a proposed tranche 2 reform, where consumers would have the 'right to erasure.' This has been adopted from the European Union's privacy laws, General Data Protection Regulation (**GDPR**), where the 'right to be forgotten' gives power to the consumer to request a business to erase their information.

During the consultation for the Privacy Act review, businesses expressed concern regarding the impracticalities of implementing this right, against what quantifiable benefits this could provide to consumers. The PC noted that most businesses were concerned with the technical difficulties and changes required to ensure all of a customer's data has been deleted from their systems.

The introduction of the right to erasure could place further unnecessary regulatory burden on industry, where there are already existing requirements under the Privacy Act like APP 11 that require entities to take reasonable steps to destroy or deidentify personal information that is no longer needed.

The PC referenced and agreed with industry comments from the Privacy review, emphasising that there should be great caution when deciding to implement the right to erasure. They noted that the practice implications and costs for businesses should be weighed against the potential benefits for consumers.

## Conclusion

The PC is currently consulting on these recommendations, with a final report expected to be submitted to the Australian Government is aimed to be provided in December of this year. The recommendations and concerns raised by the PC are likely be contentious point during consultation on the tranche 2 reforms.

# AI@WORK: PARLIAMENTARY REPORT RECOMMENDS AMENDMENTS TO THE *FAIR WORK ACT 2009* (CTH) TO BAN THE USE OF AI

**Felicity Edwards, Partner, and Elijah Royal, Associate, examine the rapid development and uptake of AI and ADM in the workplace and consider the positive and potentially negative impacts for workers.**

Artificial intelligence (AI) tools like ChatGPT, Claude AI, Gemini AI, DeepSeek, Microsoft Copilot, and Meta AI are widely available in Australia, sparking ongoing debate around their safety, reliability, privacy, and data protection.

Automated decision-making (**ADM**), powered by AI, is also on the rise—seen in technologies like mobile phone detection cameras and airport SmartGates using facial recognition.

As AI and ADM become more integrated into daily life, regulatory frameworks are slowly emerging. For instance, affidavits filed in the NSW Supreme Court must now disclose if AI was used. However, workplace use of AI and ADM remains largely unregulated, though changes may be on the horizon.

## The Future of Work report

In April 2024, the House Standing Committee on Employment, Education and Training was tasked with investigating and reporting on the rapid development and uptake of AI and ADM in the workplace. On 11 February 2025, after receiving 66 submissions and holding 11 public hearings, the Committee tabled *The Future of Work* report in Federal Parliament. The report makes 21 recommendations focused on:

- Maximising the benefits of AI and ADM in the workplace, including increased support for employers and employees as well as strengthening workforce capabilities.
- Addressing specific risks associated with AI and ADM, such as work health and safety issues and intellectual property concerns.
- Managing high-risk AI systems in workplaces and supporting proposed guardrails.
- Clarifying legal obligations for developers and deployers (employers) of ADM and AI systems as they apply to workplaces.
- Enhancing employee protections, particularly regarding data and privacy, including protections against excessive and unreasonable workplace surveillance, and safeguarding equality and inclusivity.
- Requiring meaningful consultation, transparency, accountability and procedural fairness in the use of AI and ADM.
- Developing public information campaigns to build trust in these technologies and improve understanding of the relevant frameworks for safe and responsible use.

# BUILDING A FENCE AROUND THE DIGITAL PLAYGROUND: AUSTRALIA'S CHILDREN'S ONLINE PRIVACY CODE EXPLAINED

Author: Jason Kwan (Partner) and Ella Sourdin Brown (Law Graduate)

An increase in online privacy risks for children has prompted the Office of the Australian Information Commissioner (**OAIC**) to develop a Children's Online Privacy Code (**Code**). The OAIC's mandate to do so was established under the *Privacy and Other Legislation Amendment Act 2024* (Cth), and the Code has just finished undergoing a second round of consultation.

This article examines the development of the Code, including the concerns driving its creation, its intended scope, the challenges identified during the consultation phase, and how the United Kingdom's regulatory approach is likely to influence it.

