RETHHINKING CONTRACTS IN THE AI ERA

MANAGING HIDDEN AI RISKS IN YOUR SUPPLY CHAIN

PRESENTED BY

DANIEL KILEY | PARTNER | ADELAIDE

March 2026

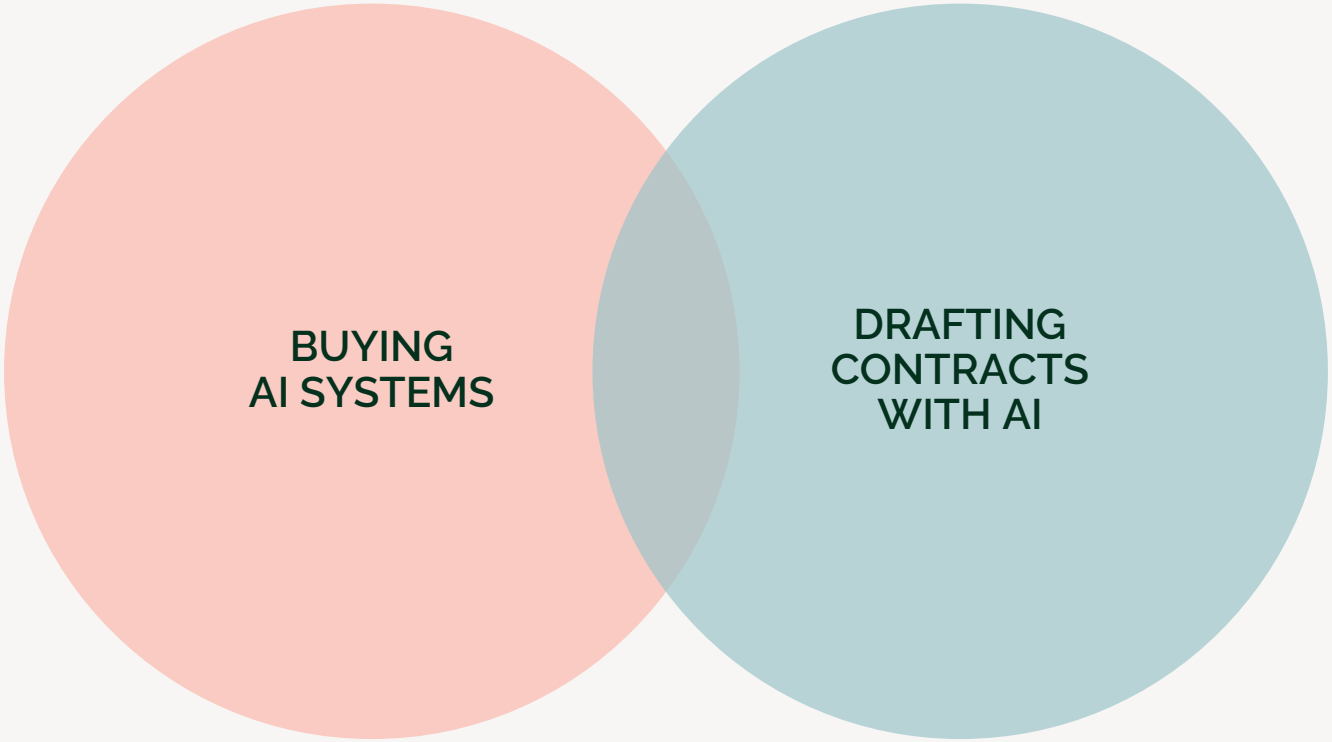
HWLE LAWYERS

ACKNOWLEDGEMENT OF COUNTRY

HWLE would like to acknowledge the Traditional Custodians of the land on which we are today. We would also like to pay our respects to Elders past and present.

HWLE
LAWYERS

What today is not



HWLE
LAWYERS

Procuring services in an AI-enabled world

- This is about services, not software
- AI is being increasingly used as part of service delivery, often invisibly
- Contracts which assume human services may no longer be fit for purpose
  - New risks
  - Rethink assumptions
  - Consider liability positions

HWLE LAWYERS

Procuring services in an AI-enabled world

ACCOUNTING TIMES

Deloitte to refund government after using AI in $440k report

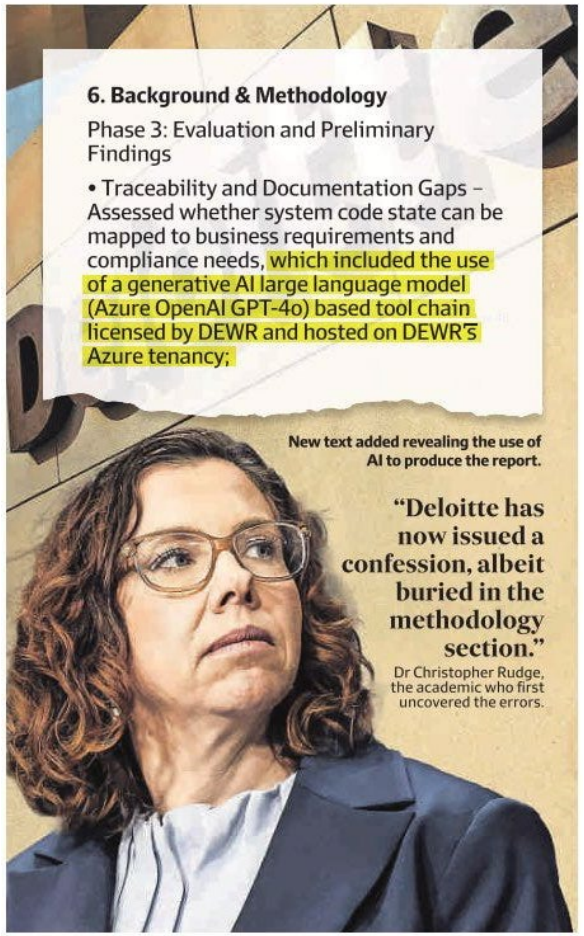
Technology | 09 October 2025 | Daniel Croft

Deloitte will partially refund the Australian government $440,000 after the company admitted to using AI to write a report for the government, which ended up being full of mistakes and made up points.

