RAIL

The Journal of Robotics, Artificial Intelligence & Law

Publishing Staff
Publisher: Leanne Battle
Production Editor: Sharon D. Ray
Cover Art Design: Juan Bustamante

Cite this publication as:

The Journal of Robotics, Artificial Intelligence & Law (Fastcase)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

729 15th Street, NW, Suite 500, Washington, D.C. 20005
https://www.fastcase.com/

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@ meyerowitzcommunications.com, 631.291.5541.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

AI for GCs: What You Need to Know

Reece Clark, Cat Kozlowski, Kelsey L. Brandes, and Bryce H. Bailey*

In this article, the authors discuss the obstacles that general counsels and business leaders face when considering whether to adopt artificial intelligence, machine learning, and predictive applications and services.

During the course of 2024, interest in generative and other types of artificial intelligence, machine learning, and predictive applications and services (collectively, AI) accelerated across industries. Some sectors, such as financial services, media, and telecom, exceeded expectations for enterprise adoption. Others, such as life sciences, healthcare, energy, and industrials lagged behind.[1] The largest obstacles to enterprise adoption have been appropriate scaling and identifying a return on investment (ROI). Those challenges continue in 2025 and require a more critical examination by general counsels (GCs) and business leaders.

Last year, companies focused on user error and bias. Yet even as companies focused on comprehensive solutions to mitigate these types of AI risks, other headwinds to AI adoption became apparent. Strategic, operational, and compliance risks have coalesced to create a more complex adoption environment that is focused keenly on ROI.

GCs are now in a position to drive conversations beyond risk mitigation and legal compliance in AI tool selection. GCs will play a key role in shaping the conversations around opportunities and risks of AI adoption, and will find themselves continually asking the questions: What is the expected ROI of the AI tool, and how does that balance against legal risk?

Empowering GCs to Diligence AI Solutions

In the nearly two years since the public reveal of ChatGPT 3.5, companies have experienced a roller coaster of reactions to the potential applications (and pitfalls) of "generative AI." Generative AI is a type of AI that individual users are more likely to directly

observe as opposed to other types of AI that may recognize patterns or make predictions regarding data, transactions, images, or events, among other applications. Unlike generative AI, other types of AI have been in use for quite some time but have garnered less attention than generative AI.

Retrospectively, the initial burst of excitement around the possibilities of AI (especially generative AI) was certain to moderate just as the picture of AI's usefulness would begin to come into focus. At the onset of the "generative AI boom," some early movers invested in AI without a complete understanding of its current limitations and risks and have experienced challenges to implementation as a result.[2] Yet even as expectations around AI have begun to normalize, new AI solutions continue to launch at a breakneck pace. How then to make sense of the market?

Seasoned GCs know that over time, business leads become more discerning and realistic about the potential value a new technology can bring to the business. Shortly after a new technology launches, for example, excitement cools as the inflated expectations around its applications and capabilities fail to fully materialize.[3] AI is no exception. Businesses now can be expected to continue recalibrating their views around AI and to further moderate their performance expectations. This trend will be further accelerated due to more frequent instances of "AI washing"—a term GCs have (or will soon) become very familiar with.[4]

AI washing occurs, for example, when vendors oversell the AI capabilities of their products, or mischaracterize routine data processes as being "powered by AI." From "robot lawyers" to bunk investment strategy tools, examples of AI washing increased during the back half of 2024 and will likely continue to pervade the market in 2025.[5] AI washing erodes trust in AI providers, risks regulatory enforcement from the Securities and Exchange Commission and Federal Trade Commission (FTC) and accelerates the pace of industry skepticism in AI capabilities and ROI.[6]

With this backdrop, GCs will experience a renewed sense of urgency to ensure proper diligence occurs on potential AI deployments. GCs should feel empowered, for example, to charge their business leads with gathering qualitative and quantitative information about potential AI deployments from both the business teams using the tool and the AI vendor. To create a complete cost-benefit view, GCs will want to consider, at a minimum, the following questions as their business leads are choosing AI tools:

- *What Data Will the AI Tool Have Access To?* This is the most important question a GC faces. If the data profiles as low risk (e.g., historical budget information), then the overall risk from the AI tool is likewise lower. Conversely, if the AI tool will have access to personal information or sensitive business information, additional diligence is critical to ensuring the vendor has complied with applicable law, industry standard or better practices and rigorous security design in the development and maintenance of the AI tool.

- *How Was the AI Tool Trained?* GCs should expect vendors to be able to produce a base level of information regarding how the AI tool, including the underlying data or model supporting such tool, were initially trained and validated and tuned and improved over time. To be clear, this is not asking a vendor to reveal trade secrets or sensitive proprietary information. Rather, a well-trained AI tool should be backed by high-quality and often proprietary datasets that are specifically targeted to the industry the tool is marketed toward. Be wary of AI vendors that have difficulty producing information about how their tool was trained or vendors that reveal their datasets were validated exclusively through open-source information (that often carry a broad "as-is" disclaimer and no representations of legality or quality). Where a vendor has used some open-sourced data, additional questions regarding infringement and privacy concerns are warranted. For example, ask whether the vendor can ensure all licenses and consents were procured from the parties or individuals who have supplied the underlying information which may include proprietary or personal information?