## Digital risks to children

The push for a Code is a response to research findings that reveal increasing online digital risks for children. A vast amount of personal information is collected from children from an early age; estimates suggest that by the time a child reaches 13 years of age, 72 million data points may have been gathered about them.[27] This widespread data collection has prompted the Government to develop the Code, with the consultation paper stating that *"Existing privacy laws have not kept pace with these changes in digital engagement or the scale of data collection."*[28]

## Origins of the Code

The timeframe for implementing the Code involves a three-stage consultation process, detailed as follows:[29]

- **September 2023: Privacy Act Review Report** released, including a proposal to introduce a Code.[30]
- **September 2024:** *The Privacy and Other Legislation Amendment Bill 2024* (Cth) was introduced.
- **December 2024:** the Bill was passed, becoming an Act.
- **January 2025 (Phase 1):** OAIC consults with children, parents and organisations focused on children's welfare.
- **May 2025 (phase 2):** OAIC engages civil society, academia, and industry stakeholders, to gather insights and perspectives on application of the Code and relationship with the APPs.
- **June 2025:** OAIC releases **'Children's Online Privacy Code' issues paper**[31], seeking stakeholder input.
- **July 2025:** Submissions close for the OAIC's issues paper.
- **Early 2026 (Phase 3):** Proposed release of the draft Code and third and final public consultation.[32]
- **December 2026:** Proposed finalisation and roll-out of Code.

[27] Office of the Australian Information Commissioner, *Children's Online Privacy Code Issues Paper* (Issues Paper, 12 June 2025).
[28] Ibid.
[29] Association for Data-Driven Marketing and Advertising, The Privacy Series: The Children's Online Privacy Code (Web Page, 2025) https://www.adma.com.au/resources/privacy-series-childrens-online-privacy-Code.
[30] Attorney-General's Department, Privacy Act Review Report (Report, 16 February 2023).
[31] n 27.
[32] s 26GC(9) of the *Privacy and Other Legislation Amendment Act 2024* (Cth)

## Scope and applicability across sectors

The Code is not intended to prevent children from engaging in the online digital world; rather its purpose is to protect their personal information in the digital space through enhanced privacy protections. Although the draft Code has not been released yet, based on the issues paper, it is expected to specify how certain services accessible by children must comply with the Australian Privacy Principles (**APPs**) under the *Privacy Act 1988* (Cth).

The Code applies to businesses and organisations that provide 'Services likely to be accessed by Children', 'Social Media Services', 'Electronic Services' and 'Designated Internet Services' as defined in the *Online Safety Act 2021* (Cth) (**Online Safety Act**). It also extends to any entity that is subject to the APPs or falls within a class of entities governed by these principles. However, it is important to note that the Code does not apply to entities providing health services, although it may apply to those offering health-related fitness or wellbeing apps and services.[33] This drafting aims to ensure flexibility by encompassing a wide range of entities while allowing the Code to specify which entities are exempt from its provisions.[34]

The **OAIC's issues paper** provides insights arising from the OAIC's previous consultation stage. These learnings, likely to inform the objectives of the Code, are summarised below:[35]

**Concerns about privacy and call for stronger protections:** the need to involve children in decisions about data use.

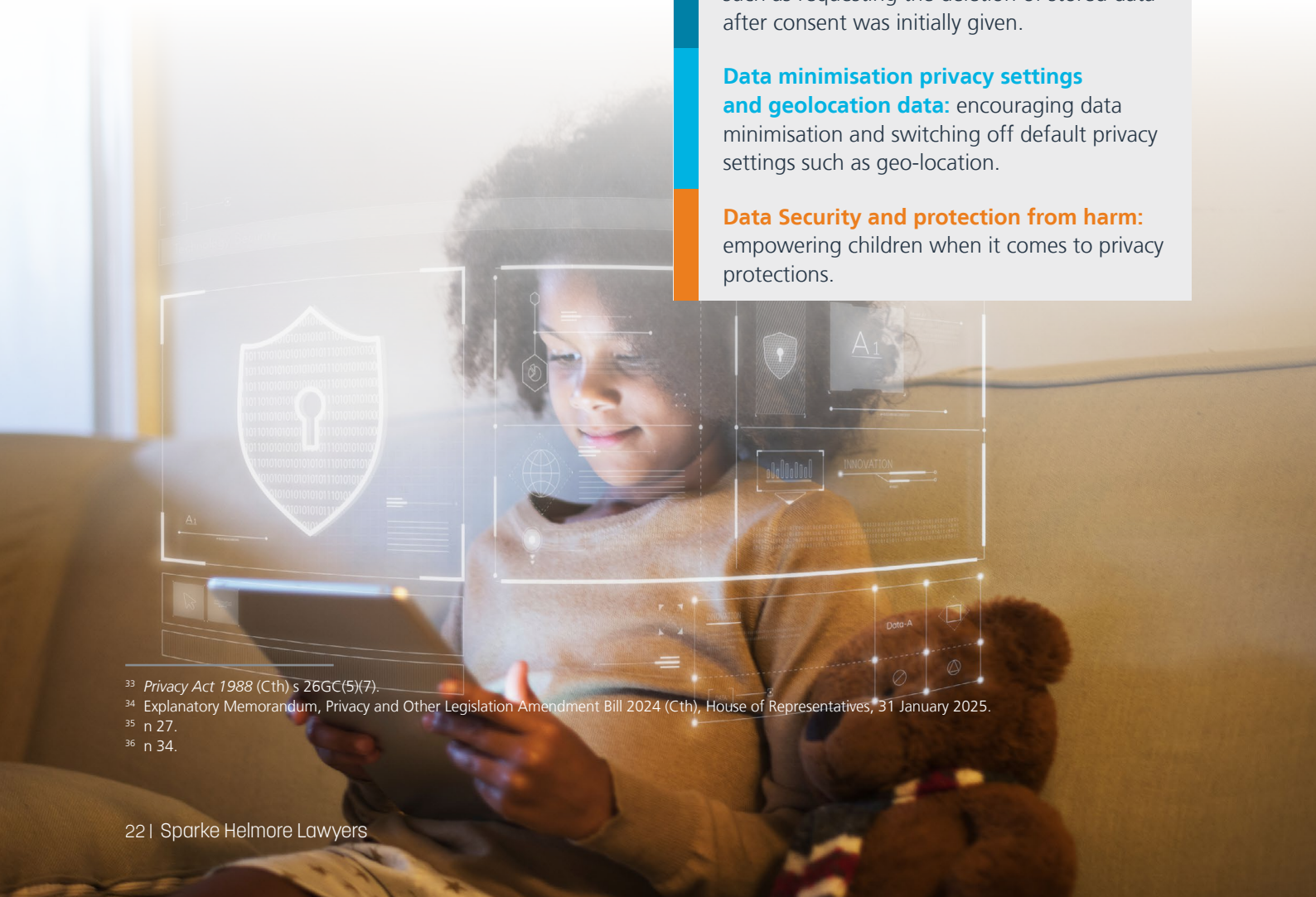
**Transparency and age-appropriate communication:** the Code should be published in plain language, have age-appropriate terms and conditions and transparent remediation processes, especially in relation to targeted advertising.