- Deloitte government report provides a practical example
  - AI assisted drafting used in a public sector advisory context
  - Fabricated citations and unverifiable sources generated by AI
  - Real world consequences: reputational damage, legal exposure, significant reimbursement for fees and failure to deliver value for money

▶ Auditor admits AI used in $440k report

Deloitte to pay for AI mistakes



Amanda Rishworth's department will receive a refund from Deloitte.

HWLE LAWYERS

What has changed in service delivery

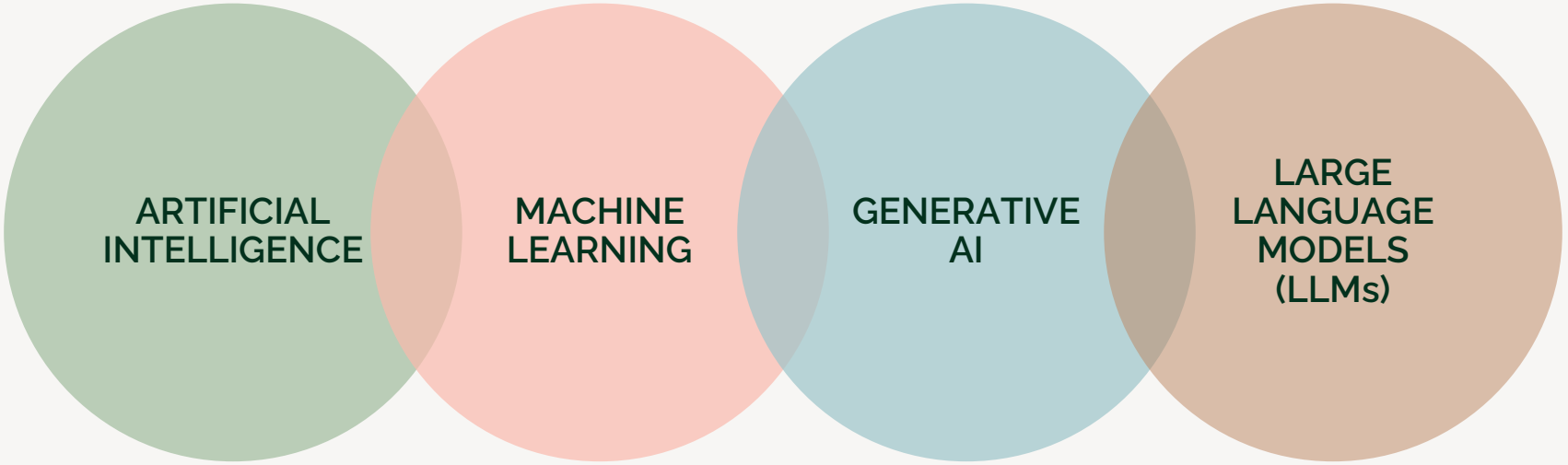
HWLE
LAWYERS

What has changed in service delivery

- Professional services are no longer delivered solely through human driven processes
- AI is increasingly embedded within everyday workflows, often operating alongside or upstream of human judgment
- In many engagements, AI is not a standalone tool but an integrated component of how work is produced reviewed and refined
- This means the use of AI may not be obvious from the final deliverable or disclosed in the contract
- Common service functions now routinely AI assisted
  - Data entry and classification
  - Drafting, summarisation, and analytical work
  - Research, source identification, and report generation

HWLE LAWYERS

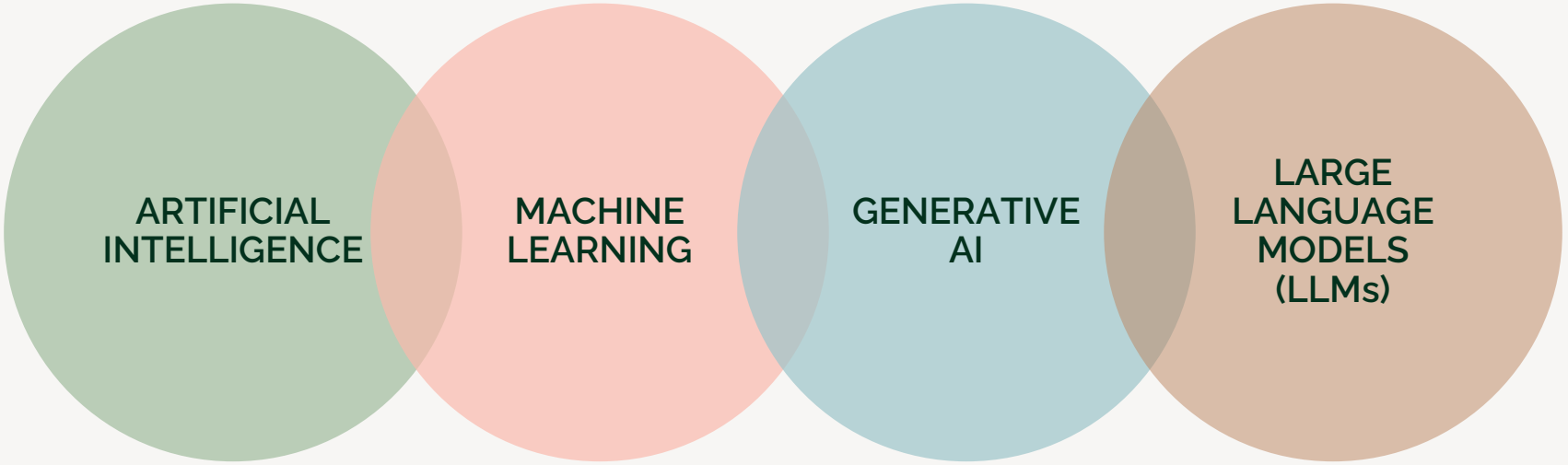
Taxonomy



AI describes an engineered system that generates outputs (such as content, forecasts, recommendations or decisions) for a given set of human-defined objectives or parameters without explicit programming

