LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Rethinking Tech Contract Terms For Governance Of AI Use

By **Marina Aronchik and Samuel Hartman** (November 27, 2023, 5:09 PM EST)


Marina Aronchik


Samuel Hartman

Artificial intelligence — the combination of computer science and data to solve problems, including through the use of algorithms that attempt to make predictions or classifications based on input data — is booming.

AI tools like ChatGPT and DALL-E have captured the public consciousness,[1] and the world's largest technology companies, including Google LLC,[2] Microsoft Corp.[3] and Amazon.com Inc.[4] have announced significant investments in AI technology.

Because the AI technology marketplace is dynamic and rapidly evolving, so too are the relevant legal terms for deals involving AI. In this article, we discuss several high-value terms lawyers should carefully consider and address in a deal that involves AI.

The Need for New or Different Terms in AI Deals

Existing deal terms and traditional considerations in technology deals are often inadequate for AI.

Businesses might expect existing agreements — including, on the procurement side, those with major technology providers like Google, Microsoft and Amazon — to be sufficient to cover AI.

Similarly, one might assume that existing contract templates and negotiation playbooks can be tweaked to cover AI-specific deal points. Yet, providers may — and often do — introduce new contractual terms for AI technology, including through links to online terms or a registration process requiring customers to consent to separate legal terms in order to use AI products.

It is also possible — though in our experience, less common — for a provider to insist that a contract for AI be entirely separate from the existing enterprise deal.

The use of AI technology by an enterprise requires technology lawyers to revisit, and in many cases, reimagine existing terms across the full spectrum of relevant contracts, ranging from procurement agreements and data licenses to customer contracts.

There are several examples of the terms and conditions governing the provision and use of AI that should be considered and addressed to mitigate the risks attendant to AI technology.

Rights to AI Input, Training Data and AI Model Improvements

The concepts of AI input including prompts, training data and model improvements — or the data processed in the AI tool and results of this processing, and the related allocation of intellectual property and other rights — are similar to the traditional constructs of customer data, usage data and foreground IP (as distinguished from background or preexisting IP) but transformed in an AI context.

In both cases, the contracting parties need to have a clear understanding of the contractual terms that govern the use of data provided to the AI tool by end users, or otherwise collected or processed by the AI tool. In an AI deal, however, the inputs into an AI tool, and the data training the AI model in such a tool, continuously refine and improve the model and thereby become inextricably linked.

For that reason, the issues of confidentiality, data rights and restrictions, and IP rights — in both data and improved AI models — are more complex and interrelated.

The analysis and associated risk assessment of these terms needs to be performed carefully on a use-case-by-use-case basis, identifying any inconsistencies and ambiguities in the proposed approach given the AI technology and relevant use case, and considering the value, risks and restrictions associated with each category of data and technology.

Any negotiated changes to the terms impacting these constructs should be traced through the agreement, such that, for example, by obtaining IP rights in a particular AI model improvement, a customer does not lose protection of the warranties that otherwise apply to the AI tool. Or, conversely, by foregoing ownership rights in an improvement to the AI model, a customer does not also grant broader-than-intended rights to the corresponding AI input.

If a customer is not able to secure appropriate contractual protections in a given area relative to the anticipated use cases, technology lawyers may be able to collaborate with technical teams to identify operational mitigation measures.

If these measures are insufficient, any remaining concerns may require narrowly tailored adjustments to the underlying use case, such as limiting the data sets that are exposed to the AI tool.

Rights to AI Output

The allocation of rights to the output of AI models raises issues closely linked to those discussed above for AI input, training data and model improvements.

Customers' contractual rights to AI output are often limited or, worse, ambiguous, which is particularly problematic given the uncertainty of IP protection that may accrue to the AI output under existing IP laws. The starting point should be to resolve any ambiguity on this important point and consider whether the express allocation of the ownership or use rights and any corresponding limitations are appropriate for the relevant use case.

There is also a risk of third-party challenges to the customer's negotiated rights to AI output, in part because AI output is often based on or derived from vast data sets obtained from a variety of sources — including publicly available data or data of other users of the AI tool — and therefore subject to a variety of use restrictions.

To assess the risk of these potential claims, you would need to conduct relatively extensive due diligence on relevant AI technology, such as: (1) the manner in which the applicable AI model was trained; (2) the data absorbed by the trained AI model; (3) the sources of such data; and (4) the confidential nature of such data and other restrictions on its use.

From the customer's perspective, it is important that these diligence disclosures be properly reflected in the relevant contract as representations, warranties and covenants, including in connection with a noninfringement warranty described in more detail below.

The AI Noninfringement Warranty

Based on extensive IP challenges and related litigation,[5] the noninfringement warranty is a key and often difficult issue in a deal involving AI, with coverage of AI models and their improvements, and AI output at the top of the list of concerns, together with the allocation of responsibilities for defense and indemnification of infringement claims.

Customers should seek to negotiate targeted provisions to address this important topic, with a particular focus on potential claims by third parties relating to the use of their content or other data to train the model, or the AI model or its improvement.

Thorough due diligence or, if and when available, trustworthy third-party certifications of compliance with third-party consents, licenses and other restrictions in the use of training data and other pertinent aspects of development and monitoring of the underlying model, will also help businesses assess the likelihood of adverse claims.

In addition to these measures, given the current landscape of IP challenges and related litigation, users of AI technology should consider supplementing any contractual protections relating to AI output with infringement searches — mirroring any existing processes for IP reviews in connection with creation and use of new data or materials — and potentially corresponding allocation of costs of these searches with the provider.

