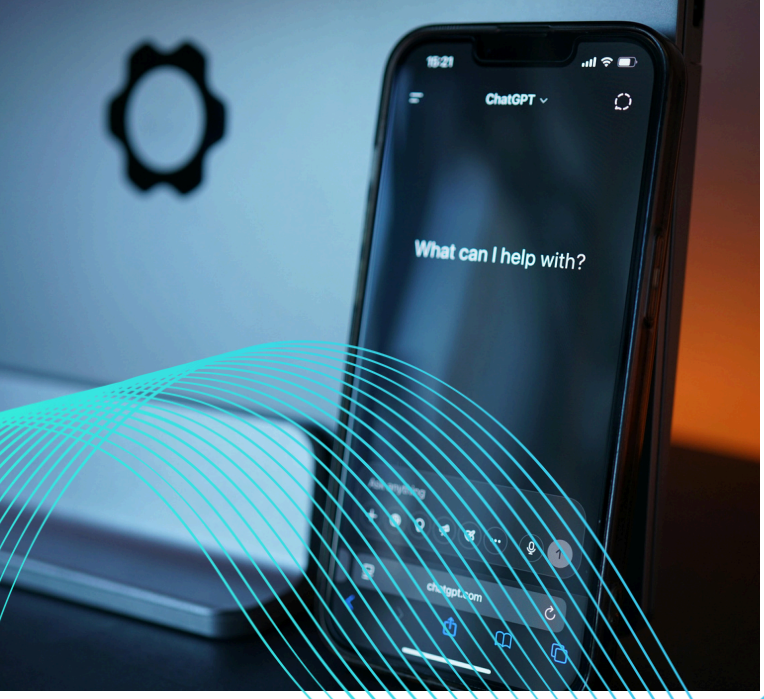


The Fine Print of AI: Managing AI Vendor Contracts in an Evolving Landscape

By Alexandra (Ali) Nienaber
and Adava Jefferson

In 2024, a staggering 78% of U.S. organizations reported using artificial intelligence ("AI"), marking a 23% increase in one year.[1] This surge in AI adoption for businesses is not surprising when considering the headlines dominating business and tech media: "5 Key Benefits of Integrating AI into Your Business,"[2] "How Does AI Improve Efficiency?,"[3] and "How Generative AI Can Boost Highly Skilled Workers' Productivity."[4] One recent study even claims that highly skilled professionals using AI can outperform their peers by nearly 40%,[5] underscoring the technology's potential to redefine productivity and performance across industries. The narrative is clear: AI is not only a tool, but a transformative force.

As organizations race to adopt AI, many concentrate solely on how much it costs and the potential productivity gains. However, this approach neglects key strategic factors, most notably, the binding agreements with third-party AI vendors ("AI Vendors") required to access these AI tools ("AI Vendor Contracts"). AI Vendor Contracts define the terms of the relationship between the AI Vendor and the organization, often including provisions related to liability; compliance with applicable regulations and law; and intellectual property rights, such as data access and retention. Each of these terms can introduce serious challenges for an organization if not properly negotiated or understood, making it essential to examine each of these terms for potential risk.

Limitation of Liability

A key provision in AI Vendor Contracts is the limitation of liability — often discussed in indemnification clauses where one party in an agreement agrees to protect the other from liability, damages, or financial loss. Often, non-AI software service agreements ("SaaS") contain indemnification clauses covering third-party intellectual property infringement claims, data security and privacy incidents, and property or bodily injury damage, when applicable. However, these standard clauses fail to address the more complex and varied risks associated with AI tools. Among these risks are algorithmic errors and inaccurate outputs, which have become more well known with generative AI as hallucinations.[6] Standard indemnification clauses also fail to address potential bias in AI tools that may lead to errors and discrimination claims. AI tools can exhibit bias due to factors like training data, algorithm design, and proxy data, which organizations typically cannot control.[7]

In addition to ignoring many AI-tool specific risks, AI Vendors tend to limit their own liability while transferring it to its customers: the organizations. Data indicates that 88% of AI Vendors impose liability caps, a rate higher than that of SaaS by 7%.[8] Yet only 38% of organizations (their customers) cap their liability in AI Vendor Contracts, compared to 44% in the broader SaaS market.[9]

Lack of Compliance with Applicable Laws

Another essential provision for AI Vendor Contracts is one that ensures AI Vendors and AI tools comply with all applicable laws and regulations. Data reveals that only 17% of AI vendor contracts committed to full regulatory compliance.[10] The lack of contractual commitment by AI Vendors to comply with applicable laws and regulations is concerning considering that in 2024 alone, U.S. federal agencies introduced 59 AI-related regulations, more than doubling the number of regulations issued in 2023.[11] This number also ignores the increasing laws being passed in cities and states, such as Illinois's Wellness and Oversight for Psychological Resource Act,[12] New York City's Automated Employment Decision Tools Law,[13] and California's Health Advice from Artificial Intelligence Law.[14] Many of these AI laws impose fines or other penalties for violations.