**Informed consent and digital literacy:** ensuring children are given opportunities to express meaningful consent and are educated on digital literacy (for example, encouraging the use of graphics, video and audio content rather than relying on written communication).[36]

**Control over personal information and privacy:** services should enable children to change their mind when it comes to consent, such as requesting the deletion of stored data after consent was initially given.

**Data minimisation privacy settings and geolocation data:** encouraging data minimisation and switching off default privacy settings such as geo-location.

**Data Security and protection from harm:** empowering children when it comes to privacy protections.



[33] *Privacy Act 1988* (Cth) s 26GC(5)(7).
[34] Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 (Cth), House of Representatives, 31 January 2025.
[35] n 27.
[36] n 34.

The Code will function as an enforceable APP code that outlines how protections in the APPs are to be applied or complied with in relation to the privacy of children.[37] The Code is likely to be based on the UK's 'Age-Appropriate Design Code' (the **UK Code**), which comprises 15 standards.[38] The most important of these standards codifies the 'Best Interests Principle'.

The Best Interests Principle restricts the use of children's data to situations where it is in their best interests. It requires this principle to be the primary consideration when designing and developing, apps, games, websites and other platforms likely to be accessed by children.[39] The other standards of the UK Code outline the types of conduct entities can engage in to ensure children are better protected online. These include 'turning off' default settings that do not protect privacy and prohibiting practices by corporations that could harm the wellbeing of children. The Code may also introduce the 'right to be forgotten', allowing individuals to request deletion of their data upon turning 18.[40] Although this right already exists in the UK for **all** individuals, if implemented in Australia under the Code, it will only apply to children's data.

## Scrutiny from stakeholders

Phase two of the consultation process concluded on 31 July 2025. Stakeholders were asked questions about:

- The scope of services that should be covered by the Code
- When and how the Code should apply to APP entities
- Age-range specific guidance
- APP specific questions including transparent management of personal information, anonymity and pseudonymity, consent mechanisms, marketing restrictions, security requirements, international interoperability, and access and correction to personal information

Several organisations have made their submissions publicly available. These submissions reveal that while some industry participants support stronger privacy protections for children, they also want to ensure that compliance obligations are proportionate to the risks involved. Such a stance is evident from submissions that support protection for children online, but urge the OAIC to ensure that the compliance obligations will reflect actual risk and avoid interference with commercial operations such as insurance.[41] Other submitters contend that the Code applies too broadly, and proposes that OAIC explicitly exclude some APP entities from the scope of the Code at the outset so there is clarity around its application.[42] In addition, there have been recommendations around how the likely to be accessed by children (**LTBA**) test should be operationalised for online services.[43] Currently, the Act, specifies that it will be up to the Commissioner to make written guidelines to assist entities in determining if a service is likely to be accessed by children, which aligns with the UK's LTBA test.[44]

