sparke HELMORE LAWYERS

Sparke Bytes

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

JUN 2025 **QUARTERLY**

CONTENTS

03 **From breach to brief:** Preserving legal professional privilege in a rapidly unfolding cyber breach

06 **Artificial intelligence transcription:** the good, the bad and the unfiltered truth

11 **Australia just got a new privacy law and it's a game changer**

13 **Connected vehicles and the Telecommunications Act:** are vehicle manufacturers becoming carriage service providers?

15 **Silent AI.** A wake-up call for insurers and insureds

17 **Australia's digital dilemma:** what really counts as an electronic signature?

19 **The hidden threat:** rising cyber incidents in Australia and the urgent need for cyber insurance

21 **Mandatory reporting of ransomware and cyber extortion payments**

24 **Enforcing force majeure in a 'SaaSy' environment**

27 **Our promise to you**

28 **What we do**

30 **Who we are**

If you no longer wish to receive this publication, email *sparkehelmorelawyers@sparke.com.au*

Copyright 2025 © Sparke Helmore. This publication is not legal advice. It is not intended to be comprehensive. You should seek specific professional advice before acting on the basis of anything in this publication.

FROM BREACH TO BRIEF: PRESERVING LEGAL PROFESSIONAL PRIVILEGE IN A RAPIDLY UNFOLDING CYBER BREACH

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

A recent Federal Court judgment regarding the 2022 Medibank data breach highlights the importance of preserving legal professional privilege in expert reports prepared following a data breach.

In that case, Medibank was unsuccessful in its attempt to claim legal professional privilege over three reports prepared by Deloitte in response to the very public data breach.

While the law surrounding legal professional privilege is well established, the unique nature of a data breach is different, as was observed by Justice Rofe, in the **Medibank Decision**, *"the production of the documents must be viewed in the context of the rapidly unfolding Cyber Incident… ."*[1]

The Medibank breach

In late 2022, Medibank experienced a cyber-attack during which threat actors accessed its IT systems using stolen credentials and exfiltrated approximately 520GB of data, affecting 9.2 million customers.

After failing to extract a ransom payment from Medibank, the threat actors began releasing the sensitive customer data on the dark web.

As part of Medibank's response to the cyber security incident, it engaged with external cyber security consultants to investigate and assist with a response plan. Medibank claimed legal professional privilege over all its reports and communications.

The "dominant purpose" test

The test for professional legal professional privilege is an objective test of whether the confidential communications in question were made for the **dominant purpose** of obtaining legal advice or for use in contemplation of litigation.[2]

In the Medibank Decision the Court observed that it is *"not sufficient that giving or obtaining legal advice or providing legal services was in part the purpose; it must be the dominant purpose of the relevant communication."*[3]

Furthermore, the purpose must be assessed at the time the communications occurred.

What was said and done

Medibank engaged its lawyers and cybersecurity experts to prepare several reports, all labelled as being prepared for the dominant purpose of obtaining legal advice.

This occurred during a busy period as events unfolded rapidly with different issues arising in quick succession including the breach, the basis of the attack, the data taken, the subsequent ransom demand and whether to pay it. In addition, numerous stakeholders and decision-makers were being called upon or were asking for updates.

1 *McClure v Medibank Private Limited* [2025] FCA 167 at [218].
2 *Ibid at* [176].
3 *Ibid at* [180].

In the glare of public and regulatory scrutiny, Medibank made several statements and took steps to establish other purposes, which the Court used to determine the purpose for each document. The Court categorised these purposes as follows:

Public relations and ASX purpose: Medibank made multiple public statements to the ASX, its customers, employees, and health partners, emphasising that it commissioned the reports to learn from the cyber incident and better protect customers.

The APRA purpose: Evidence presented during the hearing showed that one purpose of Deloitte's reports was to avoid an investigation by APRA.

The role of the Board: Board papers revealed the Board wanted an *"unvarnished view"* of the incident. They resolved to appoint Deloitte in a meeting that included no lawyers and did not express intent to have legal counsel engage with Deloitte.

Third parties and agents

Businesses are increasingly engaging with external cybersecurity and technology experts to help them contain and understand the circumstances of a cyber incident and respond to regulatory investigations or mandatory reporting requirements.

However, it is important that these third party agents are engaged for the dominant purpose of gaining legal advice or in anticipation of litigation. Simply stating this purpose is insufficient to establish legal professional privilege and *"is not established by bare ipse dixit."*[4] (that is: just by saying it doesn't make it true).

It is also important to consider that legal professional privilege is also not established *"to third party advices to the principal simply because they are then 'routed' to the legal adviser."*[5] Merely labelling reports or communications as confidential and protected by privilege is insufficient to satisfy the dominant purpose test.

What documents were privileged?

Justice Rofe determined on the evidence provided by Medibank that, despite the rapidly unfolding circumstances, some communications and reports did satisfy the dominant purpose test for obtaining legal advice and preparing for litigation. These included four reports produced by CrowdStrike and Threat Intelligence, as well as various emails and the attachments from CyberCX and Coveware.

Medibank stated that the dominant purposes included:

- advising Medibank on its compliance with the *Privacy Act 1988* (Cth)
- responding to compulsory OAIC notices
- identifying legal issues and risks (including those arising under Australia's anti-money laundering, financing or terrorism and sanctions laws)
- briefing counsel and preparing Medibank's defences in legal proceedings, and
- preparing advice to Medibank on steps it should take in relation to leaked data in order to comply with its legal obligations and mitigate any legal risk.

What was not privileged? Deloitte Reports

Medibank commissioned three reports including a 'Post Incident Review,' 'Root Cause Analysis' and 'External Review – APRA Prudential Standard CPS 234' (**Deloitte Reports**). The Deloitte Reports were found not to be protected by legal professional privilege for two main reasons:

1. **Multiple purposes:** the dominant purpose of the reports was not to obtain legal advice or for the preparation of litigation but instead for other non-legal purposes.
2. **Waiver of privilege via public statements:** Medibank's voluntary disclosure through ASX Announcements and other public statements, which disclosed the "gist or conclusions" and recommendations from the Deloitte Reports constituted a waiver of privilege.

[4] *Robertson v Singtel Optus Pty Ltd* [2023] FCA 1392 at [29].
[5] *McClure v Medibank Private Limited* [2025] FCA 167 at [186].

Multiple purposes

Justice Rofe found that the Deloitte Reports were produced for four other purposes in addition to the dominant purpose of obtaining legal advice or preparing for litigation. These included:

1. **operational**
2. **governance**
3. **APRA, and**
4. **ASX and public relations purposes.**

It was not disputed that Medibank commissioned the Deloitte Reports for legal purposes, but it was concluded that it was not the dominant purpose. Justice Rofe placed emphasis on the Board's involvement with Deloitte where Deloitte directly reported its findings to the Board. the engagement with Deloitte was heavily influenced by APRA, which *"informed the scope of the external review to ensure that it met APRA's requirements."* This aim was to avoid a separate review with APRA, which was identified as a dominant purpose of the Deloitte Reports.

Waiver of privilege through public communications

Justice Rofe concluded that even if the Deloitte Reports were protected by legal professional privilege, Medibank would have waived its claim by making public announcements.

Tips

It is essential that businesses consider various factors when conducting an investigation:

- During a cyber breach, many actions are taking place simultaneously.
- It is prudent to pause and reflect on the purpose of the various communications.
- Simply asserting a claim for legal professional privilege is not sufficient.
- Seek legal advice regarding the content of market communications and other public statements and be aware of the potential consequences.
- Assess whether the circumstances justify the preparation of different reports for different purposes.

Conclusion

Ultimately, the Court found that it *"did not consider that the provision of legal advice and/or assistance was the dominant purpose for which the Deloitte Reports were commissioned."*[6]

What is perhaps more important is that in the midst of a rapidly evolving cyber security breach—characterised by a whirlwind of information, misinformation, stakeholders, and questions—legal professional privilege can still be maintained.

To retain legal professional privilege, careful consideration must be given to the creation of the communications but also to the statements made about them (both before and after their creation), which can inform the reader about the author's mindset regarding their creation.

[6] *Ibid* at [323].

ARTIFICIAL INTELLIGENCE TRANSCRIPTION: THE GOOD, THE BAD AND THE UNFILTERED TRUTH

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

Recent advancements in Artificial Intelligence (**AI**) transcription have evolved from simple dictation to the efficient and accurate recollection of conversations that can be summarised, interrogated, and reformatted.