The AI Performance Warranty

In an AI context, an ordinary performance warranty that the AI tool complies with documentation may present a major challenge because: (1) some AI models, by their nature, are constantly evolving based on continuous training; and (2) the requirements for an AI solution may, depending on the industry and relevant use cases, be grounded in one or more of the existing frameworks and standards, such as those based on the concepts of responsible AI,[6] or other similar businesswide standards and governance processes that your organization may adopt for AI technology.

Rather than relying on existing documentation, a technology lawyer should collaborate with the relevant stakeholders to identify a clear list of parameters by which the parties will measure whether the AI tool or technology meets a contractual standard. To do so, you may consider setting a quantitative target or functional requirement for the AI tool or the output that it generates.

For example, performance warranties can be based on availability, i.e. uptime, or predictive power of the AI tool, a specified percentage in the accuracy, precision, or consistency of the answers, or an increased speed of response to customer questions.

With respect to accuracy and precision of AI output in particular, while a performance warranty is helpful, it may be prudent for an organization to implement a separate verification process or supplement the AI tool with a separate accuracy-checking solution.

As your organization establishes and advances AI governance efforts, including by implementing the requirements of trusted AI legal frameworks, AI agreements should take into account developed standards and policies.

Trusted AI Legal Frameworks and Compliance With Laws

The simplicity of an ordinary course of compliance with laws representation and its related indemnity belies the complexity of regulatory changes in a growing number of jurisdictions.

Key among them are trusted AI legal frameworks emerging in the leading proposed regulations, including the AI Act in the European Union,[7][8] the White House's Blueprint for an AI Bill of Rights[9] and the National Institute of Standards and Technology's Artificial Intelligence Risk Management Framework in the U.S.,[10] the U.K. Information Commissioner's Office Guidance on AI and Data Protection,[11] and China's Draft Measures for the Management of Generative Artificial Intelligence Services.[12]

Perhaps surprising in their consistency, these emerging frameworks tend to be modeled after the EU's AI Act, contemplating a risk-based approach for regulating AI, with compliance requirements driven largely by categorization of each AI use case into one of four established categories — prohibited, high-risk, medium-risk or low-risk — with high-risk use cases triggering the most extensive reviews and safeguards.

Beyond the AI-specific laws and legal frameworks, the principles remain that: (1) responsibility for compliance with laws should be allocated to the party that is in the best position to control the relevant area and defend the claim and (2) the use of AI or dependence on a third-party AI provider to satisfy legal requirements does not change these underlying legal requirements.

But for a variety of reasons — key among them uncertainty and relative leverage of the parties — contractual solutions to the allocation of responsibility for compliance with laws in the AI space vary significantly and must be considered on a case-by-case basis.

It would not be surprising if, in the near future, contractual responsibility for compliance with AI laws were carved out and addressed separately from the general compliance with laws warranty — similar to the approach to data protection laws — in part based on the need to address regulatory requirements with specificity in the contract, and to supplement them with ongoing operational reviews that may be more extensive than what has been "operationalized" in connection with data protection laws.

Conclusion

From business seminars to boardrooms, deal makers are evaluating the ways in which AI can streamline mission-critical processes and generate value for companies. In parallel, businesses are racing to develop internal buffer policies governing the use of AI.

As companies leverage AI tools, technology lawyers and their clients must be aware of the impact of AI

on technology deals, and develop plans for its use that include both contractual and operational safeguards.

Ultimately, clients will benefit from changes to traditional deal terms and novel contractual clauses drafted for new, AI-specific considerations.

Marina Aronchik is a partner and Samuel Hartman is an associate at Mayer Brown LLP.

[1] Kevin Roose, The Brilliance and Weirdness of ChatGPT, N.Y. Times, December 5, 2022, at https://www.nytimes.com/2022/12/05/technology/chatgpt-ai-twitter.html.

[2] Nico Grant and Cade Metz, Google Releases Bard, Its Competitor in the Race to Create A.I. Chatbots, N.Y. Times, March 21, 2023, at https://www.nytimes.com/2023/03/21/technology/google-bard-chatbot.html.

[3] Jordan Novet, Microsoft's $13 Billion Bet on OpenAI Carries Huge Potential Along with Plenty of Uncertainty, CNBC.com (April 9, 2023 at 10:40 PM EDT), https://www.cnbc.com/2023/04/08/microsofts-complex-bet-on-openai-brings-potential-and-uncertainty.html.

[4] Jordan Novet, AWS Is Investing $100 Million in Generative A.I. Center in Race to Keep Up with Microsoft and Google, CNBC.com (June 22, 2023 at 6:33 PM EDT), https://www.cnbc.com/2023/06/22/aws-invests-100-million-in-generative-ai-as-it-sees-a-long-race-ahead.html.

[5] Richard Assmus and Emily Nash, Generative Artificial Intelligence and Intellectual Property, (2023).

[6] Ayesha Gulley, Why We Need to Care About Responsible AI in the Age of the Algorithm, World Economic Forum (March 22, 2023), https://www.weforum.org/agenda/2023/03/why-businesses-should-commit-to-responsible-ai/.

[7] Draft of the European Commission's proposed AI Act (May 11, 2023) at https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence.

[8] Ana Bruder, Oliver Yaros, and Ondrej Hajda, Developments from Europe: New Laws Regulating Artificial Intelligence, Data and Digital Operational Resilience (2023).

[9] Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People, The White House (October 2022) at https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf.

[10] Artificial Intelligence Risk Management Framework, US Department of Commerce, National Institute of Standards and Technology (January 2023)

at https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

[11] Guidance on AI and Data Protection, Information Commissioner's Office (March 15, 2023) at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/.

[12] Measures for the Management of Generative Artificial Intelligence Services (Draft for Comment), Cyberspace Administration of China (April 12, 2023) at https://digichina.stanford.edu/work/translation-measures-for-the-management-of-generative-artificial-intelligence-services-draft-for-comment-april-2023/.