TLOMA Presentation

PURVES REDMOND LIMITED

September 2025

purvesredmond.com

Agenda

Purves Redmond Limited will:

Outline the leading Artificial Intelligence (AI) claims which are impacting law firms such as deepfakes, wire transfer fraud and DDoS attacks

Provide advisory surrounding traditional law firm insurance policies, such as cyber, E&O and office package and if they cover AI risk/exposure

Discuss examples of some current AI insurance policies, specifically crafted for law firms and the application process

AI and E&O Claims

Expertise. At Your Service.

Utah Claim—June 2025

- Utah Court of Appeal sanctioned lawyer for using ChatGPT for a filing where he made citations of a non-existent court case
- One case did not appear in any legal database
- Fictional case “Royer v. Nelson”

Law Acknowledged:

1. Filing was written by an unlicensed law clerk
2. Cases were researched by using ChatGPT
3. Cases were not proofed by lawyer

Punishment:

- Lawyer paid respondent’s lawyer fees for petition
- Lawyer refunded fees to client for time to prepare filing and attending the hearing
- Lawyer donated US $1,000 to Utah charity called “And Justice for All”
- Lawyer apologized to court

New York Claim—June 2023

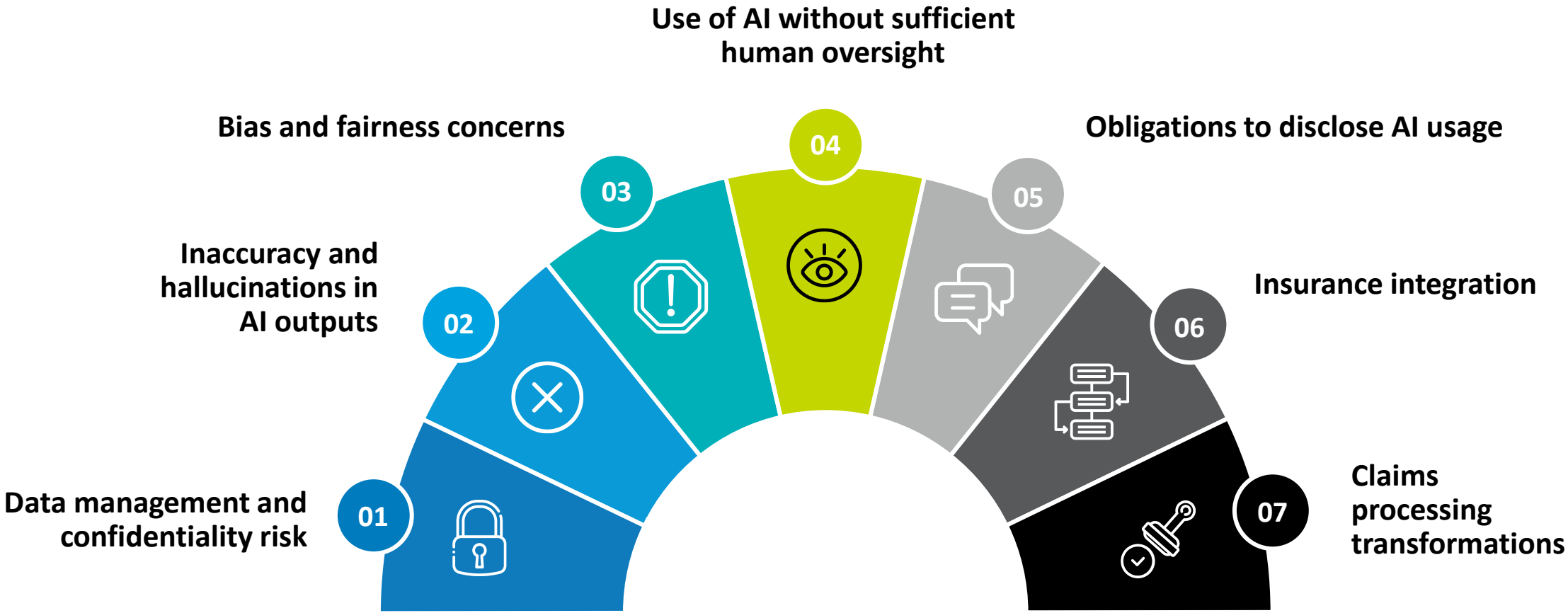
- Federal court in New York caught and sanctions two lawyers who submitted a legal brief written by AI tool ChatGPT
- It contained two errors:
  1. Citations of non-existent court opinions
  2. Fake quotes
- Judge was angry that the lawyers "abandoned their responsibilities" and that they did not come clean about using ChatGPT after the judge called them out