[37] n, 34.
[38] Information Commissioner's Office (UK), *Age Appropriate Design: A Code of Practice for Online Services – Best Interests of the Child* (Web Page, 2025) https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-Code-guidance-and-resources/age-appropriate-design-a-Code-of-practice-for-online-services/1-best-interests-of-the-child/;
[39] Normann Witzleb et al, Privacy Risks and Harms for Children and Other Vulnerable Groups in the Online Environment (Research Report, Office of the Australian Information Commissioner, 18 December 2020) https://www.oaic.gov.au/__data/assets/pdf_file/0012/11136/Report-Privacy-risks-and-harms-for-children-and-other-vulnerable-groups-online.pdf.
[40] ABC Radio National, *Could Aussie Kids Be Given the "Right to Be Forgotten" Online?* (Life Matters, 17 August 2025) https://www.abc.net.au/listen/programs/lifematters/could-aussie-kids-be-given-the-right-to-be-forgotten-online-/105609052.
[41] Insurance Council of Australia, Submission to the Office of the Australian Information Commissioner: Children's Online Privacy Code (28 July 2025) https://insurancecouncil.com.au/wp-content/uploads/2025/07/ICA-Submission_-Childrens-Online-Privacy-Code.pdf.
[42] Business Council of Australia, Submission in Response to the Children's Online Privacy Code Issues Paper (July 2025) https://assets.nationbuilder.com/bca/pages/13131/attachments/original/1753925863/BCA_Submission_-_Children's_online_Code_issues_paper.pdf?1753925863.
[43] Reset.Tech Australia, Likely to Be Accessed: Children's Data and the Case for a Privacy Code (2025) https://au.reset.tech/uploads/likely-to-be-accessed.pdf.
[44] S 26GC(11) *Privacy and Other Legislation Amendment Act 2024* (Cth)

## Broader public initiatives shaping the national conversation on children's online privacy

The development of the Code forms part of a broader government effort to address online harms. The OAIC will be consulting with the eSafety Commissioner and National Children's Commissioner before registering the Code.[45] Consequently, broader public initiatives will be important to the Code's formation. Some of these initiatives have included:

- The ongoing development and implementation of Online Safety Codes and standards [46]:
- The 'Minimum Age for Social Media Access' (the **Ban**), effective December 2025. While distinct from the Code, the Ban targets similar platforms such as those enabling user interaction and content sharing. The government has confirmed that platforms like Facebook, Instagram, TikTok, and X will be included. Unlike the Code, the Ban is unlikely to apply to platforms focused on gaming, messaging, product or service information, professional networking, education, or health services.[47]
- A **review of the Online Safety Act** has been released. Key to the review was assessing whether there should be a 'digital duty of care' for platforms to ensure user safety.[48]
- eSafety initiatives, such as **Safer Together!** and **Leaving Deadly Digital Footprints!** Have been developed specifically for Aboriginal and Torres Strait Islander children and their carers.

## Conclusion

While the final form of the Code and the factors informing its development are beginning to take shape, offering insight into its potential operation and scope, some elements remain unclear. What we know for now is that the OAIC plans to release a draft Code in early 2026 for at least 60 days of public consultation, with the aim of having the Code in place by 10 December 2026.

If you missed out on the previous consultation period that closed on 31 July 2025, we recommend participating in this third and final consultation phase.[49]

[45] n, 34.
[46] Issued under Part 9, Division 7, of the *Online Safety Act* (2021) (Cth).
[47] Josh Taylor, *How Australia's Under-16s Social Media Ban Will Be Enforced – and Why TikTok, Instagram and Facebook May Be Exempt* (The Guardian, 1 August 2025) https://www.theguardian.com/technology/2025/aug/01/how-australia-under-16s-social-media-ban-enforced-tiktok-instagram-facebook-exempt-platforms; Katina Curtis, Anthony Albanese Takes Kids' Social Media Ban, Now Including YouTube, to the World Stage (The Nightly, 29 July 2025) https://thenightly.com.au/politics/anthony-albanese-takes-kids-social-media-ban-now-including-youtube-to-the-world-stage-c-19520729.
[48] Michelle Rowland, Report of the Online Safety Act Review Released (Media Release, Minister for Communications, 4 February 2025) https://minister.infrastructure.gov.au/rowland/media-release/report-online-safety-act-review-released.
[49] eSafety Commissioner, Online Safety (Web Page, 2025) https://www.esafety.gov.au/.