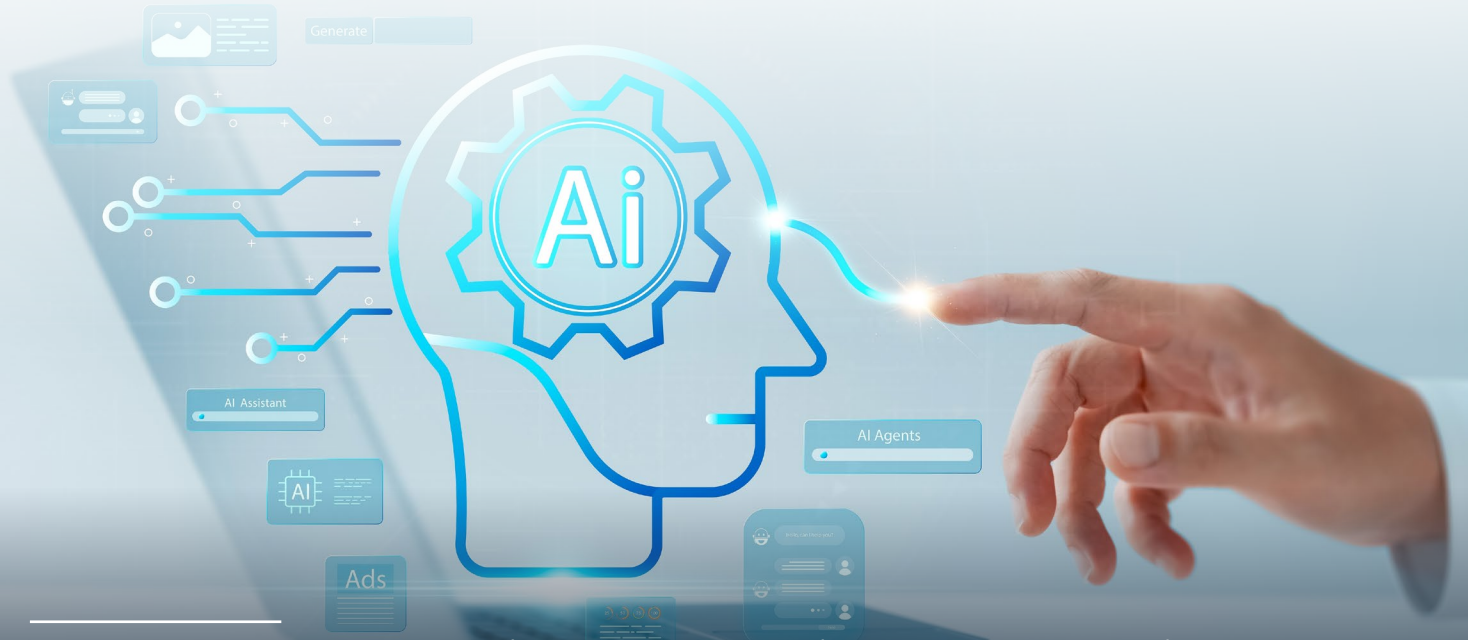
This article examines some of the main legal risks associated with the use of AI transcription tools, particularly concerning privacy, confidentiality, surveillance, and intellectual property. Organisations intending to use AI transcription tools, whether for internal purposes or in interactions with customers, patients, or clients, should be aware of these ethical and legal issues.

How do AI transcription tools differ from conventional transcription tools?

AI transcription tools generally operate through one of two ways:

1. Online Video Conferencing: audio is recorded using software and then downloaded.[7]
2. Face-to face: a microphone is used to capture speech, which is then converted into text.[8]

These tools differ from conventional transcription devices because they utilise machine learning, which allows them to adapt without explicit instructions. They also incorporate natural language processing, enabling them to understand dialects, accents, and colloquialisms, and automatic speech recognition to convert audio into written text.[9] AI tools can also be used to translate audio into multiple languages.



[7] Gabrielle Samuel and Doug Wassenaar, 'Joint Editorial: Informed Consent and AI Transcription of Qualitative Data' (2024) 20(1-2) *Journal of Empirical Research on Human Research Ethics.*

[8] A Baki Kocaballi et al. 'Envisioning an artificial intelligence documentation assistant for future primary care consultations: A co-design study with general practitioners' *Journal of the American Medical Informatics Association 27* (11) (2020) 1695–1704.

[9] Verbit 'AI Transcription: A Comprehensive Review' (Web Page, 2025) https://verbit.ai/transcription/ai-transcription-a-comprehensive-review/.

Use cases

AI transcription tools have been widely adopted across various industries.[10] They are used by organisations that traditionally rely on transcription services, such as call centres as well as companies that integrate transcription functionalities into their existing products, like Webex and Microsoft Teams (which uses Microsoft Co-pilot to transcribe meetings).[11] Below are some additional emerging use cases of AI transcription:

Industry	Use case
Education	Integration into 'Ed Tech' to transcribe lessons, provide personalised summaries, action lists based on student ability and generate real-time subtitles for lectures.[12]
Media and Entertainment	Provide efficient captioning and subtitles, enabling greater content distribution to broader audiences. The tools are also used to transcribe podcasts, audio, video, and interviews.[13]
Legal	Recording internal and external conversations to streamline administrative work such as file notetaking.
Financial advisors	Automating client notes, emails, and meetings. Compliance monitoring where financial firms might be required to record and analyse customer interactions for regulatory purposes. AI transcription can automate this process and flag words for further review to detect policy violations.[14]
Healthcare	Recording doctor-patient conversations and providing detailed clinical notes of the consultation.
Academia	Transcribing interviews for research purposes.

[10] NSW Supreme Court, *Practice Note SC Gen 23:* Use of Generative Artificial Intelligence (Gen AI).
[11] Microsoft, 'Copilot in Microsoft Teams Meetings and Events' (Web Page, 2025) https://learn.microsoft.com/en-us/microsoftteams/copilot-teams-transcription; Agam Shah, 'Cisco's AI Agents for Webex Aim to Improve Customer Service' (Web Page, 2025) https://www.computerworld.com/article/3846753/ciscos-ai-agents-for-webex-aim-to-improve-customer-service.html.
[12] StoryShell, 'The Game-Changing Impact of AI-Powered Translation, Transcription, and Dubbing in the Media and Entertainment Industry: A Case for Czech and Bulgarian Markets' (Web Page, 2025) https://www.storyshell.io/blog/the-game-changing-impact-of-ai-powered-translation-transcription-and-dubbing-in-the-media-and-entertainment-industry-a-case-for-czech-and-bulgarian-markets/.
[13] Way With Words, 'Exploring Use Cases for Speech Data in AI' (Web Page, 2025) https://waywithwords.net/resource/exploring-use-cases-speech-data-in-ai/.
[14] Milvus 'What are the use cases of speech recognition in financial services' https://milvus.io/ai-quick-reference/what-are-the-use-cases-of-speech-recognition-in-financial-services.

What legal issues arise from AI transcription use?

The use of AI transcription raises legal issues around privacy, confidentiality, surveillance, and intellectual property.

Privacy risks

The *Privacy Act 1988* (Cth) outlines the requirements for the collection, use, disclosure, and storage of personal information. Below is a summary of key privacy risks associated with the use of AI transcription.

Australian Privacy Principles (APP)	Potential risk / breach	Mitigation
APP 3 – Collection	Using an AI transcription tool to collect personal information not needed for the organisation's activities or collecting personal information in an unfair or unlawful manner.	Organisations must: (a) ensure any personal information collected using the AI transcription tool is reasonably necessary for its business functions or activities; and (b) obtain consent for the collection of sensitive information (e.g. race, health or sexual orientation).
APP 5 – Notification	Failure to inform individuals that personal information is being used to train the AI.	Organisations should ensure privacy policies inform individuals when and for what purposes their personal information is being used and disclosed (including when it is being used to train the AI).
APP 6 – Use and Disclosure	Using personal information to train the AI transcription tool without the individual's consent, or the organisation is unable to establish use for a primary purpose or secondary related purpose.	Check contracts with vendors to determine what personal information can be used for. Ensure sufficient notices are provided to individuals relating to the proposed disclosure and use of personal information.
APP 8 – Cross-border Data Transfer	Transferring data offshore without ensuring equivalent privacy protections.	Ensure there are adequate contractual obligations on AI vendors to ensure they handle personal information in accordance with Australian privacy laws.
APP 10 – Quality of Personal Information	Not taking reasonable steps to ensure the accuracy of personal information or translated material generated, used, and disclosed.	Take reasonable steps to ensure the accuracy of personal information, including AI generated transcripts.
APP 11 – Security of Personal Information	Weak security measures leading to unauthorised access, leaks, or misuse and a failure to take reasonable steps to protect personal information.	Take reasonable steps (operational and technical) to protect personal information. This includes conducting adequate due diligence around the transcription device to ensure the security of the personal information, including in relation to cyber threats.

