Open vs closed AI: Risk considerations

Risk Management Topics:

Cyber Security | Practice Management

Jennifer McMillan
Manager, Practice Support Services

From drafting emails to conducting legal research to reviewing contracts, the use of generative AI is increasing in legal practice. However, misuse of AI tools has led to several cautionary examples. In *Director of Public Prosecutions v GR* [2025] VSC 490, the defence team used an AI tool, likely a public-facing tool such as ChatGPT, to prepare submissions which contained fabricated cases and quotes. Similarly, in *Handa & Mallick* [2024] FedCFamC2F 957, a solicitor submitted a document listing cases in support of their argument, which were found to be fictitious. The Court ordered the solicitor to file submissions as to why a referral should not be made to the Victorian Legal Services Board and Commissioner, considered by the Court in *Dayal* [2024] FedCFamC2F 1166. Ultimately, the matter was referred, and the Victorian Legal Services Board imposed restrictions on the solicitor's practising certificate (see the Statement on the 'Mr Dayal' matter).

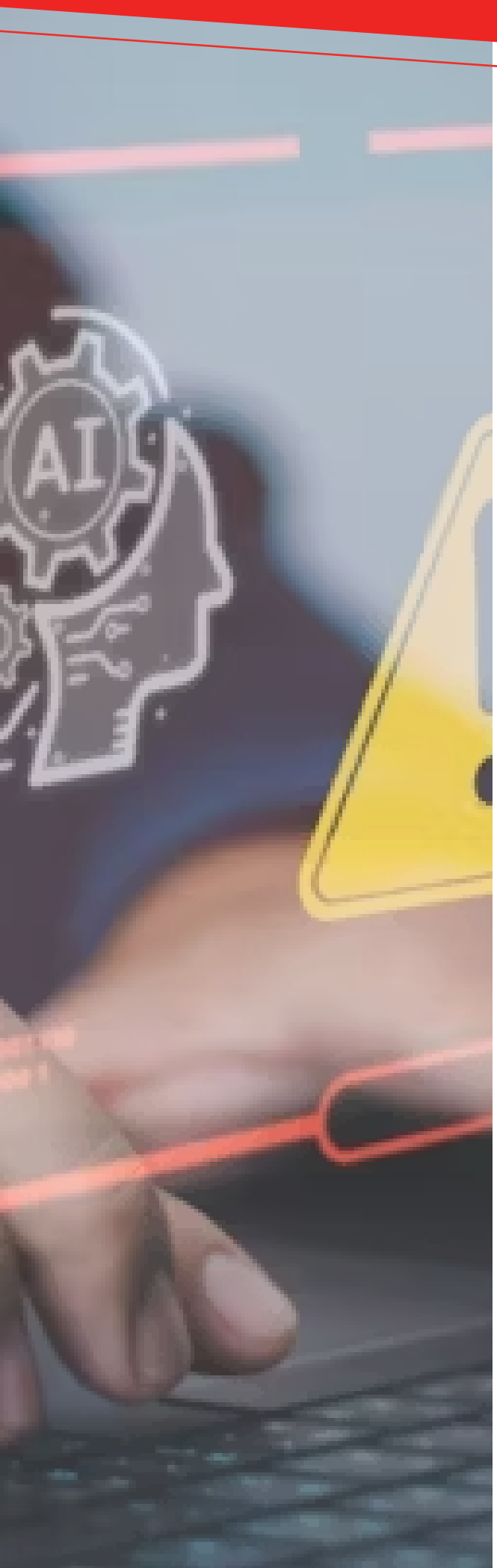
Both incidents involved open AI tools, which are accessible platforms not tailored for legal practice. But what about closed AI tools, such as those integrated into practice management systems or developed specifically for legal work? While these tools may offer greater security, they are not immune to risk.

Open (public) vs closed systems

Open AI systems allow public access and collaboration; closed AI systems are controlled by a single entity, offering more security but less flexibility. While the risks associated with generative AI tools are consistent across open and closed systems, the degree and manageability of risks vary. For instance, data security and privacy risks are higher in open systems, where control over data input and use may be limited.

A closed generative AI system, particularly one that is trained specifically for your law practice and accessible only internally, may pose less risk than a public-facing, open AI tool where data may be accessed or used indiscriminately. While the risk of data inaccuracy or bias are present in both open and closed AI, it may be more easily managed in closed environments.

Nevertheless, caution should be exercised in the use of all AI tools, and generated information should be thoroughly checked before any reliance is placed on it.



Open vs closed AI: Risk considerations

Where does the data go and how is it used?

Both open and closed AI tools present risks in terms of data input, particularly in relation to compliance with privacy and confidentiality obligations. It is essential to understand where data will go when you enter it into an AI tool, and how it will be used in future.

Start by asking some key questions aimed at understanding data security and confidentiality, such as:

- **Who are the users of the tool and who is inputting information?**
- **What data is used to train and refine the AI system?**
- **Who has access to information that has been entered into the system? How does the developer use these inputs? Will the information be accessible to third parties?**
- **What security and confidentiality protections are in place?**
- **What are the security settings?**

Open vs closed AI: Risk considerations

Assessing suitability

Whether a particular generative AI system is suitable for your law practice will depend on a number of factors, including:

– How has the system been designed?

– How is the system being used?

– What data has been used to train the AI tool and what data can it access?

– How are information inputs used and are they disclosed to third parties?

– How has the model evolved over time?

– What security is in place and how will the AI system integrate with existing systems?

Regardless of the type of AI tool under consideration, a balanced and informed approach to implementation and use is key. AI protocols, risk management frameworks and assurance review processes can assist law practices in ensuring careful and appropriate use of AI tools.

Remember: There is no presumption of privacy when using AI platforms. Unlike legal practitioners, these platforms are not subject to the Legal Profession Uniform Law, privacy legislation, or the Australian Solicitors' Conduct Rules. Inputting client names, details, or other private information into generative AI tools, even for drafting assistance, may compromise the confidentiality of that data.

Additional resources:

Short Minutes – Checking AI Outputs

Lawcover*notes* – The AI Trap: Why Solicitors Must Verify Everything

Court protocols for the use of AI in Australian jurisdictions

A Solicitor's Guide to Responsible Use of Artificial Intelligence, The Law Society of NSW