# PRIVACY AND CONSUMER DATA RIGHTS: STRIKING THE RIGHT BALANCE

Author: Hamish Fraser (Partner)

Privacy laws in Australia have governed the collection and use of personal information in the private sector for over 20 years. In that time, the concepts of privacy have become well understood, thanks in no small part to the recent high profile data breaches and legislative reforms. [link to earlier articles on reforms].

In parallel with the increasing focus on protecting personal information though, there has been the recognition that the ability to share data between businesses has the ability to allow improved competition, by allowing consumers to compare products and switch between providers more easily.

That ability to share data became known as the Consumer Data Right (**CDR**). The Federal Government announced its intention to introduce a CDR regime in 2017, with the legislation introduced in 2019. Initially, the CDR was introduced into the banking sector, commonly referred to as Open Banking. After banking the Energy Sector was included in the CDR in 2021.

The reforms were hailed as world leading, recognising the need for striking a careful balance between the risks and the benefits.

In 2023, the Federal Government paused the roll out of the CDR to the telecommunications and insurance sectors to allow the system to 'mature' They also engaged in a consultation process, which ended on 9 September 2024 proposing changes to simplify the consent process in order to reduce the barriers to participation in the CDR.

## Overlap with Privacy and CDR Safeguards

To manage the risks associated with transferring large amounts of consumer data (much of which will also be personal information) the Federal Government, in conjunction with the OAIC, developed the Privacy Safeguards.

These safeguards are generally consistent with the APPs although are more restrictive and detailed than their equivalent APPs, with a broader application, to catch all data and bind data recipients in respect of the CDR data they receive. These stronger protections are needed to manage the risks associated to the more convenient and higher frequency of transfers under the CDR, ensuring consumer confidence.

## OAIC's recent decision

A recent decision was handed down by the Privacy Commissioner, marking the first CDR determination, and gives colour to the levels of care to be taken when handling CDR data, and by extension,, personal information.

The Commissioner found that that Regional Australia Bank Limited (**RAB**) had breached Privacy Safeguard 11, which mandates data holders to take reasonable steps to ensure CDR data is accurate, up to date and complete in relation to the purpose for which it is held.

In this case, RAB subcontracted with Biza to assist in meeting some of its secure storage obligations - an approach common for outsourcing data handling of this kind.

RAB's contract with Biza was aimed at ensuring compliance with its CDR data holder obligations. However, Biza had a software issue that resulted in data mingling, leading to incorrect data being supplied to a third parties.

The Privacy Commissioner found that:

*Biza ought to have taken steps to ensure that the software issue impacting the accuracy of CDR data was not introduced in the CDR environments of its other clients.*

*Biza could have reasonably done so by ensuring that the patched software was implemented in all upgrades, including those in pre-production, thereby mitigating the risk of co-mingling further CDR data.*

*Checks ought to have been undertaken prior and subsequent to future software upgrades.*

*Such steps were reasonable in circumstances where:*

a. *Biza had a relatively small client base, noting that the respondent was Biza's oldest client[34]*

b. *they were not impracticable or cost prohibitive*

c. *the consequences of not taking such steps had the potential to cause significant harm for affected CDR consumers.*

Furthermore, the Commissioner found that despite the standard contractual language stating (that Biza was not an agent of RAB, Biza was considered an agent for the purposes of the legislation. Consequently, RAB was held responsible for the failings of Biza, even though it had no knowledge of them.

While the question of agency is perhaps unique to the CDR regime and may not apply similarly to an APP entity that does not hold CDR data, this finding is important for understanding and analysing the failings of Biza, and the standards to which data holders under a contract will be held.

### Productivity Commissioner weighs in

In an example of the complexities involved in collecting, using, and storing data, the Productivity Commissioner (**PC**) released an interim report on 5 August, following an enquiry into harnessing data and digital technology. [link to other story and modify this para maybe].

This interim report included several draft recommendations, particularly relevant to the CDR. One key recommendation is to support safe data access through new pathways that offer greater flexibility and lower costs in relation to implementation.

The PC has proposed draft recommendation 2.1, which aims to establish lower-cost and more flexible regulatory powers that would expand basic data access for individuals and businesses. Some considerations it provided included:

1. **industry-led data access codes** that allow consumers to export non-sensitive data on a regular basis through snapshots.
2. **standardised data transfers** that is assisted by government to achieve a formalise minimum technical standards to support use cases requiring high-frequency data transfers and interoperability.[50]

The PC is currently consulting on these new pathways to increase uptake of basic data access for consumers, while allowing for flexible and lower cost implementations for businesses.

