



News & Types: Intellectual Property & Technology Update

The Emergence of Agentic AI: A New Frontier in Innovation and Legal Risk

9/29/2025

By: Michael S. Golenson

Practices: Intellectual Property & Technology

As artificial intelligence continues to evolve, a new class of AI systems—agentic AI—is emerging with the potential to reshape how businesses operate. Unlike traditional or even generative AI systems that respond passively to inputs, agentic AI is designed to take initiative, make decisions, and pursue goals with limited or no human intervention. These AI agents can plan and execute multi-step tasks, interact with software and APIs, and even delegate sub-tasks to other agents. Their autonomy opens up significant efficiency gains and new capabilities for enterprises—but also introduces novel operational, ethical, and legal challenges.

To understand the significance of agentic AI, it's helpful to contrast it with generative AI. Generative AI and agentic AI differ primarily in their level of autonomy and function. Generative AI, such as large language models and image generators, produces content—text, images, code, etc.—in direct response to user prompts, functioning as a reactive tool without initiative or memory across tasks. Agentic AI, by contrast, builds on generative AI capabilities but introduces autonomy, goal-orientation, and decision-making. It can plan, execute, and adapt over multiple steps, often using tools, APIs, or external systems to achieve objectives with minimal human input. For example, an agentic AI could be tasked with researching a market entry strategy, autonomously sourcing data, analyzing competitors, drafting reports, and refining its output without continuous user input. This shift from static generation to dynamic agency marks a profound technological leap.

However, the same autonomy that makes agentic AI powerful also introduces a range of significant legal risks for businesses. For example, starting with liability, when an AI agent makes a harmful decision, acts negligently, or breaches a contract, it remains unclear who—if anyone—can be held legally responsible. Data governance poses another critical challenge, as autonomous agents may access, process, or transfer sensitive data without proper oversight, which could potentially violate privacy regulations such as GDPR, CPRA, or HIPAA. Intellectual property concerns also arise, particularly when AI agents generate content that inadvertently infringes third-party intellectual property rights or misuses proprietary data. Beyond these core risks, agentic AI raises additional legal issues including the validity of contracts formed by autonomous systems, potential for biased or discriminatory outcomes, cybersecurity vulnerabilities, cross-border regulatory conflicts, and a lack of auditability that can hinder compliance with financial or operational reporting obligations. These challenges demand proactive legal frameworks and internal safeguards to ensure safe and compliant deployment of agentic AI in enterprise environments.

Given these challenges, organizations considering the deployment of agentic AI must move cautiously. Businesses should implement robust governance frameworks to monitor agentic behavior, restrict autonomous access to critical systems, and ensure traceability of decision-making. Contractual clarity with AI vendors, rigorous risk assessments, and proactive engagement with emerging AI regulations will be essential.

If you have any questions regarding the content of this article, please contact the author or any member of Masuda Funai's Intellectual Property and Technology Practice Group.

Masuda Funai is a full-service law firm with offices in Chicago, Detroit, Los Angeles, and Schaumburg.