- *How Much Risk Does Use of the AI Present?* Like any new field of technology, AI can present a variety of risks. There are strategic considerations evidenced by the need to scrutinize vendors for AI washing or overselling of their capabilities. Likewise, replacement of internal functionality with AI may bring a corresponding loss of human skill that needs to be carefully managed. There are compliance risks as well. These range from regulatory concerns to loss of company intellectual property (IP), security risks and ethical considerations. GCs will be particularly interested in how AI reduces operational challenges like

record-keeping, internal and external oversight, and additional vendor/contract management. AI can also present new technology-based challenges, such as proper quality control for outputs and a clear user understanding of how to use the tools effectively. GCs should use extra scrutiny when leveraging AI in heavily regulated or mission critical areas as they consider risk profiles.

- *What Is the Expected ROI?* Consider the time horizon and total impact of the expected return and whether it is worth the initial capital investment. For example, will implementation of an AI tool cause a change in staffing? Efficiency gains from head count reductions may be offset by transitional efforts and additional staffing for AI management, including output review, validation, and legal or other compliance or quality reviews. Likewise, depending on the size and complexity of the implementation, the full project timeline may be quite long before seeing any payoff, and will that lengthy period justify the up-front cost? Use-case analyses can help outline the actual ROI and impact of a given service and set apart vendors offering real AI solutions from those merely AI washing their services. Finally, consider the risk from potential breakdowns in support that may come from a vendor leaving the market or tech becoming outdated, and how that change will be managed in a rapidly evolving market.

Contracting with AI Vendors: Key Considerations

Last year saw a previous trend continue: the AI Addendum. These "one size fits all" attachments are designed to cover everything AI-related—and often suffer as a result from overly broad or underinclusive terms. Some examples of potentially problematic terms include requiring AI tools to be completely free of hallucinations and bias, meet multiple ISO (International Organization for Standardization) and NIST (National Institute of Standards and Technology) standards, comply with data privacy and AI laws regardless of jurisdiction, disclose all training data, and/or divulge all the model's secrets. When treating these addenda as "nonnegotiable" regardless of vendor agreement size or AI tool functionality, these fixed forms can create a disconnect between legal, the business and the AI tool's specific use case.

The better approach is for GCs to recognize AI and general-purpose models continue to change and, as a result, the contracting terms need to evolve with those changes. GCs should tailor and scale legal terms based on the applicable AI use case. For example, representations and warranties that a vendor will follow industry standards regarding data privacy and security, ethical use, and governance will almost always be appropriate. Likewise, GCs may benefit from including transparency requirements, such as obligations on the vendor to maintain the necessary documentation to assist with regulatory inquiries or investigations in the event the vendor has or receives an adverse audit or complaint regarding the AI tool.

Other contracting considerations GCs should keep in mind:

- *Data Access Issues*. While vendors offering unpaid general purpose models predominately seek rights to use company data as training data, the largest vendors provide a method for the user to opt out of training. For paid licenses, the prevailing approach from large language model vendors continues to be for the user to own its inputs and outputs. For more negotiated downstream AI tool agreements, GCs may push to limit the vendor's use of company data to only that which is necessary to provide the contracted services or as separately agreed upon in writing. However, if the AI tool will have access to particularly sensitive data, GCs may want to also explore additional contractual pathways of protecting or further limiting use and access to the data, such as designating outputs as confidential information, restricting disclosure, explicitly prohibiting certain uses that may otherwise be assumed as a part of providing services (e.g. performance monitoring or debugging performed directly or through data aggregation), or limiting data retention.
- *Indemnification Considerations*. GCs should continue to take care in negotiating and reviewing the indemnification provisions in agreements for AI tools. If a tool has been trained or tuned on top of a general purpose AI model, GCs need to identify whether they are protected from infringement and privacy claims regarding those materials. Depending on the use case, GCs may want to highlight other specific claims, such as bias or user-related errors

and omissions. Similarly, GCs should watch out for caps and exceptions to liability, particularly for IP infringement, privacy or data breaches, and violations of law. Generally, IP indemnification clauses include reasonable exceptions, such as if the user does not have proper rights to what they input, modifies the output, or intentionally attempts to cause the model to produce an infringing output. However, GCs should watch for additional conditions and requirements for indemnification, such as mandatory mitigation practices that require additional education or training for users.

- *Accuracy Requirements.* As a final risk mitigation consideration, GCs need to be aware that AI models, by design, are not stagnant. To prevent becoming "stale," models are regularly fed new training data that may fundamentally impact accuracy and performance and require more frequent corrective maintenance. A GC may therefore want to include minimums or additional explainability, transparency, and reproducibility requirements. The more integral an AI tool will be for a company, the more precise performance and standards requirements should be, and the greater care GCs may need to dedicate to termination, vendor transition, and operational contingencies should the tool or the vendor's business fail. GCs may also seek warranties that the AI tool will operate with reasonable accuracy for the nature of the use case, undergoes regular reviews and mitigation activities for data-based bias, and is supported by a vendor team that will resolve reported errors.