### Conclusion

The obligations on data holders have become increasingly complex, and the standard of care they must uphold is high. It is essential to give careful consideration to the precise contractual obligations and the need to understand the performance of them, beyond just contractual language.

[50] Productivity Commissioner, 2025, Interim Report: Harnessing data and digital technology, pg. 39 Interim report - Harnessing data and digital technology

# INSURING YOUR TECHNOLOGY CONTRACTS

Author: Hamish Fraser (Partner) and Jon Tyne (Partner)

Technology contracts often contain a clause that mandates some form of insurance. Clauses such as this can often be a legacy from a less digital age. Do such clauses have a place in the modern technology contract and, if so, what should they say?

This article looks to address both the meaning of some of the "older" style clauses, addresses a few common misconceptions and considers what sort of clause a modern digital contract might benefit from.

## Why require insurance at all

It is perhaps trite to point out that a business takes out an insurance policy to manage risk. But why does an insurance clause find its way to a contract. What is it there for and what should it oblige a party to do?

A prudent acquirer of digital services (the customer) should look to ensure its suppliers will survive misfortune – whether a business interruption, a claim from the customer (or the suppliers' other customers) or other business shock. Following that logic, it is also therefore prudent for the customer to ask to know, or perhaps even mandate, what insurance the supplier should have.

Sometimes it is possible or even necessary for a particularly large project to have specific insurance (e.g., to take an extreme example, a satellite launch). However mostly the purpose of the insurance clause is to know and understand what protections the supplier has or should have to perform the work that is to be delivered.

One function of such clauses is to mitigate contract risks that can be insured against – for example, the risk that a supplier, which fails to meet its duties, has no assets to meet a claim by the customer. However another important purpose of the requirement to insure is to ensure (so far as possible) the supplier will remain financially viable and able to continue providing services.

Insurance clauses, like so many clauses thought of as "boilerplate", require planning and a consideration of the circumstances of the contract and a fair allocation of the risk between the parties. An understanding of the purpose of the insurance can go a long way to ensuring the right clauses are used for the right reasons, instead of the use of default language. As well as keeping contractual language clear and relevant, a tailored approach may simplify contract administration and could even improve pricing.

## Common clauses

Below are some types of clauses or parts of clauses commonly found – together with a short discussion of their strengths, weaknesses and when and how they might be used.

### Named on the Policy:

One misconception is that customers should **always** ask to be "named" in the supplier's insurance policies. This misconception can lead to clauses that are more onerous than needed. Depending on the class of insurance product and the structure of the supplier's program, it may not be possible or practical to name the customer – or the insurer simply may not agree. While there are situations where naming the customer on the policy may make good sense, it's important to understand the possible implications for policy coverage – for example, some policies exclude claims made by one insured against another.

### Noted on the Policy:

Like naming, a clause may ask that an interest be "noted". The problem with this kind of clause is that it may achieve very little, if taken literally. If a customer wants to have a right to access a supplier's insurance directly, the right it wants has to be set out clearly in the contract and must be available in the insurance market. Often, what a customer is really after is cover for liability claims against it that result from actions taken by the supplier on its behalf (a cover commonly available in the market). If so, the clause should be tailored appropriately.

**Policy wording:**

Some clauses require the supplier to provide a complete copy of the policy wording, which is typically confidential between the contract and its insurer. It is not uncommon for insurers to refuse to allow the supplier to provide policy documents to others, and the supplier may not want to do so for its own risk management purposes. The customer should assess how critical it is to see contract wordings – in some cases, it will be important; while in others seeing a certificate of currency issued by the supplier's broker or insurer, or a summary of the insurance terms, will be sufficient.

**Change of insurer:**

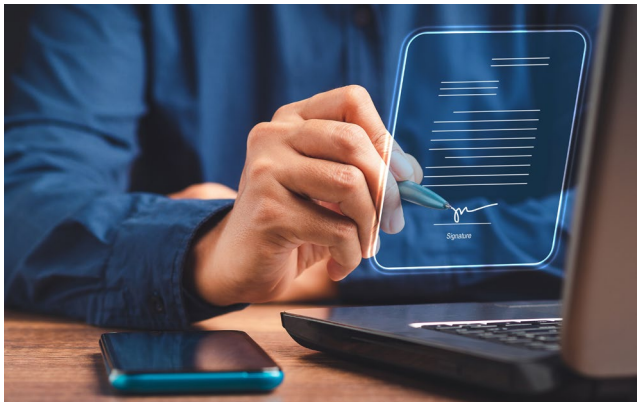
Clauses sometimes stipulate that the supplier must notify the customer of a change in insurer. This requirement is often unnecessary, especially when the contract already has sufficiently clear requirements for insurance.