Punishment:

- Lawyers were sanctioned by the court
- Lawyers and firm (3 parties) each paid US $5,000 in fines
- Lawyers had to notify each judge falsely identified as an authority of the bogus case ruling about the sanctions
- Did not compel an apology because it would not be sincere

Canadian Cases?

How AI Can Impact Canadian Law Firms



AI and Cyber Claims

Expertise. At Your Service.

AI and Social Engineering

1. A hacker spoofed the audio and visual likeness of the CEO of our client using generative AI
2. The AI likeness of the CEO called an accounts payable employee in the finance department of our insured on Teams
3. The AI likeness requested accounts payable to send funds to an outside bank as he was making a considerable charitable donation to a new not-for-profit on behalf of the company, as it was a cause close to him
4. The employee knew the transfer amount requested exceeded their authority and required C-suite sign off
5. Given the CEO himself authorized the transfer, the employee sent the funds to the charity

Amount stolen: **$250,000**

AI and Email Fraud

1. An associate at a law firm was deceived into transferring $2M dollars to a hacker
2. The associate thought that they were sending funds to pay a client's mortgage but alas they were conned by a hacker
3. The issue was that the email appeared to be from their client and it requested the change in payment instructions due to an audit
4. Specific use of AI was not confirmed but sophisticated social engineering attacked often use AI to craft convincing phishing emails by mimicking writing styles and analyzing communication patterns
5. In this case the law firm did not specifically buy social engineering fraud coverage in either their cyber or crime insurance
6. Litigation ensured against their crime insurer and the court ruled in favour of their insurer highlighting the importance of understanding your policy exclusions and the need for specific coverage for social engineering fraud

Amount stolen: **$2M + costs to pursue litigation**

AI and Extortion

1. A law firm experienced unauthorized access to its network following a brute force attack
    - **Brute force attack** is a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys. It is a simple yet reliable tactic for gaining unauthorized access to individual accounts and organizations' systems and networks
2. The hacker exfiltrated data and attempted to extort the firm by threatening to release sensitive data
3. The law firm engaged their cyber insurers who negotiated with the hackers
4. A payment was made to avoid release of confidential data and insurer continued to monitor on the dark web
5. Moving forward the firm implemented password management system for all staff

Hackers often use AI drive tools to automates brute-force attacks, identity weak password and analyze network vulnerabilities increasing the success rates of such breaches

AI and Group Ransomware Attacks

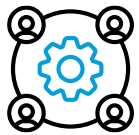
- In the last year 4 different law firms in one province suffered ransomware attacks
  - For one firm, the demand exceeded $200,000 in Bitcoin equivalent
- Hackers are increasingly leveraging AI to craft personalized phishing emails, and they are also automating attacks, making these cons more convincing and widespread
- Modern ransomware attacks often employ AI to identify vulnerabilities automate the spread of malware and evade detection
- AI is making ransomware more effective and harder to counter
- Unfortunately, 1 of the 4 firms did not have cyber insurance because they had unresolved network vulnerabilities
  - The others were protected by their cyber insurance and their costs were lower including a deductible payment, unpaid/ non-billable hours until the computers were unlocked

AI and Distributed Denial of Service (DDoS) Attacks

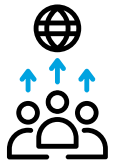
This is how DDoS attacks works:

1. Attackers infect numerous devices (e.g., computers, IoT devices) with malware, creating a botnet
2. Attackers remotely control the botnet to send massive amounts of traffic to the target which is a server or network
3. The flood of traffic overwhelms the target's capacity to handle legitimate requests, causing it to slow down or become unavailable

AI enables attackers to create more adaptive and intelligent DDoS attacks



Adaptive Attack Patterns: AI allows attackers to analyze network behavior and adjust attack patterns in real-time, making it harder for traditional defense systems to detect and block malicious traffic



Mimicking Legitimate Traffic: AI can be used to generate traffic that closely resembles legitimate user activity, making it more difficult to distinguish between normal and malicious traffic

Precision Attacks: AI can help attackers identify and target specific vulnerabilities, leading to more effective and targeted DDoS attacks

AI in Traditional Insurance Policies

Expertise. At Your Service.