Looking Ahead: Balancing Risk and Reward

In 2024, GCs grappled with the business, legal, and regulatory impacts of prospective AI implementations in their businesses. Seemingly overnight, GCs became a key figure in driving conversations regarding risk mitigation and legal compliance in AI tools and, in the process, rapidly developed new competencies in data archaeology, transparency, accessibility, and privacy.

Now, the combined effect of a more discerning environment for adoption of AI tools and the AI-related expertise GCs have

gained means GCs will feature prominently in balancing risk and reward for prospective AI implementations and for developing a clear view of expected ROI.

For some AI tools, the benefits take time to accrue, which means a company may not see a productivity return for several months or years. Now more than ever, it is key for GCs to consider ROI when analyzing AI tools to be used within the business.

When evaluating AI tools:

- Identify clear objectives that fit in with the company's goals and strategies;
- Document and monitor short-term and long-term outcomes including when outcomes transform from indirect to direct (and ask the vendor to provide evidence regarding the same);
- Ensure that the business has defined key performance indicators (KPIs) for use of AI tools and is actively monitoring such KPIs;
- Consider the total cost—including environment costs, implementation costs, training and tuning costs, and other maintenance, verification, and staffing costs.

GCs will likely be challenging business owners more on AI tools, especially those that do not offer sufficiently clear ROI use cases to the business.

With government leaders taking office in several countries beginning in 2025, GCs will need to pay closer attention to current AI regulations and laws. Companies doing business in Europe, for example, will need to consider compliance with the EU AI Act. In the United States, President Donald Trump has selected Sriram Krishnan, a former Andreessen Horowitz partner and entrepreneur, as the Senior Policy Advisor for Artificial Intelligence within the White House Office of Science and Technology Policy. This appointment signals a focus on maintaining U.S. leadership in AI innovation and a deeper focus on how AI interacts with various industries and digital infrastructure. U.S. states are also poised to continue passing a patchwork of their own AI laws and states with current AI laws (such as Colorado) may amend those laws to provide additional regulations. GCs will need to monitor both international and U.S. federal regulations and state laws applicable to their business to ensure compliance with such regulations and laws.

Conclusion

AI will continue to offer diverse opportunities to increase company efficiency and ROI when deployed strategically within the enterprise. Companies should ensure that the vendors they have selected understand the overall implementation strategy, especially at the point of initial discussions with the selected vendor. GCs should ask pointed questions about the project scope, resources needed and potential impact of the AI tool before a contract is executed and then continue to monitor the evolution of those impacts up to and after implementation. Properly scrutinizing various AI services will allow GCs and companies to evaluate the greatest ROI offerings and best vendor for a given implementation.

Notes

* The authors, attorneys with Polsinelli, may be contacted at rclark@polsinelli.com, ckozlowski@polsinelli.com, kbrandes@polsinelli.com, and bryce.bailey@polsinelli.com, respectively.

1. Brian Campbell et al., "Three Ways Generative AI Can Drive Industry Advantage," Deloitte (Oct. 30, 2024), https://www2.deloitte.com/us/en/insights/topics/strategy/artificial-intelligence-in-business.html.

2. Eliud Lamboy, The AI Integration Challenge: Why Companies Struggle to Implement Artificial Intelligence, LinkedIn (July 20, 2024), https://www.linkedin.com/pulse/ai-integration-challenge-why-companies-struggle-lamboy-rn-mba-%CE%B4%CE%BC%CE%B4-neumc/.

3. Ankita Khilare et al., "Hype Cycle for Emerging Technologies, 2024," Gartner (Aug. 8, 2024), https://www.gartner.com/en/documents/5652523.

4. Bernard Marr, "Spotting AI Washing: How Companies Overhype Artificial Intelligence," Forbes (Apr. 25, 2024), https://www.forbes.com/sites/bernardmarr/2024/04/25/spotting-ai-washing-how-companies-overhype-artificial-intelligence/.

5. Kelly Miller et al., "AI Washing Erodes Consumer and Investor Trust, Raises Legal Risk," U.S. Law Week (Oct. 25, 2024), https://news. bloomberg law.com/us-law-week/ai-washing-erodes-consumer-and-investor-trust-raises-legal-risk. "Robot lawyer" company DoNotPay faces fines from the FTC for misleading customers that it could leverage AI to draft fully usable legal documents). Sheena Vasani, "Robot lawyer" company faces $193,000 fine as part of FTC's AI crackdown, The Verge (Sept. 25, 2024), https://www.theverge.com/2024/9/25/24254405/federal-trade-commission-donotpay-robot-lawyers-artificial-intelligence-scams. Multiple investment firms have been implicated in lying about their ability to leverage AI and machine learn-

ing to improve their investment strategies. Press Release, U.S. Securities and Exchange Commission, "SEC Charges Two Investment Advisers with Making False and Misleading Statements About Their Use of Artificial Intelligence" (Mar. 18, 2024), https://www.sec.gov/newsroom/press-releases/2024-36.

6. Marr, supra note 4.