HWLE LAWYERS

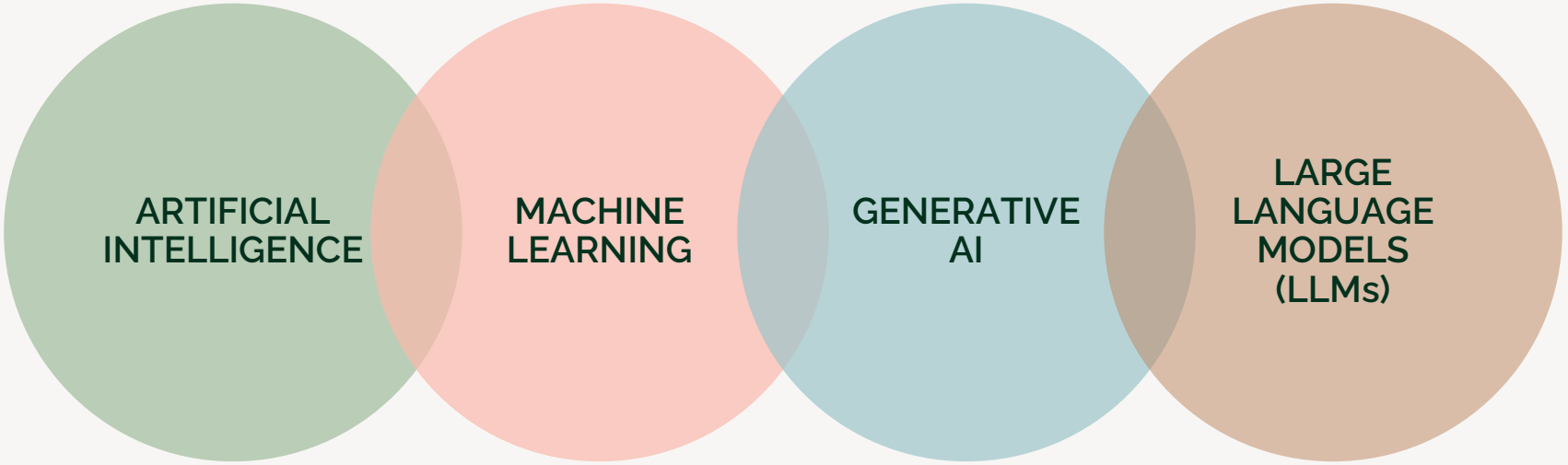
Taxonomy



Machine learning systems are trained using existing data

HWLE LAWYERS

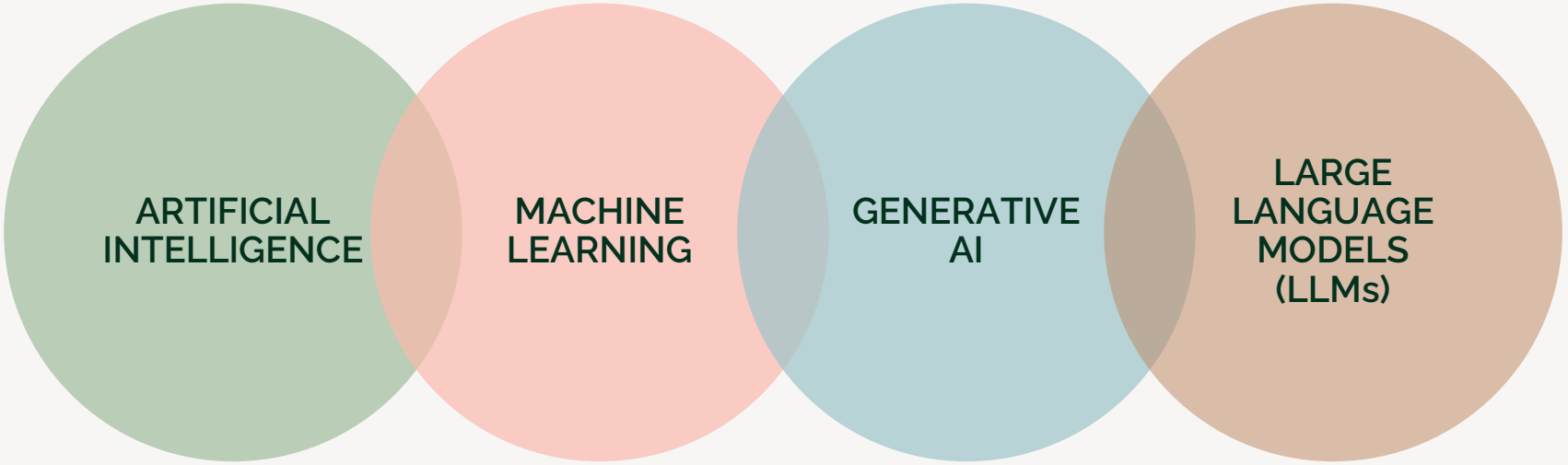
Taxonomy



Generative AI systems generate substantive output – text, images, code, video

HWLE LAWYERS

Taxonomy

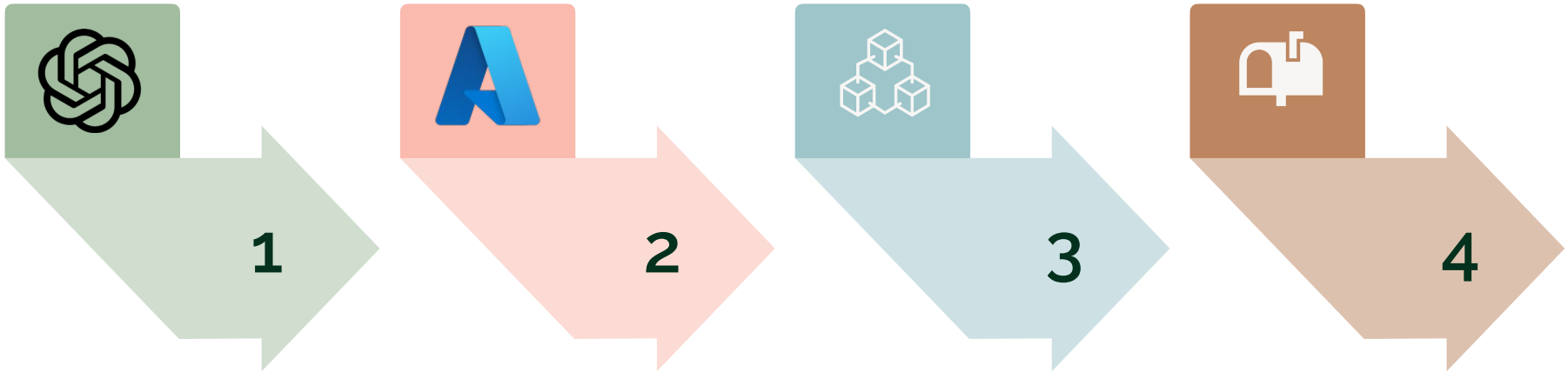


Large Language Models (**LLMs**) are a specific type of machine learning system which generate text

HWLE LAWYERS

The sub-processor problem

- Many Service Providers do not operate AI systems end to end
- Instead, they build their delivery workflows on top of multiple third-party platforms, for example:



Foundation Model Provider

Such as OpenAI's ChatGPT or Anthropic's Claude

Cloud Infastructure Provider

Such as Microsoft Azure, per Deloitte example

Service Provider Workflow

Data processing, or document analysis tool of Customer materials or customer data

Service Deliverable

Deliverable provided without knowledge of previous steps

HWLE LAWYERS

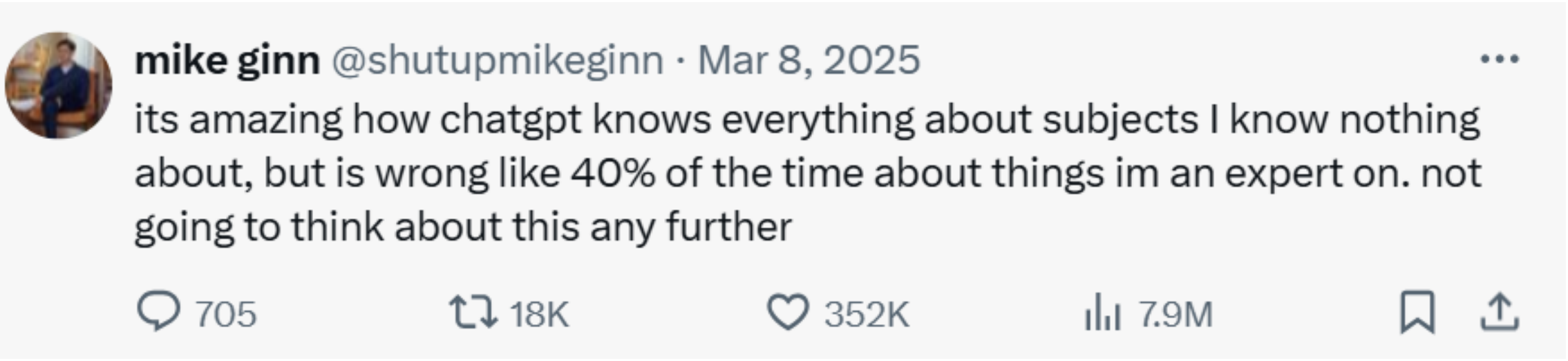
"Generative AI and Large Language Models create output that is not the product of reasoning… They use probability to predict a given sequence of words. Output is determined by the information provided to it and is not presumed to be correct."

SUPREME COURT OF VICTORIA

HWLE LAWYERS

"You should watch for the '**plausibility bias**': the fluency of ChatGPT can induce a **false sense of credibility**. If you are unfamiliar with the area… in question, you may miss subtle or even gross inaccuracies in a ChatGPT text." VICTORIAN LEGAL SERVICES BOARD & COMMISSIONER

HWLE LAWYERS



HWLE LAWYERS

Key risk categories in AI-enabled service delivery

1 INACCURACY

Outputs may contain hallucinations, fabricated sources, or subtle errors that are not obvious on review

2 DATA RISKS

Data is sent to AI vendors, adding new privacy, confidentiality and re-use risks

3 OPAQUENESS

How outputs are generated, reviewed, or influenced by AI may not be visible or auditable

4 IP ISSUES

Ownership, originality, and enforceability of rights in AI-generated outputs may be uncertain or absent

HWLE LAWYERS

Traditional contracting assumptions that may no longer hold

