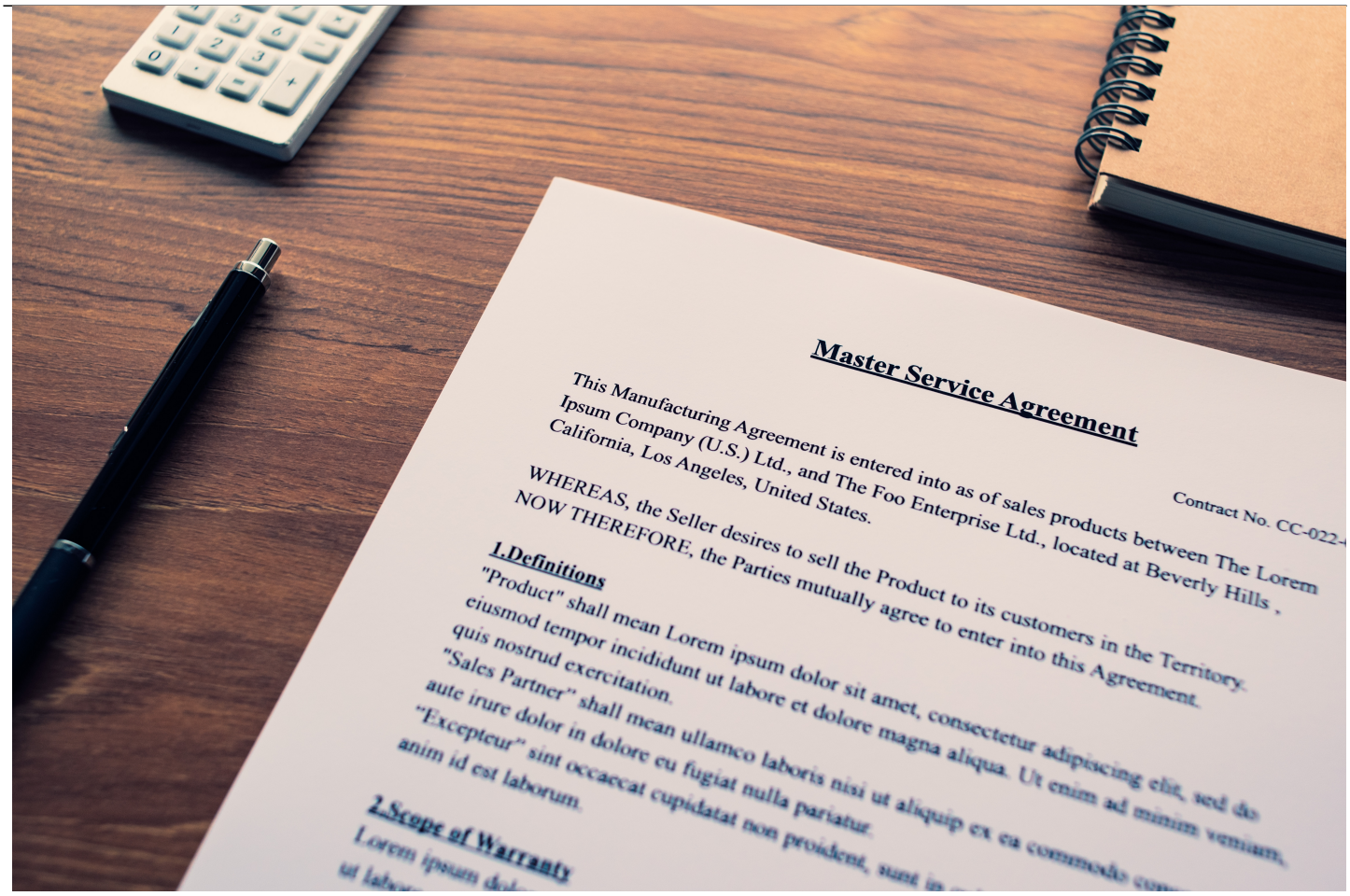
ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Legal Tech: How to Evaluate AI Vendor Risks

Commercial and Contracts

Technology, Privacy, and eCommerce



Banner artwork by Mameraman / *Shutterstock.com*

AI is exciting — and risky. No one has all the answers yet. But, we still need to ask questions.

Courts, legislators, and regulators will define AI's boundaries for years to come. Meanwhile, you want to help your company avoid leading a costly lawsuit that becomes the litmus test in a landmark AI decision.

