Legal Tech: Navigating Indemnification Clauses in AI-Related Agreements

Commercial and Contracts

Technology, Privacy, and eCommerce

Banner artwork by David Gyung / *Shutterstock.com*

In the domain of AI, the growing importance of indemnification in AI-related agreements cannot be overstated. AI introduces heightened legal complexities in areas of liability, intellectual property (IP) rights, and data security. These intricacies stem from AI's unique capabilities and the unforeseen risks associated with its deployment: potential IP infringement due to the use of an intricate web of underlying algorithms and data or liability issues arising from autonomous decision-making processes. As such, in-house counsel plays a pivotal role in strategically structuring indemnification clauses within these agreements.

Understanding indemnification in AI-related agreements

Definition and scope of indemnification

Indemnification in AI-related agreements refers to a contractual arrangement where one party agrees to compensate the other for losses or damages incurred due to specific circumstances outlined in the agreement. In agreements involving AI systems, the scope of indemnification may be opaque. It may encompass a range of potential issues, including but not limited to, operational failures of AI systems, errors in output, and unforeseen consequences of AI decision-making. Therefore, indemnification clauses emerge as critical tool for managing and allocating risks associated with deploying and utilizing AI technologies.

> Indemnification in AI-related agreements refers to a contractual arrangement where one party agrees to compensate the other for losses or damages incurred due to specific circumstances outlined in the agreement.

Necessity of indemnification for various losses

The necessity for indemnification in AI agreements is driven by the potential for various types of losses, which are unique to the technology. These may include:

- Breaches of contract: AI systems may inadvertently lead to situations in which contractual obligations are not met, necessitating indemnification to cover losses arising from such breaches.
- Intellectual property (IP) infringement: The AI landscape is rife with IP challenges, given that AI systems often rely on large datasets and complex algorithms, some of which may allegedly infringe on existing IP rights. Indemnification clauses are essential to protect against claims of such infringement.
- Legal non-compliance: AI technologies operate in a legal environment in which regulators are moving swiftly to enact laws, particularly in data privacy and consumer protection areas. Indemnification for losses arising from non-compliance with new and evolving legal requirements is crucial for both providers and users of AI technologies.

Inclusion of comprehensive indemnification clauses in AI-related agreements thus serves as a safeguard, ensuring that parties are protected against the unique risks presented by AI technologies while promoting a responsible and legally compliant approach to AI development and deployment.

Key elements of AI indemnification clauses

Addressing breaches of contract and legal compliance

Indemnification clauses in AI-related agreements should delineate what third-party claims for what breaches of contract are subject to indemnification. This is particularly crucial in AI, where non-compliance can have significant legal and operational repercussions. The clause should clearly specify AI-related obligations, such as confidentiality, security, and legal compliance, that if breached and leading to claims, will require indemnification.

Managing intellectual property infringement risks

Given AI algorithms and datasets' complex nature, the risk of inadvertently infringing on existing intellectual property rights is present. Indemnification clauses should address this risk, providing a safety net against potential IP litigation. These provisions typically require the indemnifying party to bear the cost of defending any IP infringement claims and to compensate for any damages awarded. This is vital in an environment where the ownership and use of AI-related IP can be a legal minefield.

Negligence and misconduct in indemnification clauses

While revolutionary, AI systems can be prone to errors, which may lead to negligence claims. Indemnification for negligence and misconduct is a critical aspect of these clauses, covering scenarios in which AI systems cause harm, either due to flaws in their design or operational failures. This includes both unintentional negligence and willful misconduct, offering a layer of financial protection against such liabilities.

As AI systems quickly evolve, errors can present themselves which may then lead to negligence and misconduct claims. MarutStudio / *Shutterstock.com*

Indemnification and limitations of liability

Generally, a limitation of liability applies only to direct damages and not to indemnification obligations to indemnify third-party claims. Because indemnification is a performance obligation, the cap on limitation of liability is not operative unless the language is drafted to expressly establish a limit on the indemnification responsibility. In-house counsel must ensure that indemnification obligations are not constrained by the limitations of liability, which might render the indemnification ineffective.