HWLE
LAWYERS

Traditional contracting assumptions that may no longer hold

- AI systems are probabilistic by design, meaning identical inputs can produce different outputs
- Many services clauses implicitly rely on human creation and judgment
  - Where AI generates or materially shapes content, those assumptions no longer reliably support IP ownership, originality warranties, or professional responsibility
- In conventional services, errors signal failure. In AI enabled delivery, risks such as hallucinations, fabricated sources, and bias are known and foreseeable
- Assumptions that pricing reflects labour inputs, such as traditional fee structures are built around human effort

HWLE LAWYERS

Deciding whether to permit AI in service delivery

1 EFFICIENCY

AI can reduce cost, accelerate delivery, and enable services that would not be commercially viable using human effort alone

2 QUALITY

AI-assisted outputs may be faster, but can introduce variability, hidden errors, or reduced explainability

3 ACCOUNTABILITY

Permitting AI shifts how responsibility, review, and verification operate within the service model

4 RISK

AI may be appropriate for low-risk or internal outputs

Contractual risk allocation may influence risk appetite

5 COMMERCIALS

Does AI use change pricing models, delivery timeframes, or level of autonomy

HWLE LAWYERS

Deciding whether to permit AI in service delivery

The Service Provider may determine the manner in which the Services are performed and may use its personnel, tools, systems, processes, and subcontractors to deliver the Services. The Service Provider does not warrant that the Deliverables will be error-free.

The Service Provider **must not use any AI or machine learning systems** in performing the Services without the Customer's prior written **consent**. Where such use is approved, the Service Provider **remains fully responsible** for all Deliverables. The Service Provider must not permit any subcontractor or third party engaged in delivering the Services to use AI systems in processing Customer Data or generating outputs without the Customer's express approval, and **remains responsible** for all acts and omissions of those parties.