Depending on the circumstances, a breach of the Australian Privacy Principles (**APPs**) can be considered a 'serious' or 'repeated' interference with an individual's privacy.[15] In addition, organisations should be mindful of the new tort for serious invasions of privacy commencing 10 June 2025. This tort highlights the importance for organisations to collect, use, and disclose personal information appropriately and, where applicable, with the individual's consent.

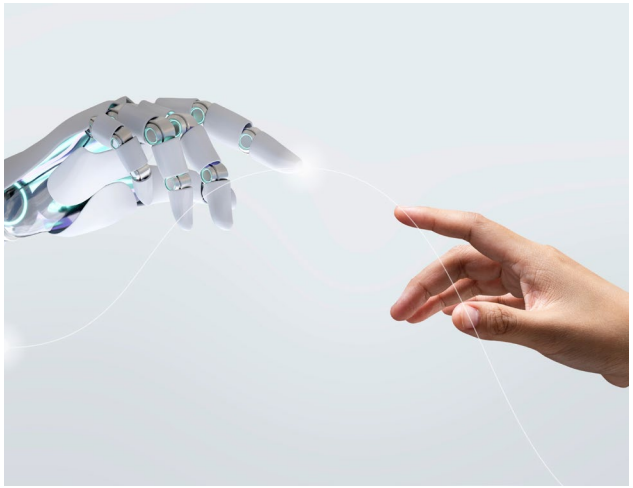
[15] s 13G of the Privacy Act 1988 (Cth).

Risk of confidentiality breaches and the internal use of AI transcription tools

AI models often struggle to understand the context of the information they receive. As a result confidential information is typically not identified as such and is treated the same way as less sensitive information. This increases the risk of confidentiality breaches for businesses that adopt internal AI transcription tools. Example risks include:

- AI tools using confidential information to train their models, leading to the potential inclusion of confidential information in generated outputs.
- Unauthorised distribution or access to conversation transcripts by third parties who are not permitted to have access to that information (for example, uploading meeting minutes to the corporation's practice management system without proper access restrictions, or sending automated emails to stakeholders with transcripts that have not been vetted for confidential information).

Organisations should consider implementing measures to mitigate these risks, such as ensuring appropriate access protocols are in place and that records are automatically deleted after the prescribed retention period. They might also explore whether certain automatic functions within the AI transcription tool can be disabled.



Do state and Commonwealth surveillance laws apply?

In Australia, states and territories have strict regulations regarding the audio recording of conversations. The legislation differs from state-to-state; however, it is generally considered a criminal offence to record private conversations or to disclose recordings of private conversations without the consent of both parties' consent (with some exceptions[16]).[17] Organisations should typically obtain informed consent before recording a conversation with an individual.[18] Informed consent means that individuals are fully aware they are being recorded and understand the consequences of that recording, including how the information obtained will be used and what it will be disclosed for if consent is granted.

Ownership of and ongoing right to use AI generated material?

In Australia, there is currently no law governing the ownership of intellectual property (**IP**) for AI-generated works.[19] Under existing laws, copyright protection requires a human author who contributes independent intellectual effort. Similarly, the *Patents Act 1990* (Cth), requires there to be a human inventor. In fact, ownership of IP rights in AI-generated material could potentially be attributed to various individuals involved in the content's generation, including the developer or deployer of the AI transcription tool, or the person who input the data used by the AI for generating the output.

Ownership of the IP in generated outputs may also depend on specific circumstances and the types of information input into the AI system. Organisations procuring an AI transcription tool should ensure that they own the IP rights in any outputs or have a perpetual licence to use such outputs.

[16] In some states and territories there are exceptions (for example, implied consent is allowed for the protection of one's lawful interests) but these exceptions are unlikely to apply in most of the use cases detailed above.

[17] ss 4, 5, 7 *Listening Devices Act 1992* (ACT); ss 7,11,12 *Surveillance Devices Act 2007* (NSW) ; ss 11 and 15 *Surveillance Devices Act 2007* (NT); ss 43 and 45 *Invasion of Privacy Act 1971* (QLD); ss 4 and 12(1)(a) *Surveillance Devices Act 2016* (SA); s 5, 11, 12 *Listening Devices Act 1991* (TAS); ss 6 and 11 *Surveillance Devices Act 1999* (VIC); ss 5, 9, 34 *Surveillance Devices Act 1998* (WA); Notably, the Commonwealth Telecommunications *(Interception and Access) Act* 1979 has a much narrower application in relation to the mechanism in which conversations are recorded or 'intercepted', so, it is unlikely to apply but it is good to be mindful of the Act's existence and potential application.

[18] Medical Indemnity Protection Society, 'AI Scribes: Medicolegal Issues' (Web Page, 2024) <https://support.mips.com.au/home/ai-scribes-medicolegal-issues>.

[19] Nirogini Thambaiya, Kanchana Kariyawasam and Chamila Talagala 'Copyright law in the age of AI: analysing the AI-generated works and copyright challenges in Australia' 2024, 1(26), *International Review of Law, Computers & Technology.*

Mitigating and managing risk – Responsible AI governance

Establishing effective AI governance frameworks and conducting AI impact assessments are important for managing the risks associated with AI usage. This includes ensuring the ethical and responsible deployment of AI systems. An AI governance framework should ideally be structured around the AI Ethical Principles. In addition, AI impact assessments can be used as an ancillary assessment tool, typically comprising three components:

1. **Assessment:** identifying potential risks and determining whether a more comprehensive assessment is required.
2. **Action plan:** setting clear goals and providing measures to track performance and report impacts.
3. **Report template:** a precedent report to help users summarise risks, publish assessment results, and share learnings.

The goal of an AI impact assessment is not to eliminate risk but to highlight the risks and benefits of the AI, balancing them against corporate and business objectives for introducing the AI. Organisations should consider the Voluntary AI Safety Standards and Proposed Mandatory Guardrails for high-risk AI when planning their assessments.

Future of AI transcription tools

While recent advances in AI-driven transcription tools have led to efficiency gains for users, risks related to privacy, confidentiality, and IP must be managed carefully. This ensures that the benefits of AI transcription tools are realised in a legally compliant and ethical manner.

AUSTRALIA JUST GOT A NEW PRIVACY LAW AND IT'S A GAME CHANGER

Authors: Hamish Fraser (Partner) and Gabe McNamara (Lawyer)

In a highly anticipated and long-awaited move, the Federal Parliament has introduced a new statutory tort for serious invasions of privacy, fundamentally reshaping the privacy law landscape across Australia.

For some time, there has been worldwide discussion about developing such a tort. This new law provides individuals with a clear and direct pathway to seek redress for privacy breaches, and importantly they do not need to prove damage to initiate a lawsuit.

What's new?

The new tort addresses two types of conduct:

1. Intrusions upon a person's seclusion—this includes physical or digital snooping and stalking.
2. Misuse of private information—for example, leaking sensitive personal data.

Importantly, to succeed in a claim, a person must prove four key elements:

a. There was an invasion of privacy.

b. They had a reasonable expectation of privacy.

c. The conduct was intentional or reckless (not merely careless).

d. The invasion was serious.

A long time coming

The move brings to life long-standing recommendations from the Australian Law Reform Commission (**ALRC**). The ALRC's 2014 report, *Serious Invasions of Privacy in the Digital Era*, laid the groundwork by urging the Federal Government to create a statutory tort that reflects international privacy norms and modern technological risks.

Until now, Australia has lagged behind countries such as the UK, New Zealand, and Canada in providing a clear recourse for privacy invasions. Although the courts have considered the concept of a tort of privacy, notably in the High Court's 2001 decision of *ABC v Lenah Game Meats*, they have stopped short of recognising a standalone tort.

This new law fills that gap.

Serious invasion? Here's what that means

The threshold for a successful claim is high; the invasion must be serious, meaning it is more than just inconvenient or mildly offensive. Courts are likely to ask, *"Would a reasonable person find this conduct highly offensive? Did it cause emotional or psychological harm, or interfere with a person's ability to go about their life?"*

This aligns with earlier decisions, like that of *Grosse v Purvis*, which emphasised the need for genuine distress or detriment—not just technical violations.