Professional Liability Insurance and AI

Lawyers Professional Indemnity Corporation Primary Insurance

- No mention of AI in the policy
- No exclusion for AI
- But no affirmative coverage either (wording confirming coverage for artificial intelligence)
- Policy excludes cybercrime “to any CLAIM in any way relating to or arising out of a CYBERCRIME(S)”
  - Coverage added back via Endorsement 14. Limited Cybercrime Coverage

PRL Excess Professional Liability Insurance

- No mention of AI in the policy
- No exclusion for AI
- But no affirmative coverage either (wording confirming coverage for artificial intelligence)
- Policy excludes cyber coverage (to encourage a separate policy)

Cyber Insurance and AI

Item	Coalition	CFC	BOXX	Travelers
Affirmative Coverage	Yes	No	No	No
Exclusion	No exclusion	No exclusion	No exclusion	No exclusion
Definition of a Security Event	The failure of security of **computer systems** caused by any artificial intelligence technology, including through the use of machine learning or prompt injection exploits			
Definition of Funds Transfer Fraud	Includes a fraudulent instruction transmitted through the use of deepfakes or any other artificial intelligence technology			

Other Insurance and AI

Policy Type	CGL	Umbrella	Crime/D&O/EPL	Property
Insurer	Chubb	Chubb	Chubb	Chubb
Affirmative AI Coverage	No	No	No	No
Exclusions	No exclusion	No exclusion	No exclusion	No exclusion
General Cyber Exclusion	No exclusion	No exclusion	No exclusion: forefront policy can provide Cyber	No exclusion

How Insurance Companies and Brokers Utilize AI

AI Tools:

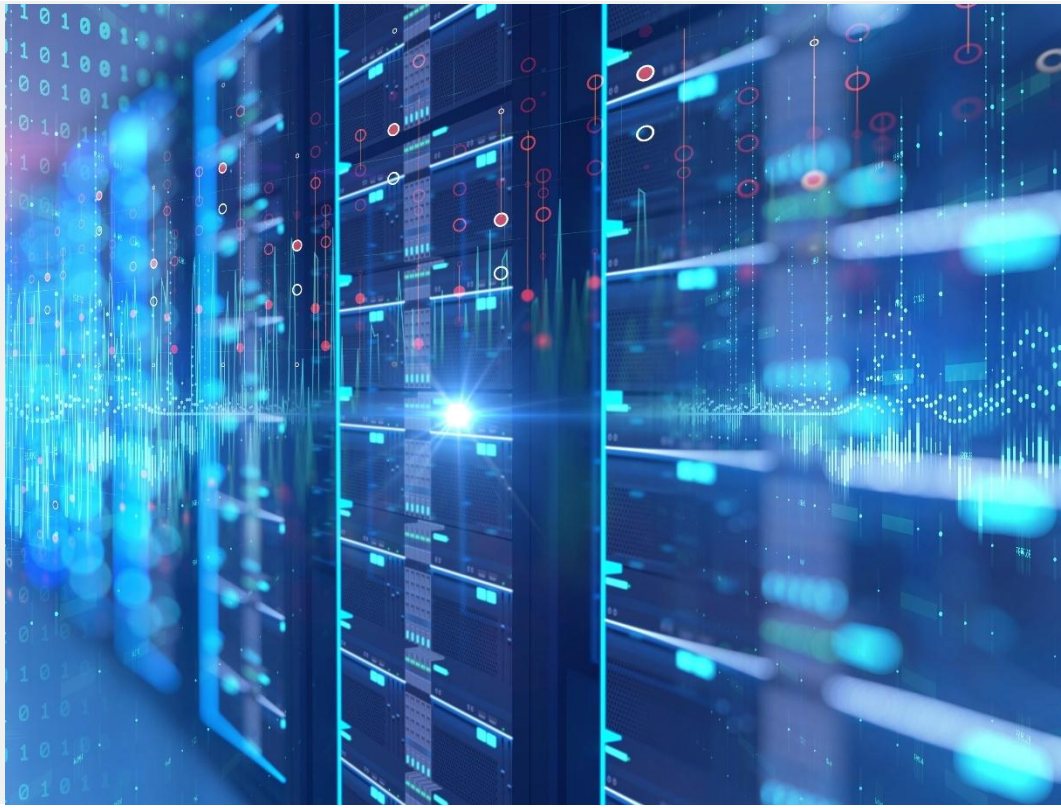
- Application review for completeness
- Generate quotes
- Automate document processing (issuing policies)
- Cut down on response times
- Analyze vast amounts of data to assessment risk and coverage eligibility
- Determine pricing
- Initiate claims handling
- Assess severity of claims, flag anomalies or assign claims professionals
- Identify patterns in litigation trends and industry benchmarks
- Seek out prospective clients who match their appetites