That means proactively asking targeted questions about the AI-driven products and services your company buys from third-party vendors. Until we have complete regulatory guidance, consider asking AI product and service vendors the critical questions below to help you navigate potential risks.

Carefully vet AI providers to mitigate potential future risks. Artwork by Pasuwan / *Shutterstock.com*

Get to know the ethics of AI-driven systems.

Start by reviewing the vendor's AI policies and procedures. Learn how they prioritize ethical considerations when developing and deploying AI-driven systems.

Questions to ask AI vendors:

- What’s your philosophy on ethics and AI? Do you have a public AI statement or policy you can forward to me?
- Can you confirm that your AI models were trained with properly licensed content?
- Can your AI tools be used to cause harm? What steps have you taken to prevent that from happening?
- In what ways could your AI system produce inaccurate or misleading results? How do you address those issues?
- Does your company face any pending AI-related litigation, threats of litigation, or regulatory inquiries?

  If vendors use data in ways that violate privacy laws or regulations, your company can suffer significant legal and reputational damage.

Prepare to collaborate with others.

To meet any future AI regulations, as well as any guidelines set by clients, internal stakeholders, or others, you'll need to understand the ins and outs of your vendors' AI processes.

Questions to ask vendors:

- What dataset did you use to train your AI model? Who trained it?
- Why did you choose the training methods you used?
- What quality control procedures do you use?
- Will you periodically retrain or continuously update your model? If so, on what data?
- Is the system auditable? Can we customize the audit process?
- Do generative AI models include links to citations to verify the case law and information it references and to support its assertions, i.e., to demonstrate that it isn't hallucinating?

Identify potential sources of privacy and security violations.

AI tools may collect and process large amounts of personal data that must be secured appropriately. If vendors use data in ways that violate privacy laws or regulations, your company can suffer significant legal and reputational damage. Hackers can exploit vulnerabilities to access sensitive data and disrupt operations.

Questions to ask vendors:

- How do you test for bias and accuracy in your AI model?
- What is your track record concerning bias and accuracy?
- Do you keep humans in the loop to review your AI model's results?

An interconnected world means additional parties.

Partnering with an AI vendor carries the same inherent risks as partnering with any vendor. The level of risk depends on how much access a vendor has to your data and systems. That risk is amplified when a vendor partners with additional product or service providers.

Questions to ask vendors:

- What AI use is on your product roadmap?
- What is the timeline for rollout?

And don't forget the time-honored catch-all question:

> **What else should we have asked you about your AI?**

Questions are currently your best tool for vetting vendors of AI tools. Actively seeking answers during vendor selection helps avoid AI bias, privacy violations, security breaches, and other potential legal liabilities. Carefully vet AI providers now to deploy AI safely and help ensure organizational processes remain reliable, ethical, and compliant with legal and regulatory requirements when they arrive.

Disclaimer: The information in any resource in this website should not be construed as legal advice or as a legal opinion on specific facts, and should not be considered representing the views of its authors, its sponsors, and/or ACC. These resources are not intended as a definitive statement on the subject addressed. Rather, they are intended to serve as a tool providing practical guidance and references for the busy in-house practitioner and other readers.

Olga V. Mack

Fellow

CodeX

Olga V. Mack is a fellow at CodeX, The Stanford Center for Legal Informatics, and a Generative AI Editor at law.MIT. Mack shares her views in her columns on ACC Docket, Newsweek, Bloomberg, VentureBeat, Above the Law, and many other publications.

Mack is also an award-winning (such as the prestigious ACC 2018 Top 10 30-Somethings and ABA 2022 Women of Legal Tech) general counsel, operations professional, startup advisor, public speaker, adjunct professor, and entrepreneur. She co-founded SunLaw, an organization dedicated to preparing women in-house attorneys to become general counsels and legal leaders, and WISE to help female law firm partners become rainmakers.

She has authored numerous books, including Get on Board: Earning Your Ticket to a Corporate Board Seat, Fundamentals of Smart Contract Security and Blockchain Value: Transforming Business Models, Society, and Communities. She is working on her next books: Visual IQ for Lawyers (ABA 2024), The Rise of Product Lawyers: An Analytical Framework to Systematically Advise Your Clients Throughout the Product Lifecycle (Globe Law and Business 2024), and Legal Operations in the Age of AI and Data (Globe Law and Business 2024).