WILLKIE

CLIENT ALERT

Optimizing AI Investments: Protecting Value and Managing Risk Through Expert Diligence

September 2, 2025

AUTHORS

Genevieve Dorment | Daniel K. Alvarez | Laura E. Jehl | Spencer F. Simon
Philip Coletto

Willkie is a trusted adviser to global investors at the cutting edge of the AI frontier. Over the course of hundreds of matters involving AI companies, Willkie's AI & Emerging Technologies team has gained invaluable experience using diligence to identify and quantify the risks presented by a particular AI investment, including the use of generative AI to produce outputs intended to be retained as proprietary, the use of agentic AI to perform tasks that may be high risk from a regulatory perspective, and the development of practical solutions and strategies to help investors optimize value from these investments.

Ultimately, investors want comfort that the success of their investments will be determined by the marketplace and companies' ability to innovate and execute in a competitive environment. Focused, thoughtful diligence can help identify whether there are other issues that may play a role, and how to protect against the attendant risks, including the use of shortcuts or vaporware that would undermine both the investment and an investor's credibility in the market.

Our experience on these matters has reinforced the importance of careful diligence, particularly on IP and privacy issues, when making an investment in an AI company. We consider here some of the key questions and areas of focus when conducting diligence in a fast evolving environment:

- Data sources and uses. Every AI tool is trained on data, therefore we need to understand where an AI company obtains the data it uses to develop and train its tools, whether from its own customers or other collection methods, or from a third-party provider, and whether it has requisite legal authority to use that data for training purposes. Where it subcontracts out some or all of the operation or development of its tools (for example, if its tool is built on a large-language model), an analysis is required to determine whether the rights, limitations, and obligations in the applicable contracts align with the contractual rights granted by the sources of the data. If the rights in and out fail to match up, the company could be in breach of its agreement with the data provider and additionally have liability for contributory infringement and under contracts with users of its products or services.

- Product ownership. One of the major legal and policy debates raised by the growth of AI in recent years has been the role of intellectual property, and the extent to which IP concepts like copyright should apply in the context of AI. While such debates (and accompanying litigation) are ongoing and evolving in real time, investors will want to know what IP risks are present in any company's AI tools. Key questions to ask include: Was another company's proprietary IP or data or any open source software used to develop, or incorporated into, the product or service? How strong are the IP protections for the product itself? Are any of the innovations embodied in the product protected or protectable by patent, copyright or trade secret?

- Ownership of and rights to use inputs and outputs. Licenses, terms of use, customer agreements, and other contracts may require nondisclosure and/or prohibit certain uses of data which may give rise to a breach of contract claim if the data used as an input to an AI model or tool is also used to train, test or validate that AI model or tool. Moreover, outputs should be validated, logged, monitored and audited and, given the uncertainty around the ability to own AI-generated content, it is important to understand whether a company's AI tool is being used to create outputs that are intended to be retained as proprietary. If outputs from a company's AI tool are to be provided to and potentially relied upon by third parties, do the relevant contracts include clear disclosures, disclaimers and limitations on liability related to their creation, use, accuracy and non-infringement of third party rights? Investors should also inquire about specific protections for inputs and outputs against leakage and adversarial attacks.

- Special risks associated with the use of personal data or confidential information. The use of personal data to train AI implicates laws like, CCPA, GDPR, and other privacy laws in the US, Europe, UK, and around the world, and may complicate companies' compliance efforts. Understanding the scope of the company's personal data collection and processing, whether and how personal data is used to develop or train the AI, and what controls a company has in place to ensure that it is prepared to respond to data subject requests (including requests to opt-out of or object to continued processing) are critical to scoping the risk and

potential liabilities presented by a particular company's practices. Likewise, if confidential, sensitive or competitively valuable data is input into an AI tool, investors will want to understand who has access to that data, will it be retained, and can it be reproduced in a way that could breach confidentiality obligations or undermine trade secret protection.

- Evolving regulatory schemes. Around the world, policymakers and regulators are adopting laws and regulations aimed at curbing potential abuse and misuse of AI tools. Most of these are aimed at so-called "high-risk" uses—for example, using an AI tool in the context of offering a job or promotion, determining whether an individual is eligible for a financial product, or the use of AI in the context of healthcare, critical infrastructure, or education—and some regulations and prohibitions are already in effect. Diligence can help investors understand the extent to which regulation may present challenges for a company's growth, and how ready the company is to address those challenges.

- Governance and risk management. Given the risks presented by the use and development of AI tools, every company should have a governance framework in place to help manage those risks by identifying both acceptable and prohibited uses of AI, and promoting visibility and compliance. Investors will want to know whether the company has an AI-specific use policy or relies on a generic acceptable use policy. Companies with AI-specific policies are better positioned to successfully manage both the risks we know about, and the risks waiting over the horizon.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Genevieve Dorment

212 728 3865
gdormant@willkie.com

Daniel K. Alvarez

202 303 1125
dalvarez@willkie.com

Laura E. Jehl

202 303 1056
ljehl@willkie.com

Spencer F. Simon

212 728 8525
ssimon@willkie.com

Philip Coletto

44 20 3580 4744
pcoletto@willkie.com

WILLKIE

BRUSSELS CHICAGO DALLAS FRANKFURT HAMBURG HOUSTON LONDON LOS ANGELES
MILAN MUNICH NEW YORK PALO ALTO PARIS ROME SAN FRANCISCO WASHINGTON

Copyright © 2025 Willkie Farr & Gallagher LLP. All rights reserved.

This alert is provided for educational and informational purposes only and is not intended and should not be construed as legal advice, and it does not establish an attorney-client relationship in any form. This alert may be considered advertising under applicable state laws. Our website is: www.willkie.com.