**Insurer rating:**

An insurance clause will commonly seek to ensure that any insurance taken has been issued by an insurer with a minimum rating from a credit rating agency. While this may give some comfort that the insurer is in a position to back their product, it may limit the supplier's access to other potentially acceptable insurance solutions.

**Notice of any claims:**

A clause seeking to be notified of claims (unrelated to the contract) is likely to be misguided. If the reason for the policy is contract specific, then claims may be known in any case. If the reason is customer prudence, an unrelated claim on a policy may be of little relevance, providing there is ongoing cover, and could well be confidential.




## Customer's liability cover (often called principal's liability cover)

Sometimes the risk that is appropriate to mitigate with insurance, is that a claim may be made against the customer based on the acts or omissions of the supplier, if acting on behalf of the customer.

Principal's liability cover extends a liability policy (taken out by the supplier) to provide cover for the loss of the customer in this scenario. This is to protect the customer in circumstance where it might have vicarious liability for the supplier's conduct. The need for this type of insurance might arise, for example, where the supplier may have some people located at the customer's premises (e.g., in software development, but this is becoming less common with the move to the cloud). Whilst the customer may already have its own insurance, it is possible (for example) that it doesn't believe it should pay for any premium uplift by having additional personnel and/or it may want to protect its claims record.

## So what if you don't comply

One difficulty with insurance clauses is the consequences of a breach of the clause. It is well understood that damages for breach of a contract are there to put the party in the position it would have been in had the contract been performed.

Assuming the obligation to insure exists, working out what loss a customer has sustained because a supplier has not taken out a required policy is problematic. If there has been no loss for which the policy would respond, it is hard to envisage a loss caused by the breach. Equally, if the party that does not effect the insurance causes a loss, either it is capable of meeting the liability (so there is no need for a policy anyway) or it is not capable of meeting the loss, in which case it may become insolvent, and there will be little value in making a claim as there are no funds to meet it.

If the purpose of the requirement to be insured is what has been described above is a prudence exercise, then best practice is to follow up that prudence with a requirement to ensure the supplier does in fact hold the policies by way of certificates of currency or other means to confirming compliance.

## Types of Policies

A key element in mandating insurance in a contract is to understand the different types of insurance.

**Claims made v occurrence policies:** A claims made policy is a policy intended to cover claims made (or circumstances notified) during the term of the policy. A claim may not be made for a significant time – potentially many years – after the events which give rise to it. For this reason, it is common to require that runoff insurance for (commonly) seven years be maintained after the end of a contract. Professional indemnity insurance (discussed below) is usually a claims made policy. Occurrence policies, on the other hand, provide cover for claims arising from events that occur during the policy period.

**Professional indemnity policy:** A professional indemnity policy covers the risks taken by a business that provides professional advice or services (e.g., a doctor or a lawyer). If a supplier is giving advice, making recommendations or providing other professional services, a prudent customer would ask the supplier to hold professional indemnity insurance (and keep it for seven years after the end of the contract).

**Public liability cover:** This type of insurance typically covers personal injury and property damage. It is commonly written on an occurrence basis.

**Cyber insurance:** Increasingly, customers are requiring their suppliers to hold cyber insurance. The principal should give thought to what precisely they want the supplier to hold insurance against and the reasons why. Cyber insurance covers first party losses – such as the costs of responding to a cyber incident, which can ensure there is a financial "safety" net and experts in place who can act quickly to rectify a breach. This class also often includes cover against third party claims based on a cyber event, but the scope of the cover can vary between products.

## Other issues

Insurance brokers are an invaluable asset when a business is trying to assess suitable insurance needs, its risk and to investigate the market for insurance.

## Conclusion

Our key tips:

- Think about your contract wording and tailor it appropriately, rather than using "default" clauses.
- Remember that insurance is only one way to manage risk. And that a supplier may pass on the cost of insurance it is required to take out to the customer. Decisions about the scope and limits of insurance required under a contract need to consider both the advantages and costs of managing risk in this way.
- Assess risk, determine who carries it, and choose suitable insurance – ideally with professional advice.
- Obtain evidence of cover and actively manage the contract.

# What we do

## Broad experience, driven and energetic

**Our Technology, Cyber & Privacy team has extensive experience advising clients in the rapidly evolving technology, data protection and privacy space.**

Whether in the course of large-scale digital transformation, uplift projects, or business as usual, we work collaboratively with clients to navigate the requirements of security and data protection including privacy compliance within the complex regulatory landscape of these dynamic areas of law.

### Technology

**IT Procurement & Contracting—**Advising on high-value contracts, vendor agreements, cloud and other 'as a service' solutions and complex IT procurement processes.