HWLE LAWYERS

Performance standards

HWLE
LAWYERS

Clauses to consider where AI is permitted

1 OUTPUT QUALITY

Deliverables must be free from material inaccuracies, misleading content, or fabricated sources, regardless of how they are produced

2 FITNESS FOR PURPOSE

Outputs must be suitable for their intended use and capable of being relied upon in the context contemplated by the services

3 HUMAN OVERSIGHT

Where AI is used, appropriate human review and validation has been applied before delivery of outputs

4 RESPON SIBILITY

Use of AI does not reduce or qualify the Service Provider's obligations, warranties, or professional responsibility

5 DISCLOSURE & COMPLIANCE

AI tools are used only in accordance with agreed scope, restrictions

Disclosure of how and when those tools used

HWLE LAWYERS

Liability caps

HWLE
LAWYERS

Why liability caps need re-thinking

- Services agreements often cap liability by reference to fees paid over a defined period, on the assumption that exposure broadly aligns with contract value
- AI-assisted delivery can create risks that are disproportionate to service fees and unrelated to routine performance issues
- The problem arises when:
  - all risks are forced under a single cap designed for a pre-AI delivery model; and
  - legacy caps reflect only the predictable failure, such as delay, rework, or service interruption; and
  - the use of AI might reduce the fees on which the cap is calculated
- AI introduces qualitatively new risks including:
  - fabricated authorities,
  - missed material issues,
  - discriminatory outputs, and
  - confidentiality breaches through AI workflows and third-party platforms

HWLE LAWYERS

Why liability caps need re-thinking

Downstream exposure can be significant

- Failures can trigger regulatory action, professional liability, or claims far exceeding value of services procured
- Treating AI failures as routine defects misprices risk
- Forcing systemic and reputational risks under a standard cap treats them as minor service issues.

What needs to change

- Routine service performance issues can reasonably sit under a fees-based cap
- AI-specific failure modes require carve-outs or enhanced caps to reflect their different risk profile

HWLE LAWYERS

Why liability caps need re-thinking

Liability

- The liability of a Party under this Agreement to the other Party for a breach of this Agreement, or in tort, or for any other common law or statutory cause of action or otherwise arising under and/or in connection with this Agreement is limited to the Total Contract Value.
- To the extent permitted by Law, neither Party shall be liable for any Consequential Loss suffered or incurred by the other Party in connection with this Agreement whether in contract, or in tort, or any other common law or statutory cause of action or otherwise.
- The limitations referred to in this clause, do not apply to liability for:
  - personal injury, including sickness and death;
  - loss of, or damage to, tangible property;
  - infringement of any Intellectual Property Rights;
  - loss of Customer Data; or
  - wilful misconduct, fraud or dishonesty.
- *Consider whether further exceptions may be required for specific AI risks*

HWLE LAWYERS

Why liability caps need re-thinking

- Where AI-generated outputs feed into your own services or advice, and your Service Provider as disclaimed liability for those outputs, there may be pressure to pass similar limitations downstream. *This approach has limits.*
- Statutory regimes such as consumer guarantees and unfair contract terms may restrict your ability to disclaim responsibility or shift risk to end users
- Caps that attempt to shift AI-related risk entirely to the Customer may not be operationally realistic where the Service Provider controls delivery methods, tools, and automation
- Liability caps ideally reflect where risk actually sits in practice, including reliance on outputs and advice
- Caps should be also assessed alongside indemnities to ensure they do not hollow out protection in circumstances where risk cannot legally or practically be shifted

HWLE LAWYERS

Insurance

HWLE
LAWYERS

Insurance

- Require professional indemnity insurance coverage via contract
  - Covers financial loss arising from reliance on advice
- Insurers may start:
  - Excluding liability for AI use
  - Interrogating use of AI as part of coverage decision
  - Placing conditions on how/when the policy applies if AI has been used
- Any contract clause should require that professional indemnity insurance is held *and* applies to the services being provided
  - Nothing done to prejudice application of policy

HWLE LAWYERS

Indemnities

HWLE
LAWYERS

Indemnities

- There is a risk that the output of Generative AI systems can regurgitate input data, creating infringing works
  - These risks are largely controlled by the tech company training and operating the foundation model
  - Some tech vendors provide customers with indemnities associated with these risks
- A downstream customer should consider looking for a corresponding indemnity from its relevant Service Provider
- In many cases, a standard IP infringement indemnity can address AI related risk without fundamental redesign, provided it is not weakened, such as:
  - knowledge qualifiers ('**to the best of the Service Provider's knowledge**' or '**work of its Personnel**') that effectively eliminate or reduce the scope of the indemnity;
  - limitations that narrow or technical use requirements that exclude ordinary, foreseeable use of the service or deliverables;
  - carve-outs that exclude claims arising from the Service Provider's subcontractors, downstream customers, third-party tools, or embedded technologies used in delivering the services

HWLE LAWYERS

Indemnities

The Service Provider will at all times indemnify and keep indemnified the Customer from and against any claims made against, or loss incurred by, the Customer where such claim or loss arises out of, in connection with, or in respect of any **infringement of the intellectual property rights** of a third party arising from the Customer's use of the Deliverables.

HWLE LAWYERS

Output ownership and IP rights

HWLE LAWYERS

Who owns what AI generates?

- Outputs generated by AI as part of service delivery may attract no copyright protection at all, if there is insufficient human authorship
- Copyright protection depends on:
  - an identifiable human author;
  - originality; and
  - independent intellectual effort
- Where AI materially generates or shapes content, the basis for ownership becomes uncertain or collapses entirely, and no copyright may exist
- Most standard ownership clauses assume that intellectual property exists
- If no copyright subsists in AI generated outputs, such clauses provide no exclusivity, no enforceable rights, and a false sense of protection

HWLE LAWYERS

Who owns what AI generates?