It's not just about hackers

You don't need to be a cybercriminal to fall foul of this law. The tort also targets misuse of personal information, meaning businesses, health providers, and even government departments must be cautious. A breach of the APPs— those extra obligations that prompt businesses to make you read a privacy policy before signing— could form the basis for a privacy tort claim.

Expectation of privacy: context is key

Not everything private is protected. Courts will examine whether a reasonable person in the affected party's position would expect privacy in that situation. Factors such as age, profession, public exposure, and the context of the intrusion are all relevant. For example, a celebrity might expect less privacy in public but could still have a case if their private medical data is leaked.

Recklessness isn't a loophole

This law isn't just about punishing deliberate acts. If someone recklessly disregards another's privacy—such as sharing data without verifying consent—they could be held liable. Courts are likely to apply an objective standard: would a reasonable person in the same position have acted differently?

While negligent acts alone might not be enough, reckless disregard definitely is.

Public interest vs personal privacy

A unique feature of a new tort is a built-in public interest balancing test. Defendants can argue that their conduct served a greater good, such as protecting national security, public health, or freedom of expression. This defence is modelled on international standards and partly borrowed from defamation law.

However, it is not a free pass. Courts are expected to weigh the public benefit of the intrusion against the harm caused to the individual. When this balance tips in favour of the individual, then so will the public interest.

So what's the price of privacy?

The courts now have substantial power to award remedies, including:

a. damages for emotional harm

b. punitive damages in exceptional cases (damages for when businesses and individuals significantly misstep)

c. apologies or corrections

d. injunctions to stop or prevent further breaches, and

e. accounts of profits (forcing businesses and individuals to relinquish money made from the breach).

However, there's a catch: damages for non-economic loss (when privacy interference causes emotional harm) must remain within the damages limit, currently capped at $478,500.00 or the equivalent amount for general damages in defamation cases.

This raises the question; how much is your privacy worth?

Time for businesses to step up

For businesses in this new established age of technology and privacy, this tort is a wake-up call. It adds another layer of legal risk, particularly regarding data security, storage, and disclosure. In short: the stakes have just gotten a lot higher.

Therefore, it's a good time to take a fresh look at your approach to privacy and ensure it remains a priority when reviewing systems and processes.

A new era for privacy in Australia

Australia's new privacy tort marks a major leap forward in protecting individuals in the digital age. It seeks to strike a balance between personal rights and public interest, emphasising that privacy is not just a courtesy but a fundamental right.

As the digital world becomes increasingly complex and intrusive, this reform arrives at a crucial moment when the law and lawmakers are working hard to keep pace.

CONNECTED VEHICLES AND THE TELECOMMUNICATIONS ACT: ARE VEHICLE MANUFACTURERS BECOMING CARRIAGE SERVICE PROVIDERS?

Authors: Jason Kwan (Partner) and Stefanie Constance (Associate)

As vehicles become increasingly connected—offering live telematics, embedded SIMs (**eSIMs**), over-the-air (**OTA**) updates, and infotainment powered by mobile data—Original Equipment Manufacturers (**OEMs**) are venturing closer to activity regulated by Australia's telecommunications framework. In particular, there is a risk that unless extra care is taken, OEMs may be classified as Carriage Service Providers (**CSPs**) under the *Telecommunications Act 1997* (Cth) (**Telecommunications Act**), with consequential regulatory obligations.

Historically, compliance in this area has been somewhat unclear, with a lack of understanding regarding key obligations. As cars become increasingly connected, and as the means to providing connectivity services are better understood, stricter compliance is likely to become essential.

This article explores how OEMs may trigger CSP classification and outlines the steps OEMs can take to manage this risk. It follows on from our previous article, Navigating privacy in the age of connected vehicles :: Sparke Helmore, which discussed some of the key privacy considerations for connected vehicles.

What is a Carriage Service Provider?

Under s 87 of the Telecommunications Act, a CSP is any person who supplies a carriage service to the public using infrastructure owned by a carrier or under a nominated carrier declaration.[20] A carriage service broadly refers to the transmission of communications by electromagnetic energy, whether guided (e.g. fibre) or unguided (e.g. mobile networks).[21]

This regulatory framework, originally designed for telecommunications companies, is becoming increasingly relevant to the automotive industry as vehicles are equipped with computer hardware that integrates connectivity not only to the manufacturer (for service and mechanical issues) but also with other vehicles and the internet more generally.

How might OEMs be caught?

Several scenarios might lead to OEMs being classified as CSPs as a result of the in-car technology they offer:

Embedded connectivity: If a vehicle includes a pre-installed eSIM[22] that provides internet access and/or telephone call capabilities, and the OEM manages the provisioning, activation, or switching of the mobile network, the OEM may be supplying a carriage service.

Bundled data access: OEMs that sell connectivity as part of a bundled subscription or offer value-added services reliant on mobile access (e.g. telephone call system, vehicle tracking, streaming, in car Wi-Fi hotspot) may be at risk of CSP classification.[23]

Acting as intermediaries: If an OEM facilitates or resells a telecommunication company's mobile service to consumers, either directly or via roaming arrangements, it could be classified as a Carriage Service Intermediary (**CSI**), a subset of CSPs.[24]

[20] Telecommunications Act 1997 (Cth) s 87.
[21] Ibid s 7.
[22] Department of Infrastructure, 'Connected Vehicles and the Telecommunications Act' (Discussion Paper, 2023)
[23] Ibid.
[24] Ibid.

Regulatory obligations for CSPs

If an OEM is deemed to be a CSP, it may become subject to several legal obligations:

Registration with the ACMA: CSPs must register with the Australian Communications and Media Authority (**ACMA**) and comply with applicable industry codes.[25]

Law enforcement assistance: CSPs must provide reasonable assistance to law enforcement and national security agencies.[26]

Metadata retention: Certain CSPs may be required to retain metadata relating to communications for specified periods (e.g. vehicle location information).[27]

Network security: CSPs must protect telecommunications infrastructure and services from unauthorised access or interference;[28] and comply with cyber incident reporting obligations under the *Security of Critical Infrastructure Act 2018* (Cth). This includes notifying the Australian Cyber Security Centre (**ACSC**) within 12 hours of a critical incident and within 72 hours for other reportable incidents. Civil penalties apply for non-compliance.[29]

Consumer service standards: CSPs must comply with relevant codes, including service guarantees and complaint-handling processes when providing services to end users.[30]

Risk management for OEMs and Australian based distributors

To minimise regulatory risk, OEMs and their in-country retailers and distributors should:

- Map their connectivity offerings to determine whether their activities mean they fall within the definition of a CSP.
- Ensure they have in place clear contractual arrangements with licensed telecommunications providers (both domestic and international) to clarify who is delivering the carriage services to end users. While the OEM may be party to agreements with offshore telecommunication providers, local access to Australian mobile networks will ultimately involve a local carrier, and compliance responsibilities must be clearly defined. This includes assigning responsibility for local compliance, network provisioning, switching, billing,[31] and ensuring appropriate risk allocation.
- Include product disclosures for multimedia or connectivity packages if included with the vehicle, clarifying that the telecommunications service is provided by a third party and subject to their licensing and terms.
- Ensure appropriate consumer awareness and consent is obtained (e.g. consent to the collection of personal information such as location or other vehicle telemetry data is collected or transmitted), and any data handled by it in its capacity as a CSP complies with APPs as well as CSP metadata obligations.[32]

Conclusion

OEMs must understand the regulatory obligations that apply if they are deemed to be a CSP. This understanding is crucial for making informed decisions about whether to offer those services and how to contractually manage the risk, particularly through their arrangements with carriers and distributors. Ultimately, OEMs should structure their connected vehicle operations in a way that aligns with their intended role in the telecommunications ecosystem. This alignment will be increasingly important as OEMs navigate evolving regulatory expectations.

[25] ACMA, About carriers and carriage service providers (Web Page, 2022) https://www.acma.gov.au/about-carriers-and-carriage-service-providers.
[26] *Telecommunications Act 1997* (Cth), s 313.
[27] *Telecommunications (Interception and Access) Act 1979* (Cth), Part 5-1A.
[28] *Telecommunications Act 1997* (Cth), Part 14.
[29] *Security of Critical Infrastructure Act 2018* (Cth), s 30BC and s 30BD.
[30] *Telecommunications (Consumer Protection and Service Standards) Act 1999* (Cth), ss 105, 106, 128,132.
[31] *Telecommunications Act 1997* (Cth) s 87 (definition of CSP); Australian Communications and Media Authority, Guidance on Third-Party Provisioning (Web Page, 2022) https://www.acma.gov.au/about-carriers-and-carriage-service-providers.
[32] Department of Home Affairs, *Data Retention Guidelines for Service Providers* (Guidelines, Australian Government, 2025) https://www.homeaffairs.gov.au/nat-security/files/data-retention-guidelines-service-providers.pdf.