AI Insurance

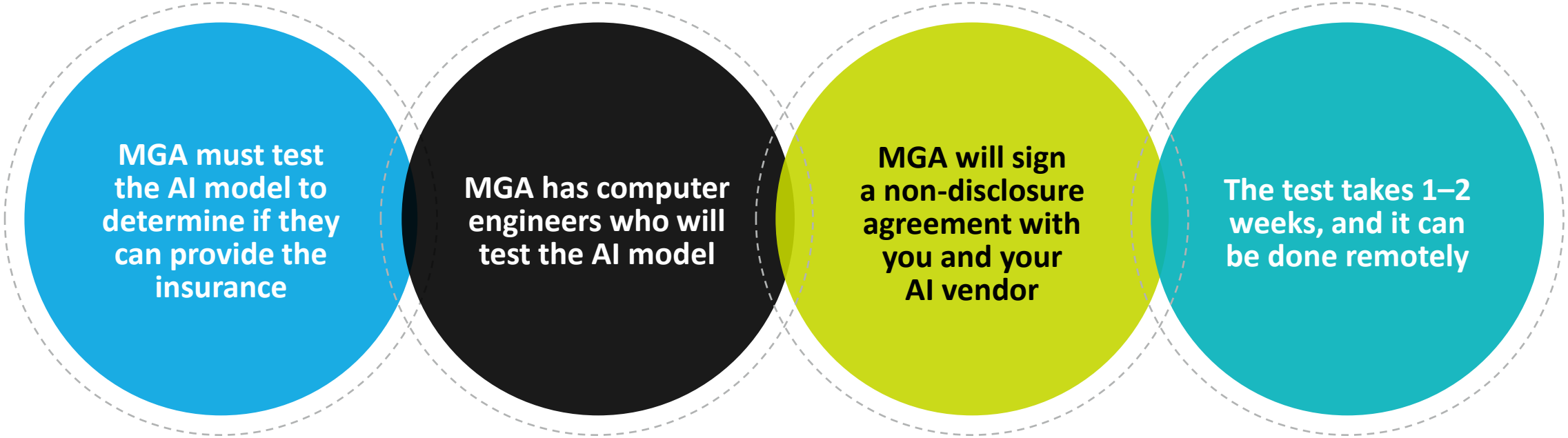
Expertise. At Your Service.

The Insurance

- Lloyd's MGA (lead is Chaucer)
- Intended for users of AI models
- The AI models do not need to be developed by the law firm, and will also include models developed by third party vendors
- Affirmative coverage for claims related to AI errors and omissions
- A few covered examples include: an AI model which causes hallucinations beyond 1% (or agreed %), leaks of private information and copyright infringement
- Limits up to $5M



Qualifications for Coverage



Other Notes

The premium depends on the limit/deductible selected and the results of the test (it can range between $10,000 to $500,000 premium)

MGA provides a certification to the vendor of the AI once they pass their tests, which is a vote of confidence

It should also give your firm confidence that the AI has been vetted by experts beyond the insurance benefits

PURVES REDMOND LIMITED

Truly Independent // 100% Employee Owned // Proudly Canadian