- You engage a graphic designer to produce artwork for an advertising campaign
- The designer uses AI tools to generate or materially shape the final artwork
- A competitor copies the artwork
- If there is insufficient human authorship, you may not be able to rely on copyright to stop the copying, even if your contract says you '**own**' the deliverables
- The commercial expectation of exclusivity exists, but the legal mechanism to enforce it may not

HWLE LAWYERS

Who owns what AI generates?

- Where AI materially generates outputs, copyright may not subsist at all
  - Reframe IP clauses away from ownership assumptions
  - Avoid assuming there is IP to 'own' and instead focus on enforceable use rights
- Internal stakeholders and Customers need to understand that:
  - traditional IP ownership concepts may not apply, and
  - control, exclusivity, and confidentiality may operate as the real levers in AI-enabled service procurement
- Focus on granting clear use and reliance rights over outputs to the Customer, rather than relying solely on vesting language that assumes intellectual property exists

HWLE LAWYERS

Who owns what AI generates?

(a) The Service Provider agrees that **ownership** of all Intellectual Property Rights in the Deliverables **automatically vest in the Customer** immediately upon creation, without the need for any further formality or documentation. Those Intellectual Property Rights will be entirely the property of the Customer in perpetuity.

(b) Any Intellectual Property Rights that the Service Provider **may otherwise possess** in the Deliverables will be deemed automatically **assigned** and transferred by the Service Provider to the Customer by this agreement. The Service Provider agrees to execute any documents reasonably necessary to confirm this fact.

HWLE LAWYERS

Ways to bolster ownership clauses

Substance of IP rights

- Bolster standard clause with :
  - obligation that Deliverables are created through identifiable human authorship sufficient to attract copyright;
  - obligation that key services are performed by personnel, with AI used only as a tool and not as the primary generator of content; and
  - warranty that Deliverables are capable of being owned, assigned, and enforced as intellectual property rights

HWLE LAWYERS

Ways to bolster ownership clauses

Confidentiality and Use Restrictions (to Approximate Ownership)

- Where intellectual property rights do not subsist, control and exclusivity can be added contractually
- Contractual limitations on Service Provider using, reusing, or disclosing Deliverables or outputs for any purpose other than performing the Services
- Restrict use of Deliverables for:
  - training, analytics, service improvement, or delivery to other customers.
- Treating outputs as confidential information, regardless of whether copyright subsists
- Limitations to this approach:
  - privity of contract
  - Deliverables that cannot be kept confidential

HWLE LAWYERS

Confidentiality and non-disclosure

HWLE
LAWYERS

Confidentiality and non-disclosure

- Standard confidentiality clauses assume risk arises from disclosure to third parties, not from internal reuse or model ingestion
- In AI-enabled services, confidential information may be processed, retained, or embedded in tools or models
- In services contracts, this issue is often obscured.
  - AI use can be framed as part of internal delivery rather than as feature or tool.
  - Standard services terms frequently permit broad data use for 'service delivery' and 'service improvement'
- Confidentiality obligations should address use of Customer information within automated or AI-assisted workflows, not just onward disclosure
- Survival periods and enforcement should reflect the persistence of data once incorporated into systems or models

HWLE LAWYERS

When you enter or upload your data into our services, we don't own that data but you grant us a licence to use, copy, transmit, store, analyse, and back up all data you submit to us through our services, including personal data of yourself and others, to:… allow us to improve, develop and protect our services; create new services; … and disclose to third party service providers and partners to enable and support such purposes.

HWLE LAWYERS

Confidentiality and non-disclosure

The Service Provider must keep the Customer's Confidential Information confidential and not **disclose** it to any third party except as permitted under this Agreement. Confidential Information does not include information that becomes public through no fault of the receiving party, was known prior to disclosure, is independently developed without reference to the Confidential Information, or is required to be disclosed by law.

The Service Provider must keep the Customer's Confidential Information confidential and not **disclose or use** it for any purpose other than performing the Services. For the avoidance of doubt, **use** includes processing, analysing, training, fine-tuning, improving, or embedding Confidential Information, or any patterns, structures, or derivatives derived from it, **in any automated system**, model, dataset, or tool that is not dedicated solely to the Customer. Confidential Information must not be retained or reused beyond the term of the Agreement except as required by law, and confidentiality obligations survive termination for five years.

HWLE LAWYERS

Privacy

HWLE
LAWYERS

Privacy

- Undisclosed use of AI by a Service Provider has potential to add new privacy risks
  - Disclosure of personal information to AI vendor (APP 6)
  - Disclosure of personal information to AI vendor *outside of Australia* (APP 8)
  - Errors in personal information arising as a result of AI hallucination (APP 10)
  - Automated decision making transparency will shortly be required to be detailed in privacy policies (APP 1.7)
  - Personal information used as part of further training of AI system (APP 6)
- If willing to permit AI usage by the Service Provider, consider drafting to address these risks

HWLE LAWYERS

Privacy

- Disclosure of personal information to AI vendor outside of Australia (APP 8)
  - Personal information (or *all* data) expressly required to remain in Australia
  - Could have trade-offs for the quality of AI tools available
- Errors in personal information arising as a result of AI hallucination (APP 10)
  - Warranties/liability for accuracy
- Automated decision making transparency will shortly be required to be detailed in privacy policies (APP 1.7)
  - Prohibition on use of computerised systems to make any decision that 'could reasonably be expected to significantly affect the rights or interests of an individual'
  - If significant decisions are expected to be made, require significant transparency
- Personal information used as part of further training of AI system (APP 6)
  - Restrictions on use of customer data for training purposes