SILENT AI. A WAKE-UP CALL FOR INSURERS AND INSUREDS

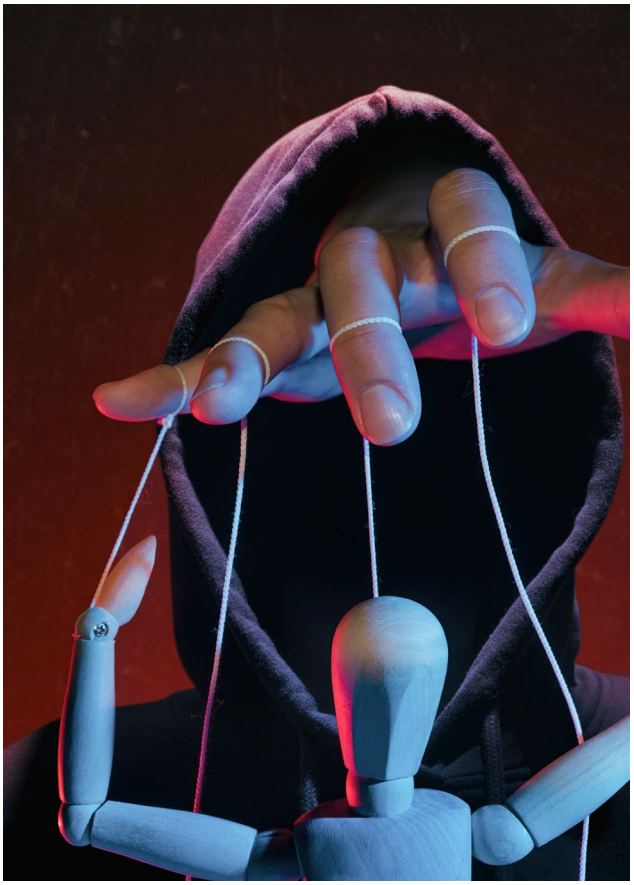
Authors: Robert Watson (Partner)

In the rapidly evolving landscape of technology, AI is experiencing explosive growth and while the possibilities offered by AI are exciting and compelling, the associated risks are becoming increasingly recognised.

Notwithstanding our understanding of the risks of AI, we are only just beginning to identify and manage those risks effectively.

One way to manage risk is through insurance; however the insurance industry is still fully coming to grips with AI-related risks.

As the insurance industry builds its understanding of AI risk, parallels are being drawn between cyber risk and AI risk. Indeed, many would remember the issues of 'silent cyber' and the term 'silent AI' is now being used to describe the similar impact of AI on insurance.



What is silent cyber?

Silent cyber is the situation where cyber-related losses are neither explicitly included nor excluded from an insurance policy. This ambiguity can force insurers to cover losses under policies that were not specifically designed for cyber risk.

The insurance risk of 'silent AI'

There is growing recognition that AI is the next silent cyber. Put simply, claims are likely to be made under insurance policies for risks that are AI-related, even when those policies do not expressly cover AI-related risks. Examples include:

- Operational errors from machinery that uses AI which may lead to property damage or personal injury.
- Incorrect predictions made by AI, resulting in incorrect financial forecast or medical diagnoses, resulting in financial loss or medical negligence.
- Intellectual property (**IP**) infringement and third-party IP breach claims arising from information generated by AI.
- Data errors that cause bias, leading to claims of discrimination.

What are the implications of AI for insurers?

Given the significant risks and the silent coverage of AI related risks, insurers need to consider updating their policies to clearly define which AI-related claims are an insurable risk and the exclusions that may apply.

As a starting point, insurers may soon offer coverage for losses caused by AI only if the AI is identified, the associated risks are understood and managed, and the approach is compliant with relevant domestic law and policy [33].

In addition, insurers should look to:

- Gather detailed information from their insured on what AI is being used and where, including

embedded AI – that is, AI embedded in other non-AI systems.

- Undertake detailed risk assessments of the AI being used by the insured to determine the risks involved, how they are being managed, and then price accordingly.
- Request disclosure of the insured's regulatory compliance. For Australian Prudential Regulation Authority (**APRA**) regulated institutions, such as deposit taking institutions, superannuation funds and insurance companies, this may include disclosure of the steps taken to manage AI risk, such as having a comprehensive governance framework for identifying AI (including embedded AI in procured or existing systems) and measures to manage these risks.
- Provide education and training to policyholders about the risks associated with AI and how to manage those risks.
- Consider offering insurance products specifically designed for AI-related risks.

What are the implications of AI for the insured (i.e. government and industry)

For those holding insurance policies, including government and private sector organisations (superannuation funds, banks, financial services institutions, and corporates), the impact of the risks of AI and the inevitable insurance changes have significant consequences.

While some organisations actively deploying AI may be doing so in a manner that manages the risk and complies with Australia's AI related policy, the penetration of AI into goods, services, and infrastructure, leaves the vast majority of organisations (government, superannuation funds and private sector) exposed to the risk of acquiring an increasing volume of AI without fully understanding or managing the associated risks, which can extend throughout their entire supply chains.

Key recommendations

To address the risks associated with AI and ensure that AI-related risk are insurable, organisations should:

Identify AI use: Determine what AI technologies are currently being used (included embedded AI).

Manage AI acquisition:

- When expressly procuring AI, ensure that the procurement and subsequent management of the AI aligns with the Voluntary AI Safety Standard[34] as applicable.
- Recognise that nearly every procurement (of products, services, infrastructure etc) may include embedded AI (even if not explicitly requested) and ensure that these systems are understood and risk managed according to the Voluntary AI Safety Standard[35] , as applicable.

Conclusion

The concept of silent AI is akin to the earlier issue of silent cyber but could have even more severe consequences. As new AI systems with differing risks emerge on an almost daily basis, insurers must consider revising their underwriting procedures and guidelines. This revision should include detailed disclosure requirements for AI and clearly outlining which AI-related risks are covered and which are excluded, to mitigate the silent AI risk.

Businesses, superannuation funds and government must take proactive measures to understand and manage the AI systems they utilise, particularly those embedded within other systems. Failure to do so may result in an entity finding that their insurance policy does not respond.

Ultimately, close collaboration among the insurance industry, businesses, and government is essential to identify, allocate, and price these risks effectively. This collaboration will enable all parties to focus on exploring the vast potential of AI technology.

[34] Noting that Implementing the Voluntary AI Safety Standard now *will help businesses start to develop practices required in a future regulatory environment* as stated in the Safe and responsible AI in Australia proposal paper for introducing mandatory guardrails for AI in high-risk settings, published by the Department of Industry, Science and Tourism, 5 September 2024

[35] See above

AUSTRALIA'S DIGITAL DILEMMA: WHAT REALLY COUNTS AS AN ELECTRONIC SIGNATURE?

Authors: Aston Joppich (Partner) and Gabe McNamara (Lawyer)

In today's fast-moving digital economy, contracts and deals are increasingly sealed with a click, a typed name, or a sent email. However, as technology evolves faster than legislation, a crucial question remains: what constitutes a valid electronic signature under Australian law?

This is where the *Electronic Transactions Act 1999* (Cth) (**ETA**) and its state equivalents comes into play. This legislation aims to modernise traditional contract law for the 21st Century. While the ETA opens the door for digital dealings, it notably lacks a clear definition of what an 'electronic signature' actually is. For lawyers, businesses, and everyday users, this ambiguity can be the difference between a binding agreement and a costly misunderstanding.

No wet ink? No worries ... sometimes

The primary intention of the ETA is to ensure that a transaction isn't invalid simply because it happens electronically. Whether it's a contract, agreement, or a legal declaration, as long as the parties can be identified and their intent is clear, digital communications can carry full legal force.

So, what qualifies as a valid electronic signature? The answer lies in three simple but nuanced criteria:

1. The method identifies the person and their intent to sign the document.
2. It's reliable under the circumstances.
3. The parties agree (either explicitly or implicitly) to the use of that method.

Sounds straightforward, right? But in practice, the devil is in the digital details.

Broad definitions, real risks

The ETA adopts a broad, functional view of electronic signatures. Forget formalities like styluses or signature pads; even just typing a name at the end of an email can do the job. This low threshold aims to keep the law adaptable to new technologies, but it also opens the door to confusion.