> In-house counsel must ensure that indemnification obligations are not constrained by the limitations of liability, which might render the indemnification ineffective.

Insurance for indemnification obligations

Ensuring that indemnification obligations are backed by adequate insurance is crucial. This may involve specialized insurance policies that cover unique AI-related risks, such as errors and omissions, cyber liability for data breaches, and other operational failures. Insurance adds a layer of financial security and offers peace of mind, ensuring that the indemnifying party has the means to fulfill their obligations under the indemnification clause.

Structuring indemnification clauses

Nuanced understanding of AI risks

The first step in crafting an indemnification clause for an AI-related agreement is to thoroughly understand the specific risks of the AI technology. This includes general technology risks and those unique to AI, such as unpredictable decision-making, evolving algorithms, and complex data dependencies. An effective clause must address these unique AI characteristics and risks to adequately protect the parties against AI-related liabilities.

The first step in structuring an indemnification clause for an AI-related agreement is to develop a nuanced understanding of the specific risks associated with the AI technology in question. This involves recognizing not just the general risks common to technology agreements but also those unique to AI, such as the unpredictability of AI decision-making, the evolving nature of AI learning algorithms, and the complexities of data dependency. An effective indemnification clause is tailored to address these unique characteristics and potential risks of AI, ensuring that the parties are adequately protected against specific AI-related liabilities.

Clearly defining the scope of indemnification

Clarity in the scope of indemnification is paramount. The clause should explicitly define what constitutes indemnifiable events or circumstances in the context of the AI technology being used or provided. This includes detailing the types of damages, losses, or liabilities covered, such as those arising from AI system malfunctions, data inaccuracies, or failure of the AI to perform as represented.

It's also crucial to define what is not covered, setting clear boundaries to the indemnification obligations. For example, many indemnification clauses in the AI space specifically exclude "self-trained" AI models, the outputs of the AI model, modifications to the provided AI components, or the combination of the provided AI components with any other components, including consumer-provided components. Because AI models are nearly always incorporated into larger systems, many existing indemnification clauses provide miniscule (or even illusory) coverage. The aim in drafting your own indemnification clause, therefore, is to leave no room for ambiguity, thereby minimizing the potential for future disputes over the clause's interpretation.

Clearly specify liabilities covered and not covered when drafting an indemnification clause, leaving no room for confusion and limiting possible controversy. create jobs 51/ *Shutterstock.com*

Software malfunctions, data breaches, incorrect outputs, and failure to audit

Given that AI systems rely heavily on software algorithms and data processing, indemnification clauses must specifically address indemnification for third-party claims arising from risks like software malfunctions, data breaches, incorrect outputs, and the failure of the provider to audit outputs. For software malfunctions, the clause should cover scenarios in which the AI system fails to operate as intended. For data breaches, it should address the consequences of unauthorized access or loss of data, particularly sensitive data. As for incorrect outputs, the clause should cover the implications of the AI system providing incorrect or inappropriate results, which could lead to operational failures or incorrect decision-making. Finally, for failure to audit, the indemnification provisions should cite applicable audit frameworks, such as the bias audit requirements under [NYC Local Law 144 of 2021](#).

Best practices for indemnification in AI-related agreements

Establishing clear definitions and scope of indemnity

Ambiguities in legal documents can lead to contentious interpretations. Therefore, it is essential to define key terms such as "AI system," "data breach," or "system malfunction" and clearly delineate the scope of indemnity. This includes specifying the types of damages covered, the circumstances under which indemnification is applicable, and any exceptions to the indemnity.

Setting limitations and exclusions in limitation of liability clauses

Indemnification clauses can create unlimited obligations depending on the language used and any express limitations of liability. Setting reasonable limitations and exclusions is necessary to have a fair allocation of risk. The limitation of liability disclaimer will typically exclude consequential damages in most commercial agreements. It should also be modified to include an exception related to breaching the delivery of AI-related services as promised because the nature of those damages is primarily consequential. Diligent in-house counsel should thoroughly investigate whether the limitation of liability should apply to claims arising from user-trained or user-altered AI models, the outputs of the model (for example, in response to a user-generated prompt), or combinations with components not provided by the AI vendor.