HWLE LAWYERS

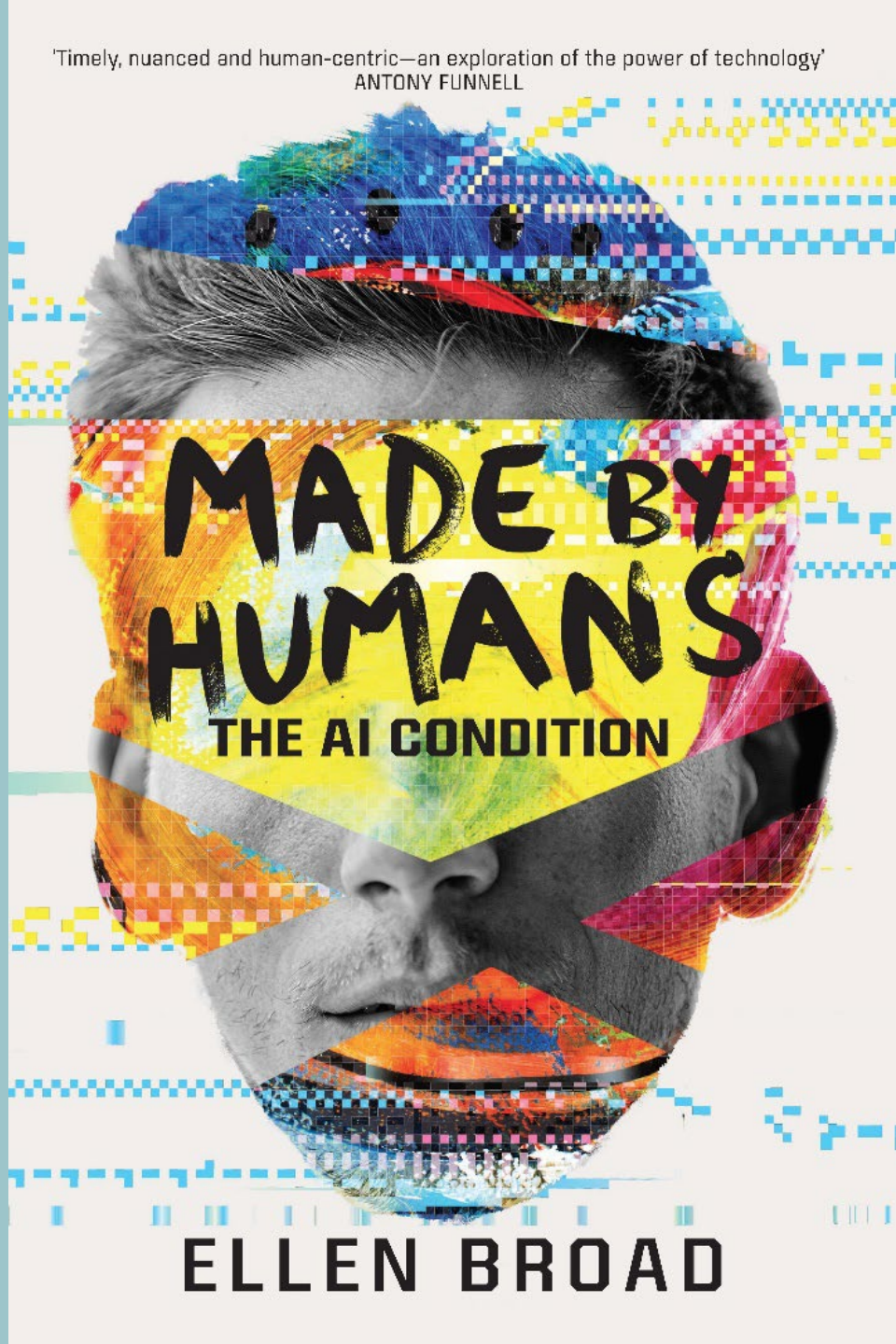
Audit rights

HWLE
LAWYERS

Machine learning is often described as being a '**black box**'— that is, precisely how it works and how decisions are made are impenetrable. What happens between practitioners inputting lots of data and getting their results can be **unclear**

This is not true of all machine learning models; some are more intelligible—that is, it is easier to trace through their decision-making process and understand them—than others

The problem is, **the least intelligible methods tend to be more accurate**



Audit rights

- AI systems cannot be audited in the same way as human work
- Traditional audit rights assume:
  - identifiable authors;
  - reviewable working papers; and
  - traceable decision-making
- In AI-enabled delivery, meaningful audit may require access to:
  - records of AI system use in the engagement;
  - prompt logs or input histories supplied to AI tools;
  - descriptions of model types or platforms used;
  - confirmation of whether outputs were logged, cached, or retained; and
  - certification of deletion across AI systems and third-party platforms
- Without express audit and certification rights, Customers may rely on assurances rather than verification

HWLE LAWYERS

Audit rights

The Customer may, on reasonable notice, audit the Service Provider's records and processes relating to the performance of the Services to verify compliance with this Agreement.

Where AI or automated systems are used in performing the Services, the Service Provider must, on reasonable request, provide the Customer with sufficient information to verify compliance with this Agreement, **including records of AI system use in the engagement, descriptions of the types of systems used, and confirmation of whether Customer Data or outputs were logged, retained, or reused**.

HWLE LAWYERS

Termination and transition out

HWLE
LAWYERS

Termination and transition out

Control on Exit

- Ensure clear rights to retrieve Customer data, outputs, and work in progress in a usable form, including material generated through AI-enabled workflows.

What remains after exit

Address what may persist after the relationship ends, such as prompts, drafts, logs, or derived materials, and how these are handled.

Post-exit restrictions

Consider restrictions on the Service Provider's use of customer data or outputs for training, analytics, or service improvement after termination.

Transition support

Termination clauses may provide for practical transition support, including data return, assistance with migration, and temporary continued access on agreed terms.

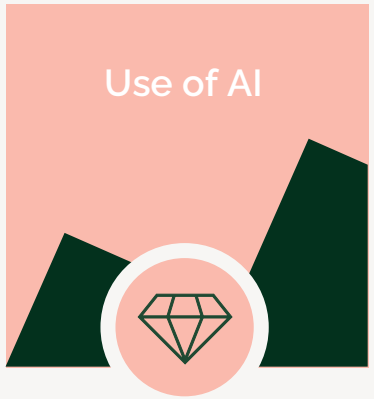
HWLE LAWYERS

Practical takeaways

HWLE
LAWYERS

Practical takeaways

Define the intended service and deliverable to procure, along with mechanism of ownership

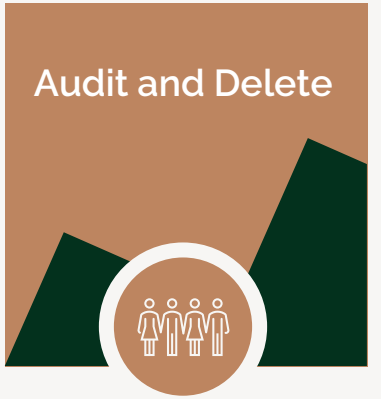


Is AI to be used by the Service Provider and how?

