

Contracts Corner: Aligning AI Contract Clauses with Business Goals

Commercial and Contracts

Technology, Privacy, and eCommerce



Banner artwork by Andrey_Popov / *Shutterstock.com*

AI is now standard in B2B technology offerings, yet the commercial contracts governing the use of those tools often still rely on generic AI disclaimers or cursory AI exhibits. That improvised structure does not address key aspects that are important for the customer and vendor. This article provides a framework for in-house counsel to assess and address issues related to AI tools, products and services in commercial agreements from both the vendor's and the customer's perspectives.

Discussion Prompts for Counsel to use with business stakeholders:

1. What is the AI tool supposed to do?
Not every AI offering presents the same risk. Counsel should distinguish among back-office applications, customer-facing functionality, model training, and autonomous decision-making.

2. What company assets and data may be exposed by using the AI tool?
The key issues usually involve confidential information, personal data, scraped content, regulated data, and IPR concerning inputs, outputs and improvements.

3. What happens if the AI goes awry?
The contract should address responsibility for errors, hallucinations, bias, infringement, security failures, regulatory noncompliance, and changing functionality over time.

Start with your company's AI governance policy

The best starting point for AI-related contracts is not the customer's form or your SaaS form (if you are the vendor). Rather, it is your company's internal AI governance policy.

> The best starting point for AI-related contracts is not the customer's form or your SaaS form (if you are the vendor). Rather, it is your company's internal AI governance policy.

Your company's AI governance policy can provide a strategic framework to transform technology contracts into active risk management tools, ensuring accountability, ownership clarity, and alignment with regulatory requirements. As Caroline McCaffery who leads OutsideGC's Artificial Intelligence, Cybersecurity and Data Privacy Practice Group, advises, "There are at least 9 AI governance frameworks to choose from. Counsel should pick the one that aligns best with their company's current processes, particularly around privacy and cybersecurity, to streamline adoption." "Many companies are moving beyond the AI addendum and initial AI use policies to Phase 2, where different use cases of AI receive different scrutiny, just like any risk matrix."

As customer's counsel, your company's AI governance policy will guide your baseline positions vis-à-vis your negotiations with the vendor's team. For example, if your policy mandates strict limitations on how vendors may use customer input data, then the contract should clearly define ownership of outputs.

If no formal AI policy or baseline exists, it may signal the need for counsel to convene a cross-functional taskforce to consider developing an AI governance policy and consult with expert outside counsel for guidance.



Defined terms deserve attention

Definitions matter, especially because AI terminology remains unsettled. Contracts often use terms such as “artificial intelligence,” “machine learning,” and “generative AI” as though they are interchangeable. They are not. For example, a broad definition of AI might include simple automated scripts (e.g., basic "if-then"), which could subject routine, automated scripts to burdensome compliance obligations under the contract.

Likewise, common AI-related descriptors such as “autonomous,” “closed,” and “train” deserve clarity. For example, the definition of “autonomous” should distinguish between tools that simply automate tasks versus those that use machine learning to make autonomous decisions. If the contract describes "training", as “ingestion of data to improve the model”, a more in-depth definition of “training” could determine whether a vendor can use customer's proprietary data to improve their public model, which could potentially expose trade secrets – a risk that counsel for customer would likely not want to expose their company to.

Broad definitions quickly create problems in the AI arena. Contract definitions that focus on functionality using specific examples like those above are better for both the vendor and the customer. Precise definitions add clarity and reduce friction for the business parties once the tool is deployed.

Add AI language into the IP and warranty framework

AI provisions should be integrated into the contract’s broader treatment of key commercial provisions like data privacy, confidentiality, indemnification, IP, warranties, liability, etc. Below we discuss the benefits of adding AI language into provisions that concern intellectual property and warranties.

This starts with clear ownership distinctions among deliverables, preexisting materials, underlying tools, models, and AI-generated outputs. If AI is used in creating deliverables, the agreement should address what the customer owns, what the supplier retains, and what rights are being granted for use of outputs and related materials.

Counsel for both sides should also approach warranties and disclaimers with care. For example, customer's counsel should be skeptical of broad “as-is” disclaimers, especially as concerns outputs and their accuracy. If the vendor’s marketing materials make claims about the AI tools capabilities, customer counsel should consider including performance metrics that align with those claims and are measurable along with termination rights or “gratis subscription term extension” if those targets are not met. For vendor’s counsel, including appropriate disclaimers concerning output accuracy may make sense especially if the disclaimer absolves vendor of liability due to inaccuracy of training data or customer inputs beyond vendor’s control.

Once counsel and her business stakeholders have assessed the AI tool’s intended use vis-a-vis the company's AI policy, counsel may more appropriately address related risks within the contract’s existing IP, warranty, and liability framework in a clear and intentionally bounded way.

Regulatory Compliance: Prepare to pivot

AI regulation is evolving quickly, and sector-specific rules may already apply in areas such as healthcare, financial services, employment, consumer products, and government contracting. State laws like the Colorado AI Act impose specific obligations on vendors of high-risk AI systems. Requiring vendors to comply with “all applicable laws and regulations during the Term” is a

reasonable ask from the customer side. In addition, the contract should provide for a method to amend its terms, so the parties may adjust it to accommodate for new laws or regulations without renegotiating the entire agreement.

At the same time, flexibility should not come at the expense of operational clarity. The strongest clauses use compliance language that is adaptable enough to account for changing legal requirements (e.g., “vendor shall comply with all applicable laws and regulations during the Term”) while remaining concrete enough for the business to implement.

As AI becomes part of ordinary products and services, careful contract drafting by in-house counsels is what separates responsible adoption from preventable risk for both sides.

Join ACC for more AI insights!

Disclaimer: The information in any resource in this website should not be construed as legal advice or as a legal opinion on specific facts, and should not be considered representing the views of its authors, its authors’ employers, its sponsors, and/or ACC. These resources are not intended as a definitive statement on the subject addressed. Rather, they are intended to serve as a tool providing practical guidance and references for the busy in-house practitioner and other readers.

Billie Munro Audia



Partner and Retail, Marketing & Media Practice Area Leader

Outside GC

Billie Munro Audia writes the Contracts Corner column, partnering with in-house counsel, for *Corporate Counsel Now*. She is a partner with Outside GC, the provider of choice for on-demand general counsel services, and she leads the firm’s Retail, Marketing & Media Practice. Billie has 20+

years of commercial legal experience in the retail, media, and technology sectors, including 7 years in London as European General Counsel for two Silicon Valley technology companies and 4 years in San Francisco as the Director of Commercial Transactions for Gap, Inc. At the beginning of her career, she was an associate with Covington & Burling.

Ana Liggio



Assistant General Counsel

Catalent Pharma Solutions, LLC.

Ana O'Keefe Liggio is an Assistant General Counsel with Catalent Pharma Solutions, LLC., a global provider of delivery technologies, development, drug manufacturing, biologics, gene therapies and consumer health products. Ana is a healthcare, tech, and life sciences attorney, with over 15 years of experience advising clients on commercial matters such as contracting, data privacy and security, dispute resolution, and compliance. Ana is a member of the Association of Corporate Counsel and frequently participates in ACC conferences.