**Digital Transformation—**Guiding organisations through digital strategy implementation, cloud services, and technology outsourcing.

**Data & IP Management—**Supporting IP licensing, software development, data transfer, storage and governance structures.

**Emerging Tech & Innovation—**Advising on AI, blockchain and Web3, fintech, quantum and other emerging and disruptive technologies, including rapidly evolving compliance and regulatory issues.

Assisting suppliers and buyers of telecommunications services, with high value, whole of business or redundancy management.


## Cyber

**Cyber coverage—**Managing cyber coverage disputes (including serving as monitoring counsel), advising on risk management strategies and trends in the market, indemnity/claims issues regarding commercial contracts and projects, and drafting and reviewing cyber policies (both personal and company policies) for compliance and determining whether coverage exists.

**Cybersecurity Strategy—**Advising on regulatory compliance, risk assessments, and policy development for robust cybersecurity.

**Incident Response & Crisis Management—**Assisting with data breach responses, cyber-attack containment, and regulatory reporting requirements.

**Cyber Risk & Insurance—**Advising on risk mitigation and insurance policies specific to cyber threats and data loss.

**Regulatory Compliance & Reporting—**Ensuring alignment with APRA, ASIC, OAIC, and other regulatory guidelines on cyber resilience.

## Privacy

**Privacy Compliance & Data Protection—**Supporting compliance with the Privacy Act and APPs including consent management, and cross-border data transfers.

**Data Breach Management—**Advising on NDB scheme obligations, breach response, and crisis communication.

**Managing emerging privacy risks—**advising on the privacy and cyber risks associated with automated decision making and artificial intelligence.

**Employee Privacy & Surveillance—**Navigating employee monitoring, privacy rights, and compliance with workplace privacy obligations.

**Spam—**Advising and assisting businesses with Spam compliance and complaint management.

# Who we are

## Technology, Cyber & Privacy team

**Hamish Fraser**
**Corporate & Commercial**
Partner
t: +61 2 9373 3616
e: Hamish.Fraser@sparke.com.au

**Jason Kwan**
**Corporate & Commercial**
Partner
t: +61 3 9291 2376
e: Jason.Kwan@sparke.com.au

**Chantal Tipene**
**Government Public & Regulatory**
Partner
t: +61 2 9260 2542
e: Chantal.Tipene@sparke.com.au

**Nick Christiansen**
**Corporate & Commercial**
Partner
t: +61 2 9260 2443
e: Nick.Christiansen@sparke.com.au

**Jehan Mata**
**Commercial Insurance**
Partner
t: +61 3 9291 2374
e: Jehan.Mata@sparke.com.au

**Stephen Putnins**
**Corporate & Commercial**
Partner
t: +61 3 9291 2392
e: Stephen.Putnins@sparke.com.au

**Felicity Edwards**
**Workplace**
Partner
t: +61 2 9373 1469
e: Felicity.Edwards@sparke.com.au

**Jon Tyne**
**Specialty Lines**
Partner
t: +61 2 9260 2683
e: Jonathan.Tyne@sparke.com.au

# Contributing authors

## Thank you to our additonal authors for their contributon


**Marianne Robinson**
**Corporate & Commercial**
Special Counsel
t: +61 2 9260 2755
e: Marianne.Robinson@sparke.com.au

**Dinah Amrad**
**Commercial Insurance**
Associate
t: +61 3 9291 2212
e: Dinah.Mmrad@sparke.com.au

**Nicholas Chan**
**Corporate & Commercial**
Associate
t: +61 3 9291 2287
e: Nicholas.Chan@sparke.com.au

**Stefanie Constance**
**Corporate & Commercial**
Associate
t: +61 3 9291 2277
e: Stefanie.Constance@sparke.com.au

**Robert Fraser**
**Corporate & Commercial**
Associate
t: +61 3 9291 2343
e: Robert.Fraser@sparke.com.au

**Elijah Royal**
**Workplace**
Associate
t: +61 2 9260 2723
e: Elijah.Royal@sparke.com.au

**Jasmine Thai**
**Corporate & Commercial**
Lawyer
t: +61 2 9260 2540
e: Jasmine.Thai@sparke.com.au

**Ella Sourdin Brown**
**Corporate & Commercial**
Law Graduate
t: +61 3 9291 2398
e: Ellasourdin.Brown@sparke.com.au

**Maxwell Watson**
**Casualty**
Paralegal
t: +61 3 9291 2257
e: Maxwell.Watson@sparke.com.au

# Putting you at the heart of everything we do.

www.sparke.com.au

adelaide | brisbane | cairns | canberra | darwin | melbourne | newcastle | perth | sydney | upper hunter