For example, courts have held that simply signing off with a name and email address may be enough to fulfil the signature requirement. In *Bullhead Pty Ltd v Brickmakers Place*, that combination satisfied the signature requirement. Similarly, in *Stellard Pty Ltd v North Queensland Fuel Pty Ltd*, the Court allowed additional evidence to help determine identity and intent.

However, in *Russells Solicitor v McCardel*, the Court made it clear: there is no one-size-fits-all list of what constitutes a signature. Everything depends on the context.

Reliability: a signature's silent strength

The second component of the test—reliability—focuses on whether the method used can link the signature to the person who made it. Importantly, the law does not require a typed name or scanned signature; even a simple mark that reliably identifies the signer and confirms their intent can suffice.

This was illustrated in *Attorney-General (SA) v Corporation of the City of Adelaide*, where a solicitor's name and certification in an email were found to be reliable and valid.

However, reliability must reflect the specific context. A method that works in one scenario might fall short in another. This brings us to one of the more ambiguous areas of the ETA: the automatic email signature.

Not all signatures are made equally

An automatic email footer (the pre-filled lines with your name, title, and contact information) may seem like a signature, but the courts have taken a stricter view. Since these footers are inserted without the sender's direct input, they may not count as a signature at all.

In contrast, a deliberately typed name in an email body clearly demonstrates the intent to be bound. This subtle difference could determine the enforceability of a million-dollar deal.

Solicitors: beware the "accidental contract"

For legal practitioners, the rules surrounding electronic signatures can have even greater implications. Courts have found that lawyers, as agents of their clients, can bind their clients to agreements just be hitting send on an email.

This risk is especially high during the final stages of contract negotiations. Without clear disclaimers or warnings indicating that no binding agreement is intended until all parties have signed a final document, lawyers could inadvertently commit their clients to terms that haven't been finalised.

Lessons for the digital age

What does this all mean for everyday users and businesses? Here are some key takeaways:

Be deliberate. Don't rely on auto-signatures if you don't intend to sign.

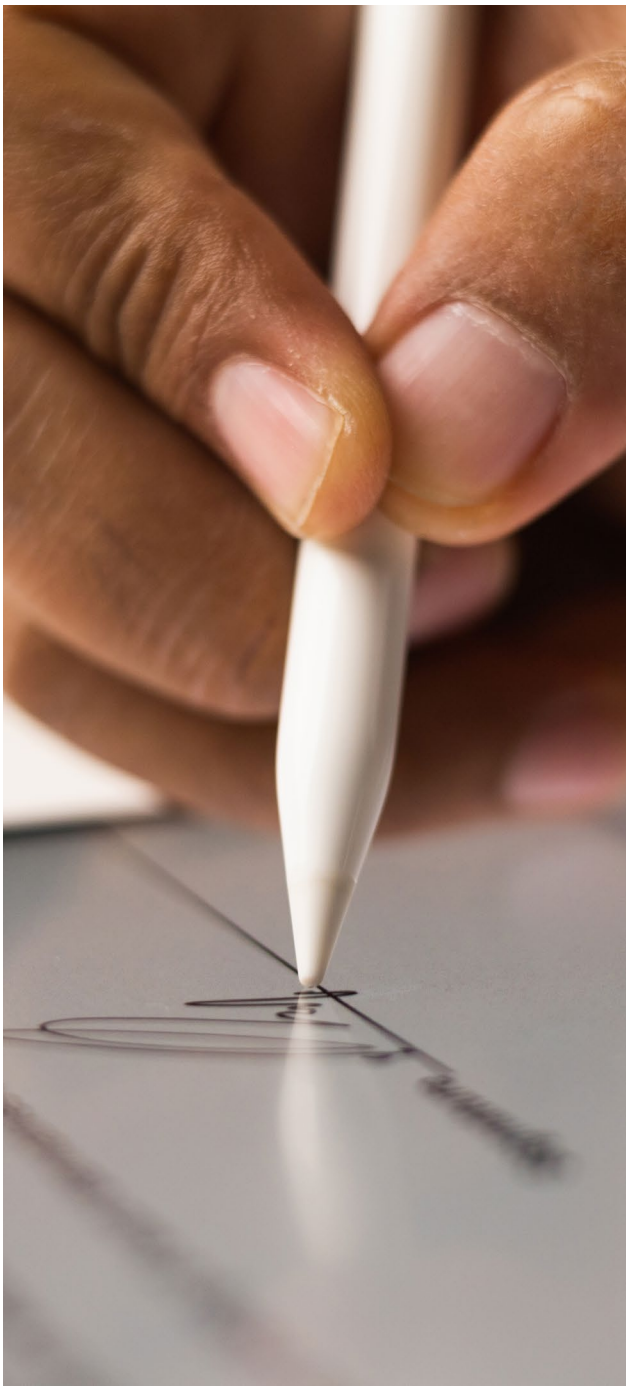
Be clear. If you're negotiating but not ready to commit, say so explicitly in writing.

Be cautious. Assume that anything you send electronically could potentially bind you.

For legal professionals, remain vigilant. Use disclaimers in emails, confirm when final agreements are intended, and never underestimate how a casual email can turn into a binding contract.

The final word

As Australia navigates a digital-first future, the ETA offers flexibility but demands caution. In a world where signatures are just as likely to be typed as they are penned, understanding the law is not just helpful—it's essential. Whether you're signing off on a deal or advising a client, remember that in the digital age, every click counts.



THE HIDDEN THREAT: RISING CYBER INCIDENTS IN AUSTRALIA AND THE URGENT NEED FOR CYBER INSURANCE

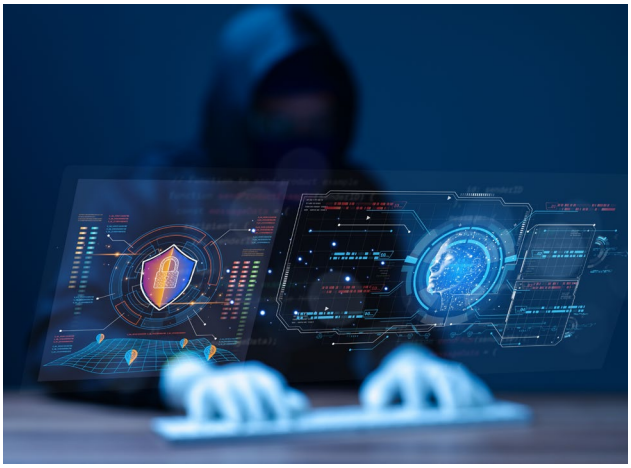
Author: Jehan Mata (Partner), Dinah Amrad (Associate), and Maxwell Watson (Paralegal)

Cyber incidents are recognised as one of the key risk facing businesses globally. This risk has rapidly reached Australian shores, driven by technological advancements that have enhanced the capabilities and threats posed by cybercriminals and state actors. The Australian Signals Directorate Cyber Threat Report (**CTR**) identifies the most reported forms of cybercrime as email impersonation attacks, fraud, ransomware, and data theft extortion.

Prime targets for cybercriminals

The Australian Cyber Security Centre warns that small to medium-sized enterprises (**SMEs**) are particularly vulnerable to these risks due to insufficient cybersecurity defences. According to the CTR, the high financial burden of cybercrime is significant; SMEs lose an average of $49,600 per incident, medium businesses $62,800, and large businesses $63,600. The Office of the Australian Information Commissioner noted a significant increase in cybercrimes in the first six months of 2024, with 527 data breach notifications, marking the highest level in three and a half years.

Industries most frequently targeted by cyber attacks including healthcare and financial services, with the education sector also being a significant target.



The role of cyber insurance

As cyber threats become more sophisticated, cyber insurance is becoming an essential measure to mitigate financial and operational risks. While policies vary, cyber insurance typically provides financial protection against incidents that involve:

- forensic investigations to determine the breach source
- data restoration and system recovery
- customer notification and rectification services
- regulatory fines and penalties
- legal advice on ransom payments and compliance, and
- business interruption losses due to cyberattacks.

In addition, some insurers offer negotiation services for ransomware incidents and indemnification for ransom payments.

Impact of AI on cybersecurity

The integration of AI into cyber operations is rapidly increasing the sophistication of cyber threats and the effectiveness of cybersecurity measures. AI technologies enhance real-time threat detection and automated defensive responses. However, cybercriminals and malicious state actors are also leveraging AI to conduct highly targeted attacks, such as deepfake-based fraud, automated phishing campaigns, and adaptive malware. As these threats evolve, Australian businesses must proactively strengthen their cybersecurity posture to safeguard digital assets and prevent financial losses.

