MCLE Days 2025-2026

WILSON
SONSINI

Agentic AI and Other New Developments

Scott McKinney
smckinney@wsgr.com

What is "Agentic" AI?

Agentic AI

- ***An AI system or application that***
  - ***Performs tasks autonomously (or relatively autonomously)***
  - ***Makes informed (or semi-informed) decisions***
  - ***Can adapt to changing conditions or environments***

No One Universal Definition

- ***Huge variance in what "agentic AI" might mean***
- ***Lots of puffery in the industry***
- ***Many things described as agentic AI that aren't really that***

What is “Agentic” AI?

Common Types of AI agents

- ***Different than a chatbot***
  - ***But sometimes interrelated or with chatbot functionality***
- ***Work or process or workflow optimization agents***
  - ***Digital workers***
- ***Public facing / public interacting agent***

Examples:

- ***Travel agent***
- ***Calendar agent***
- ***Payments agent***
- ***Workflow optimizer***
- ***Customer support agent (beyond just a chatbot)***

Exemplary Categories of AI Agents

Category	Definition	Common Uses
Business-task agents	Can take actions in multiple enterprise software apps	Invoice processing, data entry, document classification, scheduling
Conversational agents	Text or voice chatbots that resolve customer support tickets or employees' IT or HR questions through a back-and-forth exchange	Customer service, IT service tickets, HR tasks
Research agents	Retrieve, analyze, and validate information from trusted sources, including academic literature or web content.	Academic-style research, sourcing citations, answer hard technical questions
Analytics agents	Analyze structured data to product graphics/charts or reports.	Data querying, creating dashboards, business insight summaries
Developer agents	Assist software engineers by handling complex coding tasks	Code completion, documentation, debugging, refactoring, site reliability engineering
Domain-specific agents	Specialized agents built with domain knowledge or high-stakes or regulated fields.	Contract analysis, medical triage, financial analysis.

Key Questions

- ***Key questions and considerations:***
  - Is the AI agent legally authorized to take actions (e.g., make payments, enter into contracts, etc.) on behalf of the user or company?
  - Who is responsible for the actions of the AI agent?
  - What if the AI agent acts outside the scope of its authority or direction?
  - How can we attribute a specific AI agent's actions to a specific person or company?
- ***New frontier of AI and the law – lots is unsettled. What legal frameworks apply?***
  - Common law principles of agency
  - Consumer protection laws and agencies
  - UCC
  - UETA
  - Card network rules (for payments)
  - Privacy regulations
  - AI regulations

Agency Theory

Agency Principle	Traditional Agency	Agency Principles Applied to Agentic AI?
Principal-Agent Relationship	A principal gives an agent authority to act on their behalf and subject to their control. For legal agency to exist, both parties must be "persons".	Generally thought that an AI is considered a "mere instrumentality" of the human or corporation that uses it, not a separate legal person. The person or organization that deploys the AI would be treated as the principal and is held responsible for the AI's actions.
Actual Authority	The authority the principal explicitly or implicitly gives to the agent.	The AI's programming and instructions function as its actual authority. If the AI acts within these defined parameters, the principal is (or should be) liable. For example, if a user tasks an AI agent to book a hotel room, the user is bound by the reservation.
Apparent Authority	Authority a third party reasonably believes the agent has based on the principal's actions or representations.	If a principal has given an AI agent the appearance of authority (e.g., via titles or branded tools), a third party may reasonably rely on that authority and hold the principal liable, even if the agent overstepped its actual instructions.
Fiduciary Duty	An agent's duty to act with loyalty and care solely for the principal's benefit.	Legal and ethical considerations suggest that AI agents should be designed and trained with "loyalty" to the principal as a core value. A system that benefits itself or the developer at the expense of the user could be a violation of this principle.
Liability for Misconduct	A principal can be held liable for an agent's contractual breaches or tortious acts within the scope of their authority (known as respondeat superior).	One of the most-debated areas. When an AI "goes rogue," courts could consider/ investigate if the responsible party was negligent in the AI's design, training, or supervision.
Liability for Unforeseeable Actions	A principal's liability is often tied to the foreseeability of the agent's actions.	The "black box" nature of some AI makes it difficult to prove the root cause of an unexpected or harmful action. This challenges the traditional legal requirement of proving causation.

Product Liability Consideration for Agentic AI

Is agentic AI a "product"?

- There is no clear test of what constitutes a "product". Social media providers have traditionally argued that they provide "platforms" or "services", as opposed to products. For technology providers, courts increasingly distinguish between recommendation algorithms or product features (which are more likely subject to product liability) vs. ideas and content (which may instead be protected by Section 230, First Amendment, or other protections).

Compare:

- Wilson v. Midway Games, Inc. (Dist. Conn. 2002): Plaintiff whose son was killed by friend after playing Mortal Kombat sued Midway Games for product liability, alleging that the game's interactive nature addicted her son and led to his death. Court holds Mortal Kombat not to be a product because the alleged harmful features are not distinct from the "ideas and expressions" in the game.
- Brookes v. Lyft Inc. (Fla. Cir. Ct. 2022): Plaintiff struck by driver sued Lyft for product liability, alleging that Lyft's app was defective and distracted the Lyft driver. Court holds Lyft's app to be a product because claims "ar[ose] from the defect in Lyft's application, not from the idea[s] or expressions in the Lyft application."

The EU's new AI Liability Directive and updated Product Liability Directive are explicitly extending product liability to software and AI systems, removing the tangibility requirement. US law may be leaning in a similar direction.

Contrast generative features of AI (such as image generation) with action-oriented features (such as purchases or hardware operation).

