PUBLICATION

Artificial Intelligence as a Litigation Multiplier: Contract and Risk Issues for AI-Enabled Services

Authors: Scott M. Douglass, John D. Koesters, Clinton P. Sanko
May 28, 2026

AI Is Not a Standalone Tool - It Is a Layer Across the Data Stack

Artificial intelligence (AI) is increasingly deployed not as a discrete product, but as a layer embedded across existing technology services. AI functionality now appears inside software as a service (SaaS) platforms, operating systems, security tools, customer support software, and data analytics environments. For most enterprises, AI is encountered as a feature of the existing technology stack, not as a new or separate procurement decision.

This reality matters when disputes arise. Litigation involving AI rarely turns on abstract questions about the technology itself. Instead, disputes typically focus on how AI was deployed, what contractual promises govern its use, and how responsibility for AI-driven outcomes is allocated between providers and customers.

As with other data-driven technologies, AI tends to magnify risk that already exists in the contracting relationship. Where responsibilities are unclear, data use is poorly defined, or liability is heavily disclaimed, AI does not introduce new problems so much as accelerate or exacerbate existing ones.

Inputs, Prompts, and Outputs: Where Most AI Disputes Begin

From a litigation perspective, nearly every AI dispute can be traced back to one or more of three concepts: customer-owned data and inputs, customer-designed prompts, and AI outputs.

- Inputs and prompts raise questions about ownership, confidentiality, and permissible use. Disputes frequently arise over whether customer inputs or the prompts themselves can be retained, reused, used to train models, or troubleshoot global issues with the system. This is particularly acute where those inputs contain proprietary, regulated, or sensitive information, or the material is otherwise subject to some other privilege or immunity.

- Outputs raise different issues, including accuracy, reliability, and intellectual property rights. Claims often involve alleged reliance on incorrect outputs, downstream business impacts, or disputes over who owns or can exploit AI-generated results.

Most AI providers' terms of use attempt to resolve these issues in advance through broad disclaimers, "as-is" language, and express allocation of human verification responsibility to the customer. When litigation arises, courts and arbitrators will need to assess whether those provisions are enforceable in the context of how the specific AI was marketed and deployed, and the reasonableness of the reliance upon its outputs.

General Models, Closed Systems, and the Data-Use Divide

One of the most consequential distinctions in AI disputes is whether the AI system operates as an open, general model or as a closed or enterprise-controlled system.

General models often reserve expansive rights to use customer inputs to improve services or train models, with limited confidentiality protections (and often limited protections for attorney-client privileged or other

protected material). Closed or enterprise systems may promise tighter data controls, restricted training use, or segregation of customer data, but those assurances must be clearly documented and consistently implemented.

Litigation frequently follows when customer expectations about data isolation or non-training collide with contractual language that quietly allows broader use. These disputes are rarely resolved by technical testimony alone; instead, they turn on how data-use rights were described, documented, and prioritized across the contract layers.

"Human-in-the-Loop" and the Reallocation of Risk

AI agreements increasingly include "human-in-the-loop" requirements, professional-advice disclaimers, and express warnings against reliance on outputs without independent verification. These provisions are designed to shift risk away from providers and onto customers.

In litigation, such clauses can become a focal point. Plaintiffs may argue that the disclaimers are inconsistent with how the AI tool was marketed, sold, or integrated into operational workflows. Defendants, in turn, rely on the same clauses to argue that reliance was unreasonable as a matter of contract.

The practical takeaway is that human-in-the-loop language is not merely boilerplate. It has real consequences for how fault, causation, and damages are framed when disputes arise.

Acceptable Use, Silent Updates, and Moving Targets

Another recurring source of AI-agreement-related risk involves acceptable use restrictions and unilateral updates to terms of use. AI providers frequently reserve the right to modify acceptable use policies, usage limits, or feature availability with little notice.

Problems arise when customers deploy AI tools at scale based on one set of assumptions, only to find those assumptions altered midstream. In regulated industries or mission-critical applications, such changes can trigger operational disruptions, compliance issues, or audit findings. Each of those scenarios may cascade into disputes over breach, reliance, or unfair practices.

These risks are amplified where AI terms are layered on top of existing SaaS or services agreements without clear precedence rules. Some AI providers diligently update SaaS or services agreements to address AI-specific functionality. However, for many, the original terms of the underlying software often are not updated to reflect the add-on AI application (or, at least, are not updated sufficiently). Thus, the contract documents do not adapt appropriately to "fit" the purpose of the software as it has evolved and become integrated with the AI functionality. This contract mismatch between the language used in the documents and the operational reality can amplify the risks to both parties in the event of a dispute.

Contract Structure Matters More Than Novel Legal Theory

Despite the rapid pace of AI innovation, most AI disputes are resolved using familiar contract-law principles. Courts are not inventing new doctrines so much as applying existing ones to new facts.

Key provisions that repeatedly shape outcomes, and where parties should increasingly direct their attention in contract negotiations, include:

- The definition and scope of AI-enabled services;
- Data ownership, training rights, and reuse provisions;
- Disclaimers related to accuracy, non-infringement, and reliance;
- Limitations of liability and exclusions for consequential damages; and

- Integration and precedence clauses governing clickwrap, enterprise agreements, and third-party flow-down terms.

Where AI is embedded through resellers, platforms, or value-added providers, disputes also turn on who bears responsibility for upstream AI failures versus downstream services, and whether that allocation is explicit or merely assumed.

Preparing for AI Disputes Before They Arise

AI-related litigation remains relatively nascent, but its contours are already predictable. Disputes tend to emerge not from cutting-edge legal questions, but from misalignment between party expectations, actual operations, and contract language that has not evolved to specifically address the issues.

Steps your organization can take now to better position itself for AI disputes include understanding how and where AI is deployed across their technology stack; evaluating AI terms in the context of their broader contractual ecosystem; aligning internal policies on data use, confidentiality, and reliance with external agreements; conducting periodic gap analyses between AI capabilities and contractual protections; and resisting the temptation to treat AI add-ons as purely technical upgrades rather than legal risk events requiring contract adaptation.

Looking Ahead

The next article in this series will turn to cybersecurity disputes, where AI can play a supporting role or a consequential role – or to the chagrin of some parties, both a supporting and consequential role – in detection, monitoring, and response. The final article will examine what happens when technology failures escalate into formal disputes, including evidence preservation, logging, and early litigation strategy.

Across all of these topics, the central lesson remains consistent: AI changes how disputes unfold, but contracts still determine how they end.

***

If you have questions about this alert and what it means for your organization's technology-provider relationships and data-risk posture, please reach out to Scott M. Douglass, John David "J.D." Koesters, Clinton P. Sanko, or any member of Baker Donelson's Data Privacy and Cybersecurity team.