WeirFoulds LLP

From Generative to Agentic AI: Legal and Privacy Risks for Organizations

October 2, 2025

By James G. Kosa, Vipal Jain and Matt Gaulton, Student-at-Law

Introduction: Why Agentic AI is Different

A new phase in artificial intelligence (AI) is emerging: agentic AI. Unlike generative AI tools like ChatGPT, which respond to prompts, agentic AI goes beyond by taking autonomous actions such as sending emails, booking meetings, and updating records across systems. For example, an AI agent in HR could screen resumes and schedule interviews automatically by interacting with email and calendar systems. This delivers efficiency at a new level, but also introduces risks. A generative model might give a wrong answer, while agentic AI could act on that wrong answer, potentially causing real harm (e.g. sending a mistaken email or making an unauthorized purchase). With less human oversight, mistakes can have greater consequences, making it critical for organizations to address legal and privacy risks before deploying agentic AI.

Key Legal and Privacy Risks for Organizations

These risks fall into several key areas that organizations should manage proactively.

1. *Risk of Hallucination and Errors*

AI agents can hallucinate – in other words, generate false or inaccurate information – and then act on those errors. An autonomous agent could misinterpret data or instructions and take inappropriate actions. For instance, it might send out a wrong invoice or make an improper decision based on a misunderstanding. These kinds of mistakes can create legal and regulatory exposure, as well as financial loss or reputational harm.

2. *Liability and Accountability*

If an AI agent causes an error, it raises the question of who is held responsible. In practice, unless agreed to otherwise in a contract, the deploying organization would likely be held responsible for its agent's actions as opposed to the vendor. For example, if the agent offers an unauthorized discount or violates a law, the organization would likely be responsible for those actions.

3. *Security and Misuse Risks*

Since AI agents can connect across systems, they create new security risks. Attackers can try to exploit the agent. For example, a malicious input might trick the AI agent into performing unauthorized actions, and if the agent has excessive privileges, a hacker could misuse it to gain entry into sensitive systems, effectively turning the AI agent into a new attack vector.

4. *Data Handling and Privacy*

AI agents are designed to retain memory of past interactions, which raises privacy challenges. They may store more personal information, sometimes longer than necessary. An agent may also pull from various data already inputted into the system, which could exceed the purposes for which the data was originally collected.

Another concern is third-party disclosure. When an agent interacts with external tools or APIs, it may amount to a disclosure of personal information, triggering contractual and privacy law obligations. The organization would generally be held responsible, even if the AI agent is the one interacting with the external tools or API.

5. *Transparency and Explainability*

AI agents often function as black boxes, making it difficult to trace how or why decisions are made. This lack of transparency creates risks, particularly where laws require organizations to disclose the factors and parameters underlying automated decisions made using personal information. Without sufficient explainability, it becomes harder to demonstrate accountability, challenge errors, and satisfy regulatory obligations.

Practical Guidance for Organizations

To safely harness agentic AI, organizations should consider these practical steps, which we have grouped into three categories.

1. *Due Diligence Before Adoption*

Vet AI agents thoroughly before deploying them. Find out from vendors how their AI agent works and handles data.

Before widely adopting the AI agent, start with a small-scale pilot test of the agent and monitor its behavior closely. Involve the relevant stakeholders to evaluate how the agent performs and to catch any issues early.

2. *Contractual Protections*

Ensure that your contract with the vendor addresses the unique risks associated with agentic AI. For example, the contract should define limits on agent autonomy, allocate liability for unauthorized or harmful actions, specify vendor security commitments and describe how the AI model is trained and maintained.

3. *Governance & Oversight*

Internally, establish clear policies on how agentic AI may be used, specifying where it is permitted and where human approval is required. Human oversight should always be maintained for tasks that pose a high risk – an AI agent should not have the final say on critical matters like financial transactions or hiring decisions. Finally, staff should be trained on the risks of over-delegating authority to AI systems.

Regulatory Considerations

The steps outlined above reflect best practices, but specific legal requirements may apply based on jurisdiction and are not addressed here. For instance, the European Union's Artificial Intelligence Act and Quebec's Law 25 set out specific obligations regarding the use of AI. These examples highlight how the regulatory landscape for AI is evolving quickly, and the list of obligations will continue to expand as legislators and regulators respond to the growing use of AI.

If you have any questions about how agentic AI may affect your organizations, or if you would like to discuss practical steps for

implementing these technologies, please reach out to the authors for further guidance.

The information and comments herein are for the general information of the reader and are not intended as advice or opinion to be relied upon in relation to any particular circumstances. For particular application of the law to specific situations, the reader should seek professional advice.

For more information or inquiries:

James G. Kosa

Toronto
416.947.5043

Email:
jkosa@weirfoulds.com

James Kosa is a partner at WeirFoulds with a practice focused on information technology and intellectual property law. He is the Co-Chair of the firm's Technology & Intellectual Property and Privacy & Access to Information Practice Groups, and Co-Chair of the Blockchain and Digital Assets Practice Group.

Vipal Jain

Toronto
416.619.6294

Email:
vjain@weirfoulds.com

Vipal's practice focuses on privacy and technology matters. She advises organizations across various sectors on matters relating to privacy law compliance, technology contracting, cybersecurity incidents and artificial intelligence.