Ensuring compliance with relevant laws and regulations

The indemnification should provide coverage for a violation of applicable law. As the applicable laws on AI are rapidly evolving, explicitly citing specific laws with which compliance is expected, like New York City's law on Automated Employment Decision Tools, can provide additional certainty. However, it is important to ensure that a specific legal citation is accompanied by language that contemplates compliance with applicable laws promulgated after the agreement's effective date. Staying abreast of legal developments and adapting the indemnification clauses accordingly to have more specificity is essential for legal soundness and enforceability.

> It is important to ensure that a specific legal citation is accompanied by language that contemplates compliance with applicable laws promulgated after the agreement's effective date.

Mastering AI indemnification clauses

In conclusion, navigating indemnification clauses in AI-related agreements is crucial for in-house counsel. Current trends highlight the need for a deep understanding of AI's risks, careful clause structuring, and balanced risk protection. By conducting detailed risk assessments, defining indemnity clearly, and ensuring legal compliance, legal professionals can create clauses that are robust, fair, and practical. Such clauses protect organizations from AI's unique risks and foster sustainable business relationships, underscoring in-house counsel's evolving role as strategic advisors in the digital era.

[Join ACC](#)

[Olga V. Mack](#)

Fellow

CodeX

Olga V. Mack is a fellow at CodeX, The Stanford Center for Legal Informatics, and a Generative AI Editor at law.MIT. Mack shares her views in her columns on ACC Docket, Newsweek, Bloomberg, VentureBeat, Above the Law, and many other publications.

Mack is also an award-winning (such as the prestigious ACC 2018 Top 10 30-Somethings and ABA 2022 Women of Legal Tech) general counsel, operations professional, startup advisor, public speaker, adjunct professor, and entrepreneur. She co-founded SunLaw, an organization dedicated to preparing women in-house attorneys to become general counsels and legal leaders, and WISE to help female law firm partners become rainmakers.

She has authored numerous books, including Get on Board: Earning Your Ticket to a Corporate Board Seat, Fundamentals of Smart Contract Security and Blockchain Value: Transforming Business Models, Society, and Communities. She is working on her next books: Visual IQ for Lawyers (ABA 2024), The Rise of Product Lawyers: An Analytical Framework to Systematically Advise Your Clients Throughout the Product Lifecycle (Globe Law and Business 2024), and Legal Operations in the Age of AI and Data (Globe Law and Business 2024).

Brian Mack

Partner

Quinn Emanuel

Brian Mack is a partner in Quinn Emanuel's San Francisco, California, office. His practice focuses on high-stakes complex commercial litigation and intellectual property disputes, including data privacy, patent, copyright, trade secret, and trademark actions. He also specializes in antitrust and unfair competition matters. Mack has tried cases in state and federal courts throughout the country, as well as before the [US International Trade Commission](). He has helped clients develop and license international patent portfolios and has tackled many complex intellectual property issues, including fair, reasonable and non-discriminatory ([FRAND]()) licensing, standards setting organizations, patent exhaustion, patent interferences and patent reexamination proceedings. He has also been admitted to practice before the [US. Patent & Trademark Office](). Mack was recently named a Rising Stars by Law360 in the Technology practice area and selected by the National LGBT Bar Association as one of the Best LGBT Lawyers Under 40.

[Foster Sayers]()

Vice President of Legal Operations

Foster Sayers is vice president of legal operations for symplr. His career includes 15 years of in-house legal experience that began as a staff attorney for Mainline Information Systems, IBM's largest channel partner in North America, and he most recently was general counsel and chief evangelist for Pramata Corporation and before that legal counsel for private equity-backed Vertafore.

He also has experience as an entrepreneur and inventor, having founded two companies (including his most recent venture, Tactile VR) and is a first-named inventor on three US patents and a Canadian patent. He is published author and speaker on topics such as contracts, cybersecurity, employment practices, ethics, and artificial intelligence.