Meanwhile, the emergence of AI raises new concerns, such as the potential for 'silent AI'—unintended coverage for losses resulting from the implementation, embedded or otherwise, of AI technologies and unforeseen risks. This highlights the need for insurers to stay informed about economic and legal trends that could affect AI-related claims on traditional policies. Underwriters should investigate how their insureds utilise AI to evaluate these risks. See 'Silent AI' article on page 15.

Privacy reforms

In Australia, the second tranche of the upcoming privacy law reforms (**Tranche 2**) is expected to amplify the financial risks associated with cyber incidents, underscoring the importance of cyber insurance in managing potential liabilities. Stricter regulations on data protection and breach reporting will impose substantial penalties and could lead to reputational damage for non-compliance. Notably, the removal of the small business exemption under Tranche 2 will significantly expand compliance obligations.

Furthermore, mandatory reporting of ransomware and cyber threat payments recently come into effect for all entities with annual revenue of $3 million or more.

Key takeaways

For SMEs / businesses

Given that even minor cybersecurity incidents can have significant financial impacts on SMEs, the Australian Cyber Security Centre recommends simple and cost-effective measures to improve cybersecurity, such as enabling multi-factor authentication, updating software, and backing up information. SMEs should also consider cyber insurance as an added protective layer to mitigate risk exposure. This can ensure that any breaches can be promptly and efficiently addressed by an experienced breach coach.

Businesses should proactively assess their cybersecurity frameworks, invest in robust data protection strategies, and secure cyber insurance to safeguard against potential regulatory penalties and financial losses.

For insurers

For insurers, the key takeaway regarding cyber insurance is that the market is constantly evolving, with increasing demand as well as growing risks and challenges. Although premiums are decreasing in some areas due to competition and improved awareness, the frequency and severity of claims remain high. This situation requires insurers to carefully manage their risk appetite and capacity.

As a final note, while the Federal Government has committed $15 billion to strengthen the current cybersecurity framework, the high level of risk in this space indicates that the private sector must prepare for increasingly costly digital challenges in the near future.

MANDATORY REPORTING OF RANSOMWARE AND CYBER EXTORTION PAYMENTS

Authors: Marianne Robinson (Special Counsel)

According to the Report of the **Australian Cyber Network State of the Industry Report** in April 2024, Australia is one of the top five most targeted nations for cyber threats against critical infrastructure in the world; on average a cybercrime report occurs every six minutes.

It should come as no surprise with these types of statistics that the Federal Government has taken steps to record incidents that seriously prejudice or are seriously prejudicing:

- the social or economic stability of Australia or its people, or
- the defence of Australia, or
- national security.

Mandatory reporting obligations commenced 30th May 2025

One of the key objectives of the *Cyber Security Act* 2024 (the **Act**) is to *'encourage the provision of information relating to the provision of payments or benefits (called ransomware payments) to entities seeking to benefit from cyber security incidents by imposing reporting obligations on entities in relation to the payment of such payments or benefits.'* (Section 3(b))

Mandatory reporting obligations are imposed by Part 3 of the Act. The reporting obligations are imposed on entities that have been impacted by a **cyber security incident** and made a ransomware payment to an entity seeking to benefit from the impact or the cyber security incident.

Incidents where the obligation to report is triggered

Part 3 applies when:

- an incident has occurred, is occurring or is imminent, and
- the incident is **a cyber security incident**, and
- the incident has had, is having, or could reasonably be expected to have, a direct or indirect impact on a reporting business entity, and
- an entity (the **extorting entity**) makes a demand of the reporting business entity, or any other entity, in order to benefit from the incident or the impact on the reporting business entity, and
- the reporting business entity provides or is aware that another entity has provided on their behalf, a payment or benefit (a **ransomware payment**) to the extorting entity that is directly related to the demand.

What is a cyber security incident

An incident is a cyber security incident for the purposes of the Act if:

a. the incident involves a critical infrastructure asset, or

b. the incident involves the activities of an entity that is a corporation to which paragraph 51(xx) of the Constitution applies, or

If the incident is or was effected by means of a telegraphic, telephonic, or other like service within the meaning of paragraph 51(v) of the Constitution (including, for example, by means of the internet); or (d) the incident is impeding or impairing, or has impeded or impaired, the ability of a computer to connect to such a service, or (e) the incident has seriously prejudiced or is seriously prejudicing:

i. the social or economic stability of Australia or its people, or

ii. the defence of Australia, or

iii. national security.

Who has to report a payment?

An entity must comply with reporting obligations if, at the time the ransomware payment is made, it is conducting a business in Australia with an annual turnover that exceeds the $3 million threshold for the previous financial year.

The term 'entity' can refer to an individual, body corporate, partnership, unincorporated association with a governing body, a trust, or a responsible entity for a critical infrastructure asset as defined under Part 2B of the *Security of Critical Infrastructure Act 2018*. Commonwealth or state bodies are excluded from these obligations.

What constitutes a payment

The legislation captures *both* **monetary** and **non-monetary benefits** that are given or exchanged with an extorting entity, constituting **ransomware or cyber extortion payments**. This may include gifts, services, or other benefits to an entity provided in response to the demand.

Information to be reported

The reporting must be in the format required by the Australian Signals Directorate, which is designated as the information collector by the Department of Home Affairs.

Section 7 of the *Cyber Security (Ransomware Payment Reporting) Rules* 2025 prescribes the information required for a ransomware payment or cyber extortion report. This information includes the following, where it is known or able to be known by reasonable search or enquiry:

- The contact and business details of the entity that made the payment, including an Australian Business Number (**ABN**).
- Details of the cyber security incident, including its impact on the reporting business entity.
- When the incident occurred or is estimated to have occurred.
- When the reporting business entity became aware of the incident.
- The impact of the incident on the reporting business entity.
- The impact of the incident on the reporting business entity's customers.
- What variant (if any) of ransomware or other malware was used what vulnerabilities (if any) in the reporting business entity's systems were exploited; and information that could assist the response to, mitigation or resolution of the cyber incident by a Commonwealth body, or state body. For example, this may include the Australian Signal's Directorate or the Australian Cyber Security Centre.
- The other entity's contact and business details including the ABN and address (in cases where the ransom was paid by another entity).
- The demand made by the extorting entity o the amount or quantum of the ransomware or cyber extortion payment (including non-monetary benefits) demanded and the method of provision demanded the ransomware payment.
- The amount or quantum of the ransomware or cyber extortion payment (including non-monetary benefits) given and the method of provision.

- Communications with the extorting entity relating to the incident, demand and the payment.
- The nature and timing of any communications with the extorting entity.
- A brief description of those communications (if any).
- A brief description of any pre-payment negotiations undertaken in relation to the ransomware demand or payment.

Timeframe for reporting

Entities have **72 hours to make a ransomware or cyber extortion payment report** from the time when the ransomware or cyber extortion payment is made, or from the time the entity is aware that a payment has been made on its behalf.

Lessons from maritime pirates

For centuries, ship owners and maritime insurers have been forced to develop policies on how to deal with extortion demands from pirates who take control of ships, cargo and crew. Ince & Co, once an international law firm that monitored piracy demands, estimated that ransoms of about US$75 to US$85 million were paid in 2010 to secure the release of 21 ships. By March 2011, it was estimated that the average ransom payments had reached about US$4 million, doubling the figure from January 2010. This was the period where the threats from Somali pirates were at their peak.

Shipowners established predefined response protocols and guidelines on how to collaborate with security partners and engage expert crisis management specialists to ensure they are equipped to navigate complex security incidents. Key to managing these risks is the collaboration among shipowners, insurers, security professionals, and even the navies of various countries to deter piracy and extortion demands. The kidnapping of crew and the very real threat to life have been motivating factors for this approach.

However, one key aspect to the risk management is that very little is known about ransom payments outside this closely-knit insurance sector. This confidentiality is intentional to prevent encouraging further acts of piracy.

Where to from here

As with any new legislation imposing compliance obligations and penalties for non-compliance, the new mandatory reporting obligations requires impacted entities to develop and implement policies and protocols in advance of a ransomware or cyber extortion event.

Each entity must determine its approach to extortion demands, which will vary according the risks it faces. Factors to consider include the nature of the information at risk of exposure, the value of the information to the entity or its own clients, and the potential for such information to be sold to the dark web or made public.

It is important for entities to establish their position on payment of extortion demands in advance and develop processes for managing such situations. With the proliferation of cyber breaches and the extortion demands made on high profile Australian companies, including law firms and a Law Society, the likelihood of facing demands is rapidly rising. Being prepared in advance can save more than just reputations – it can save individuals.