Does this effect the ownership position of the deliverable?

What data will be used and retained with the Service Provider? Where is the data held?

Look for 'improve,' 'enhance,' 'analytics,' 'aggregate'



What governance, review, audit and delete controls currently exist?

HWLE LAWYERS

Negotiating terms

'We cannot agree to minimum accuracy thresholds'	'We cannot make guarantees around infringement'	'Data deletion upon termination is technically impossible'
		
Restrict use for critical or sensitive deliverables. Consider a joint monitoring protocol to establish baselines of human review or oversight	Query the Service Provider's maturity. Push to at least be provided with the benefit of any protections provided by foundation model provider	If the Service Provider cannot delete or de-identify Customer Data, that is a significant infrastructure concern, not a negotiation position

HWLE LAWYERS

Contact details

Expetise

- Intellectual Property
- Technology / AI
- Privacy, Data Protection and Cyber Security
- Security of Critical Infrastructure
- Consumer Law
- Trade Marks
- Media and Communications

Daniel Kiley

Partner | Adelaide

+61 8 8205 0567

+0458 295 387

dkiley@hwle.com.au

HWLE LAWYERS

Questions?

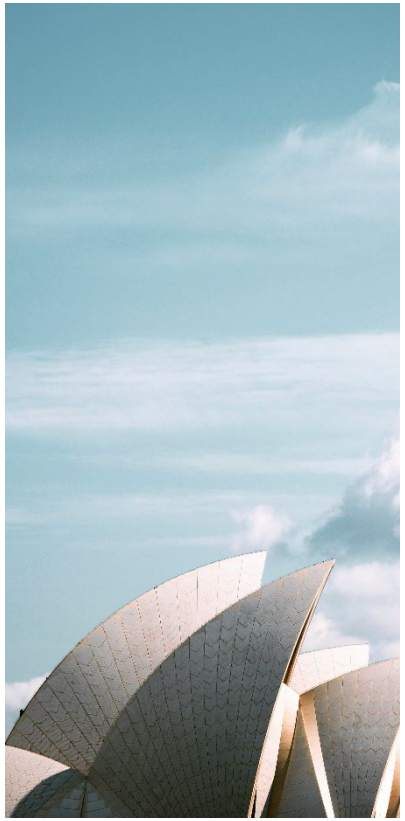
HWLE
LAWYERS

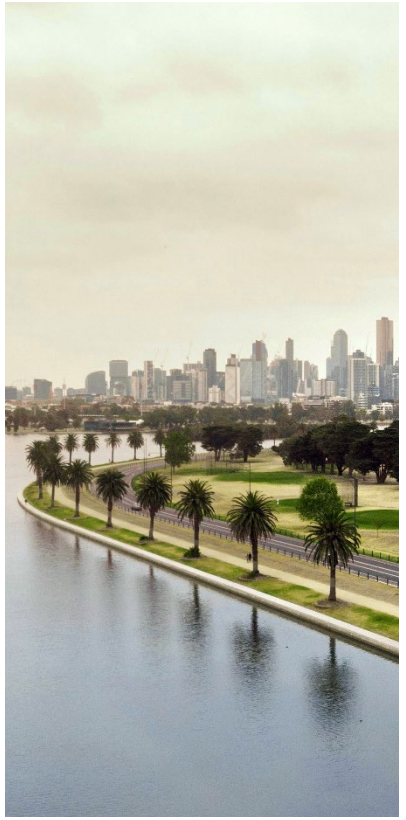
This seminar and accompanying documentation is not intended to be legal advice and should not be relied upon as such.

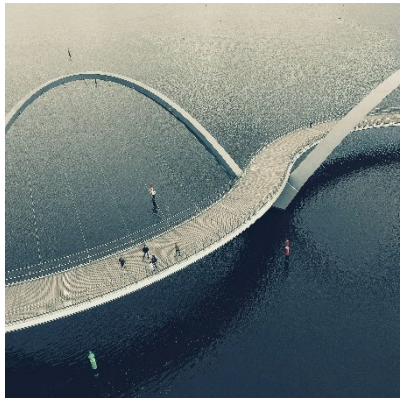
HWLE
LAWYERS

HWLE
LAWYERS

Legal solutions that make commercial sense







Different for all the right reasons

Our locations

ADELAIDE
Level 14
83 Pirie Street
Adelaide SA 5000
P +61 8 8205 0800
F 1300 464 135

BRISBANE
Level 24
360 Queen Street
Brisbane QLD 4000
P +61 7 3169 4700
F 1300 368 717

CANBERRA
Level 5
HWL Ebsworth Building
6 National Circuit
Barton ACT 2600
P +61 2 6151 2100
F 1300 769 828

DARWIN
Level 9
Mitchell Centre
59 Mitchell Street
Darwin NT 0800
P +61 8 8943 0400
F 1300 307 879

HOBART
Level 9
85 Macquarie Street
Hobart TAS 7000
P +61 3 6210 6200
F 1300 377 441

MELBOURNE
Level 8
447 Collins Street
Melbourne VIC 3000
P +61 3 8644 3500
F 1300 365 323

NORWEST
Level 3
21 Solent Circuit
Norwest Business Park
Norwest NSW 2153
P +61 2 9334 8555
F 1300 369 656

PERTH
Level 20
240 St Georges Terrace
Perth WA 6000
P +61 8 6559 6500
F 1300 704 211

SYDNEY
Level 9
5 Martin Place
Sydney NSW 2000
P +61 2 9334 8555
F 1300 369 656

HWLE
LAWYERS