The need for a provision addressing legal compliance is also becoming more urgent as courts turn their attention to how AI tools are deployed by AI Vendors and organizations. A leading example of this new attention is *Mobley v. Workday*.[15] In *Mobley*, Derek Mobley filed a class action against Workday, Inc., alleging that Workday's AI tool (a resume screening tool) discriminated against him and others similarly situated.[16] While Workday attempted to have the class action against it dismissed by asserting it was not the employer making the employment decision, the federal court in the Northern District of California denied it, holding that Workday could be held liable as an agent of its customers.[17] Though *Mobley* is only a single case, its determination of "agency" raises concerns of potential liability it creates for customers of AI vendors. The *Mobley* case also highlights how traditional legal frameworks, like age-discrimination claims, are being adapted to address the use of AI tools. These developments are particularly concerning given AI Vendor Contracts often limit AI Vendor liability compared to organizations.

AI Vendor Use of IP

The final provision of concern for AI

Vendor Contracts is organization's IP rights, specifically the use of an organization's data and retention of it. Data shows that 92% of AI Vendor Contracts provide AI Vendors with data usage rights that exceed the usage necessary for them to provide their services.[18] Many AI Vendor Contracts also allow the AI Vendors to use the organization's data and train its models with it. This is concerning as some AI tools may have access to sensitive information, such as financial transactions, emails, client lists, HIPAA-protected information, or strategic plans. Training on this material could accidentally be leaked if the AI tool regurgitates the sensitive information in response to a third-party prompt.[19] Leaking of this information, while unintentional by the organization, could lead to limited protections of this sensitive data under trade secret laws.

Takeaways for AI Vendor Contracts

Before entering an AI Vendor Contract, an organization and its legal team should include the following provisions:

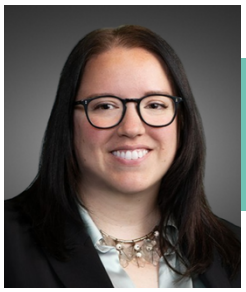
- Mutual liability caps;
- Require AI Vendor to state it will comply with all applicable laws and regulations related to its AI tool;
- Prohibit AI Vendor's data usage rights that exceed the usage necessary for the AI Vendor to provide its services;
- Limit the AI Vendor's retention of sensitive information through deletion mandates; and
- Exclude the AI Vendor from using the organization's data to train the AI tool if being provided to third parties.

As organizations continue to race to adopt AI, organizations (and their legal teams) must remain hyper-vigilant with understanding, reviewing, and negotiating AI Vendor Contracts. Particular attention should be paid to these provisions that may limit the AI Vendor's liability, sidestep legal and regulatory responsibilities, or make broad claims over the organization's IP.

These provisions, if neglected, may lead to serious strategic disadvantages to the organization and potential legal

consequences. That is why it is important to slow down to read and understand the fine print on AI Vendor Contracts and challenge potentially harmful provisions.

[1] *Artificial Intelligence Index Report 2025*, Stanford University Human-Centered Artificial Intelligence 17, https://hai.stanford.edu/assets/files/hai_ai_index_report_2025.pdf (accessed October 16, 2025).
[2] Kate Gibson, *5 Key Benefits of Integrating AI into Your Business*, Havard Business School Online (Aug. 1, 2024), https://online.hbs.edu/blog/post/benefits-of-ai-in-business.
[3] Teaganne Finn & Amanda Downie, *How Does AI Improve Efficiency?*, IBM Think, https://www.ibm.com/think/insights/how-does-ai-improve-efficiency (accessed October 17, 2025).
[4] Meredith Somers, *How Generative AI Can Boost Highly Skilled Workers' Productivity*, MIT Sloan School of Management (Oct. 19, 2023), https://mitsloan.mit.edu/ideas-made-to-matter/how-generative-ai-can-boost-highly-skilled-workers-productivity.
[5] *Id.*
[6] *What Are AI Hallucinations?*, IBM Think, https://www.ibm.com/think/topics/ai-hallucinations (accessed Oct. 19, 2025).
[7] *See* Alexandra Jonker & Julie Rogers, *What Is Algorithmic Bias?*, IBM Think, https://www.ibm.com/think/topics/algorithmic-bias (accessed Oct. 19, 2025).
[8] Olga Mack, *Navigating AI Vendor Contracts and the Future of Law: A Guide for Legal Tech Innovators*, Stanford L. Sch. (Mar. 21, 2025), https://law.stanford.edu/2025/03/21/navigating-ai-vendor-contracts-and-the-future-of-law-a-guide-for-legal-tech-innovators.
[9] *Id.*
[10] *Id.*
[11] *Artificial Intelligence Index Report 2025, supra* note 1.
[12] Wellness and Oversight for Psychological Resources Act, 225 Ill. Comp. Stat. 155/1 (2025).
[13] N.Y. Comp. Codes R. & Regs. 20, § 870 (2021) (requiring a bias audit to be conducted on an automated employment decision tool).
[14] Cal Bus. & Prof. Code § 4999.8 (2025).
[15] *Mobley v. Workday, Inc.*, 740 F. Supp. 3d 796 (N.D. Cal. 2024).
[16] *See* Daniel Wiessner, *Workday Must Face Novel Bias Lawsuit over AI Screening Software*, Reuters (July 16, 2024), https://www.reuters.com/legal/litigation/workday-must-face-novel-bias-lawsuit-over-ai-screening-software-2024-07-15.
[17] *Id.*
[18] Mack, *supra* note 8.
[19] *AI Model Training: Silent IP Theft in Progress?*, InclusionCloud Digital Engineering (Apr. 29, 2025), https://inclusioncloud.com/insights/blog/ai-model-training-business-data-risks.



Alexandra (Ali) Nienaber
Perez Morris
anienaber@perez-morris.com

Adava Jefferson
Perez Morris
ajefferson@perez-morris.com