AI IN PE TRANSACTIONS: RETHINKING VALUE, RISK AND EXECUTION

FEBRUARY 2026

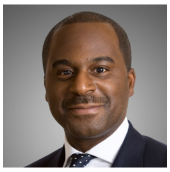
Weil

AI is changing how we assess value, risk and execution in technology-related PE deals. This note sets out just some of the key issues to consider across IP, data, operational resilience and governance and liability, and how AI can reframe elements of both the investment thesis thinking and traditional diligence.

Investor issue	Key focus areas
Intellectual property as a value driver and moat	
Proprietary source code alone may no longer provide a durable moat AI-assisted development is making it easier and cheaper to build and replicate software. This means that source code alone may not provide the lasting competitive edge it once did, unless coupled with other value drivers. Investors are already asking this question, and we have seen this reflected in how the market is valuing software businesses.	▪ How central is proprietary source code to the investment thesis? ▪ Is the code itself the moat, or is value actually driven by data, domain expertise, customer relationships or service integration, or a mixture of all of the foregoing? ▪ How does the business expect its software advantage to remain durable as AI-assisted development becomes more widespread and sophisticated?
Ownership of AI-generated assets is uncertain Legal frameworks for IP ownership were not designed with AI in mind. Ownership of AI-generated outputs (including AI-generated code) is evolving and may vary significantly by jurisdiction and fact pattern. Unclear ownership creates execution and exit risk.	▪ How is AI used to develop outputs that are material to the business? ▪ What level of human involvement exists in shaping, directing or refining those outputs? How are those outputs reviewed, modified or integrated? ▪ What technical and contractual controls are in place to prevent leakage, misuse or unauthorised access to those outputs? Have there been any instances of disclosure to third parties (e.g. for AI-generated source code)?
Data rights and control	
AI strategy depends upon having the correct data and data rights AI-driven value rests on access to quality, relevant data - but access alone is not enough. The business must have the legal rights to use that data for its intended AI purposes.	▪ What is the business entitled to do with the data it holds? Can the data be used across customers, products or markets, or is use limited to specific customers, use cases or contexts? ▪ Who controls the data, and on what terms (including exclusivity and termination rights)? Can customers use or access the same data? ▪ Do sector-specific rules restrict how the data can be used (e.g. in payments/ fintech, PSD2 and related payment services rules may limit use of transaction or customer data to authorised purposes)? ▪ Were AI models trained on data the business was entitled to use for that purpose? Is there any exposure from historical training practices?

Investor issue	Key focus areas
Data and AI-derived insights can leak or erode. If data is key to the business but it does not effectively control how its data and outputs are used, then proprietary insight may be diluted or commoditised over time. If the data advantage erodes, so does the investment thesis/ exit risk is created.	▪ How is access to proprietary data controlled? How is it protected when interacting with third party tools? ▪ Do customers or partners receive outputs that could allow them to reverse-engineer underlying data or models? ▪ Are there restrictions on customers using outputs for certain purposes, e.g. benchmarking, model training or competitive purposes?
Operational resilience and governance	
AI shifts critical risk to third parties Reliance on external AI models introduces an additional layer of dependency on top of existing cloud risk. AI systems actively shape outputs and decisions-so provider failure, degradation or restriction can have immediate operational impact, exposing the business to disruption and value erosion, even where core systems remain operational.	▪ How much visibility does the business have into third-party security and resilience (e.g. audit rights, certifications, incident reporting)? ▪ Which third-party models or providers are critical to AI functionality? Is there concentration risk around a single vendor? ▪ What would be the impact of a provider outage, price increase or regulatory restriction? ▪ Can the business switch models or providers without material disruption? Is there evidence of multi-model or fallback capability?
Rigid AI governance can become a drag on value AI regulation is increasing and diverging across jurisdictions. If governance frameworks are too narrowly tied to current rules, the business may struggle to adapt, slowing deployment, limiting scalability and creating compliance headaches.	▪ How is AI governance structured? Is it principles-based or tied to specific current laws? ▪ How does the governance framework adapt when regulations change or differ across jurisdictions?
Liability	
AI liability is hard to pin down and could leave the business exposed AI systems often operate as a "black box", making it hard to pinpoint responsibility when something goes wrong. Is it the model provider, the developer, or the deployer? Market practice is still evolving, and the exposure will depend on how much the business relies on AI and how it is integrated. Unquantified liability affects value, unclear allocation creates execution risk, and buyers will scrutinise these frameworks closely at exit.	▪ How does the business allocate liability for AI-related errors or harms in its contracts? ▪ Is there clarity on who bears responsibility across the AI supply chain-model provider, developer, or deployer?

FOR MORE INFORMATION



BARRY FISHLEY

+44 20 7903 1410
barry.fishley@weil.com

CHLOE KITE

+44 20 7903 1206
chloe.kite@weil.com

WEIL.COM

Weil