ENFORCING FORCE MAJEURE IN A 'SAASY' ENVIRONMENT

Authors: Jason Kwan (Partner) and Zach Smale (Associate)

Force majeure clauses have gained renewed attention following the CloudStrike outage in 2024. With a shift away from traditional on-premise software to cloud-based software-as-a-service (**SaaS**) solutions such as CloudStrike, organisations should consider the implications for force majeure clauses and make sure they are adequately protected.

In this article we set out some of the key issues to keep in mind.

What is SaaS?

Traditionally, software was installed and run on a company's own hardware infrastructure, within the company's physical premises (**On-Prem**).

In recent times, On-Prem is being replaced with cloud-based SaaS solutions. In this model, the same software now sits in the cloud, allowing multiple customers to access the same core product simultaneously. The SaaS provider will typically provide unique configurations for its customers, making the core product compatible with their system.

The economies of scale afforded by SaaS translate into costs savings for the customer, who does not need to maintain servers or as many in-house IT experts. However, SaaS can also come with a greater risk of service failures that are beyond the customer's control.

Service failures can range from minor bugs to critical system outages. The CloudStrike incident was an example of both. A minor update intended to patch systemic bugs unintentionally blocked user access to entire operating systems—turning a routine patch into a sudden economic shutdown. Additionally, SaaS solutions are also vulnerable to malicious attacks targeting either the provider or the cloud host.

What is force majeure?

Force majeure is a concept derived from the French Civil Code, referring to extraordinary events or circumstances beyond a party's reasonable control that prevent or delay performance of contractual obligations. Due to its origin, there is no equivalent concept in Australian common law. Accordingly, in the absence of an express force majeure clause, a party cannot rely on a parallel common law doctrine to excuse non-performance.

Why might force majeure pose particular concerns for SaaS customers?

Business continuity is an important concern for customers contracting with SaaS providers, especially for critical solutions. With On-Prem, businesses have control and access to the software in the event of a failure. In contrast, with SaaS customers must rely on the SaaS provider's infrastructure and their ability to restore service in the event of an outage.

For this reason, SaaS agreements will typically include a service level agreement (**SLA**), which sets out service levels relating to the availability of the solution, along with response and resolution times where support is provided. These service levels should be backed up by the obligation on the SaaS provider to pay service credits and with appropriate termination rights. SLAs will usually have a list of specific exclusions, including force majeure events.

For customers regulated by APRA CPS 230 (Operational Risk Management), certain provisions must be included in agreements with material service providers. These include a force majeure clause that indicates the parts of the agreement that will continue upon the occurrence of a force majeure event.

Important consideration when negotiating a force majeure clause

The following are important considerations when negotiating a force majeure clause:

1 Definition of 'force majeure event'

A 'force majeure event' is typically defined by a list of circumstances including acts of God, natural disasters, and war, followed by a catch-all phrase such as 'all other events beyond the control of the parties'. In On-Prem scenarios, a force majeure event may extend to failures in the customer's own infrastructure or network that prevent the customer's ability to install, operate, and maintain the software. In SaaS contexts, force majeure events often include triggers related to the vendor's infrastructure, network, operations, or third party providers.

Parties should agree the boundaries of what falls within a force majeure event and when liability for service performance failures is excluded. Examples of issues include:

Cloud and data centre failures: SaaS platforms are hosted in virtual environments supported by cloud infrastructure, which rely on physical data centres. Failures in either layer, virtual or physical, can cause a full-service outage. On-Prem systems are less vulnerable since they operate on infrastructure under the customer's control.

Cybersecurity attacks: SaaS applications, being internet-facing, are more exposed to threats like Distributed Denial of Service (DDoS) attacks. Even with robust security in place, such attacks can severely disrupt service availability. If the provider has taken all reasonable preventive measures, these incidents may be treated as force majeure events.

Third-Party integration failures: Many SaaS platforms integrate with external systems (e.g. banks, payment gateways, logistics platforms) to deliver real-time data and functionality. If one of these external services fails, it can impact the performance or usability of the SaaS solution. On-Prem software generally does not have this level of reliance.

Recently, we have observed organisations attempting to expressly exclude the failure of a service provider from the definition of a 'force majeure event'. Inevitably, however, SaaS providers will argue that they cannot ultimately control the actions of their service providers, and that this scenario is no different from any other event beyond their control.

Depending on how force majeure events are defined, a circumstance that causes performance to become more burdensome or expensive is unlikely to qualify as a force majeure event, particularly where other alternative means of performance are available.

If there are specific circumstances a party is concerned about, it should look to articulate these in the agreement.

2 Ensuring a causal connection

A party should only be excused from non-performance to the extent caused by the force majeure event. Occasionally, the language in contracts is vague, which can lead to a party attempting to excuse any non-performance simply due to an occurrence of a force majeure event—rather than the non-performance being directly attributable to it. The wording should be reviewed to ensure the counterparty cannot use the occurrence of a force majeure event to avoid their obligations more broadly.

It is also advisable for the parties to specify certain obligations, such as the customer's payment of the license fees that are intended to survive during force majeure events, removing any argument over causation.

3 Requirement to mitigate

Ideally, an express obligation should be included for the parties to mitigate any loss or delay arising from a force majeure event and for the parties to continue to perform all other unaffected obligations. It may be possible to imply a mitigation obligation in certain circumstances, but it is preferable to point to an express obligation, especially in turbulent situations, where such clauses are often invoked.

4 Right to terminate

Likewise, the parties should include an express right to terminate the agreement upon written notice if the force majeure event continues for a certain period of time, rather than relying on an implied right of termination. Consideration should be given to whether this termination right should benefit both parties or just the party not invoking the force majeure event.

Conclusion

With the growing popularity of SaaS, organisations should consider the associated risks, particularly the potential for service failures and the circumstances in which a SaaS provider may rely on force majeure provisions to excuse non-performance. A well-crafted force majeure clause should reflect the nature of the agreement and provide balanced protection for both parties in the face of events beyond their control.

Our promise to you

A client first approach

Your success is our success and we wouldn't have it any other way. With our client first commitment we adopt a long-term, mutually respectful approach to our relationship. We are committed to delivering high-quality, pragmatic and market relevant service.

National coverage

We are future ready. This means we can deliver genuine national capacity and expertise to our clients right now, and into the future. We are large enough to be a national commercial law firm, but small enough to have a local and personal touch, and believe we offer value with targeted and responsive legal support.

Pragmatic matter management

We work with you to understand your needs and the market you operate in. We develop pragmatic, timely and cost effective solutions with you. Our experience in and knowledge of the Hunter Region means we have an understanding of this market which is unparalleled.

The right team and capacity

Service consistency starts with the right combination of people, with the right experience, capacity and availability. We constantly review performance, including outcomes and client satisfaction to improve our service delivery. We will listen to you carefully, engage with you proactively to identify your needs and bring together the right team for your particular requirements.

A commitment to diverse and inclusive thinking

We want all our people to bring their whole selves to work, to be comfortable putting forward their opinions, and bringing fresh ideas to the table for the benefit of our clients.

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

Alexandra Wedutenko
Projects & Government Commercial
Partner
t: +61 2 6263 6378
e: alexandra.wedutenko@sparke.com.au

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

Mark Doepel
Commercial Insurance
Partner
t: +61 2 9260 2445
e: mark.doepel@sparke.com.au

Robert Watson
Projects & Government Commercial
Partner
t: +61 3 9291 2388
e: robert.watson@sparke.com.au

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

Adam Payne
Projects & Government Commercial
Special Counsel
t: +61 2 9260 2410
e: adam.payne@sparke.com.au

Kelly Matheson
Government Public & Regulatory
Special Counsel
t: +61 2 6263 6309
e: kelly.matheson@sparke.com.au

Contributing authors

Thank you to our additonal authors for their contributon

Aston Joppich
Corporate & Commercial
Partner
t: +61 7 3059 6303
e: aston.joppich@sparke.com.au

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

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

Zach Smale
Corporate & Commercial
Associate
t: +61 2 9373 3596
e: zach.smale@sparke.com.au

Georgie Aidonopoulos
Commercial Insurance
Lawyer
t: +61 3 9291 2235
e: georgie.aidonopoulos@sparke.com.au

Gabe McNamara
Corporate & Commercial
Lawyer
t: +61 7 3016 5177
e: gabe.mcnamara@sparke.com.au

Georgia Mineo
Commercial Insurance
Lawyer
t: +61 3 9291 2317
e: georgia.mineo@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

www.sparke.com.au

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