Categories of Product Liability

Manufacturing Defects

- Liability applies when a product does not function according to its intended design.
- AI LEAD Act would establish a product liability framework for AI systems. Where "manufacturing" appears in traditional product liability law, the Act would substitute the term "development or process used to produce".

Design Defects

- Product designers have a duty to design a "reasonably safe product". Courts may employ the risk-utility test, which analyzes whether a reasonable person would believe the foreseeable risks of a product outweigh the utility, considering cost, safety, and functionality.
- Lemmon v. Snap (9th Cir. 2021): Snapchat included a "Speed Filter" feature that measured and documented speed with a built-in reward system. After users died in a car crash while using the "Speed Filter" feature, parents sued Snap, alleging failure to design a reasonably safe product. Court held that (a) because the claims did not treat Snap as a publisher or speaker, the claims were not barred by Section 230 and (b) Snap was a "manufacturer" who had designed and made the product available.

Contributory Negligence

- Product provider may argue that a user's own actions contributed to their injury. Similar arguments as common indemnity carveouts.

Criminal Liability

Can agentic AI systems commit crimes?

Systems themselves lack personhood, *mens rea*, and the ability to face criminal punishment.

Criminal exposure may extend to developers or operators of agentic AI systems.

Developers may be exposed to liability for knowing deployment of a dangerous system.

- NY RAISE Act imposes penalties for “critical harm” resulting from AI systems. “Critical harm” includes “a model engaging in criminal conduct without meaningful human interaction”.

Operators may be exposed to liability for the criminal acts of an agentic AI system.

- E.g., agentic AI system commits fraud or trades on MNPI.
- Does the operator have the requisite *mens rea*? How “autonomous” is the system?

Agentic Actions – Who is Responsible?

Autonomous nature of agentic AI makes assigning liability or responsibility complex and uncertain

Difficulty assigning blame when an agent causes harm

- Developer?
- Deployer / customer?
- Other end user directing the agent?
- Traditional legal concepts like vicarious liability might fail because there is no human "agent" to hold primarily responsible for the act

Applying existing laws:

- Tort law, product liability, agency, negligence, etc.
- Difficult to apply given the AI's unpredictable actions, which may not be foreseeable by its human operators

CLE Code:

711XNF

Key Considerations for the Agentic AI World

Technical Infrastructure

- ***How do agents interact with a platform?***
- ***Does the platform or application allow agents (from a technical and/or legal perspective)?***

Platform Mitigations and Safeguards

- ***Rate / load limiting***
- ***Authentication mechanisms, agent registrations, etc.***
- ***Regular Audits and monitoring***
- ***Agent attribution infrastructure or tracking functionalities***
- ***Clear agentic rights***
  - ***E.g., what is / isn't allowed?***

Will a Universal Agentic Interoperability Standard Emerge?

Key Considerations for the Agentic AI World (2)

Deployment of Agents

- ***Clear AI notices / disclosures***
- ***Clear grant of authority***
- ***Human Oversight, auditing, monitoring***
- ***Extra safeguards for high(er) risk agentic actions?***
  - ***Gates requiring further user consent to finalize a payment or purchase***

Agentic Scraping

- ***Agents may need to "scrape" or otherwise access platforms or applications, without permission, in order to function***
  - ***What is platform? Is it a competitor?***
  - ***Will the agent scrape or access data or the platform behind a gate? Will a user account be created?***
  - ***What is the type of content being access or scraped? How will it be used? Will it be stored permanently?***
  - ***Privacy issues***

Key Considerations for the Agentic AI World (3)

Contractual issues

- ***Privity?***
- ***Clear Terms of Service***
  - ***Need <u>affirmative assent</u> to grant agency or assume or disclaim responsibility***
  - ***Will likely need extra-strong indication that agency was meant to be granted***
  - ***Disclaimers and prohibitions***

UETA

- ***The Uniform Electronic Transactions Act addresses automated transactions:***
  - ***an electronic agent's ability to form contracts on behalf of a person***
  - ***the effect of an error made by an individual in dealing with the electronic agent of another person***

Agentic AI Product Guardrails

- ***Accuracy of Decisions***
- ***Tracking of Decisions and Interactions***
- ***Bias mitigation***
- ***Human (end user or operator) Decision Gates for High-Risk Actions***
- ***Human Review***

Agentic AI – Other Best Practices

- ***Provide clear, concise, and easily accessible disclosures about how the AI agent operates, what authorizations are involved, and what risks users assume***
- ***For payments or purchases, use plain language designed to ensure users understand payment timing, fees, error resolution rights, and how to revoke or modify the AI agent's permissions***
- ***Avoid misleading or ambiguous statements about the capabilities or limitations of the AI agent to mitigate the risk of unrealistic user expectations***
- ***Ensure users receive advance notice of any material changes to AI agent functionality, terms of use, or payment initiation processes***
- ***Implement robust consent mechanisms that require affirmative user action with respect to authorizing the AI agent to initiate payments on the user's behalf, with easy-to-use controls for managing or revoking authorization***
- ***Monitor ongoing use for signs of misuse or unintended consequences and provide users clear avenues for reporting issues***

These materials have been prepared by Wilson Sonsini Goodrich & Rosati for informational purposes only and are not legal advice. Transmission of the information is not intended to create, and receipt does not constitute an attorney-client relationship. Audience should not act upon this information without seeking professional counsel. The information contained herein is provided only as general information which may or may not reflect the most current legal developments. This information is not provided in the course of an attorney-client relationship and not intended to constitute legal advice or to substitute for obtaining legal advice from an attorney licensed in your region. The views expressed here are those of the speaker and do not reflect those of his/her firm or clients.

Thank you

Scott McKinney
smckinney@wsgr.com