Artificial Intelligence: A Transactional Guide to the Perplexed

Harry Rubin and Michelle Park, Kramer Levin

Bloomberg Law

Transactional Guide to AI

Contributed by Harry Rubin and Michelle Park, Kramer Levin

Before the expected self-improving, self-perfecting and, ultimately, self-perpetuating AI eliminates lesser life forms, such as lawyers, we hasten to proffer a practical legal approach to AI for technology transactions and acquisitions. AI requires legal and technological context-driven and customized diligence queries and representations and warranties (RW).

AI is rapidly becoming ubiquitous, dominating the headlines and exponentially impacting technology, business, public policy and law as few would have predicted. The US Patent and Trademark Office (USPTO) has requested public comments on ensuring the ongoing encouragement and incentivization of AI innovation. Its recent analysis found that 80,000 of utility patent applications in 2020 involved AI, which is 150% higher than in 2002. AI now appears in 18% of all utility patent applications. Remarkably, this is more than 50% of all the technologies examined at the USPTO.

Much of what is now labeled AI is not necessarily AI. To qualify as AI today, the general consensus is that technology must exhibit some level of adaptable self-learning and improving. The boundaries of AI will shift as technology evolves. Machine Learning (ML) algorithms in AI allow computers to learn by training on data inputs, including to recognize patterns and make predictions. ML uses artificial neural networks (ANN), mimicking the neural networks in the human brain, to process data with limited or no human intervention. ANN consists of three layers of input: initial data, hidden (where the computation occurs) and output (the results generated by inputs).

Legal Context

ML AI technologies and platforms, such as ChatGPT and Midjourney, raise novel legal issues, especially concerning copyrights, patents, liability, and privacy. Governmental bodies in the EU and US are grappling with the momentous public policy implication of AI, contemplating groundbreaking responsive AI regulations and controls.

Intellectual Property

Generative ML technologies train on big data—e.g., text, audio, images, software codes and videos—scraped from the internet, frequently without permission from their copyright owners. As copyright owners allege infringement, defendants are expected to use fair use defenses—that the nature of outputs are transformative uses that do not compete with the copyrighted works. Several lawsuits are ongoing. See, e.g., *Getty Images (US), Inc. v. Stability AI, Inc.* No. 1:23-CV-00135 (D. Del. Feb. 3, 2023); *J. Doe 1 v. GitHub, Inc.*, No. 4:22-CV-06823 (N.D. Cal. Nov. 3, 2022); and *Andersen, v. Stability AI Ltd.*, No. 3:2023-CV-00201 (N.D. Cal. Jan. 13, 2023).

In the US, copyright protection can only be granted to a human being, not a machine. Copyright protection is possible for machine generated work, but requires substantial human contribution. The US Copyright Office issued guidance on protection for Works Containing Material Generated by Artificial Intelligence. The key criterion for US copyright protection is whether the work is one of human authorship, with the computer merely being an assisting instrument, or whether the traditional elements of authorship in the work—literary, artistic, or musical expression or elements of selection, arrangement, etc.—were actually conceived and executed not by human, but by machine. Notably, human authorship is not required for copyright protection in many other countries, including U.K., Ireland, Hong Kong, India, New Zealand, and South Africa, all of which may grant copyright protection for computer generated work, thereby requiring careful proactive legal counsel, setting the stage for forum shopping and a conflicts-of-law imbroglio.

Whether the AI technology company or the user owns the content or prompt inputted into the AI machine in order to generate outputs is an equally pivotal controversial issue. Significantly, contractual terms now assume a decisive role in the identification and mitigation of AI legal risk and liability and AI input and output ownership allocation. The terms of use for many generative AI technologies to date, such as ChatGPT and Midjourney, elaborately protect the AI technology company with provisions disclaiming all warranties, liabilities, and indemnities.

Plaintiff copyright owners typically assert that AI outputs are derivative works of their contents used as training data. In response, some defendants assert that plaintiffs failed to identify specific copied works. Since AI technologies ingest colossal amounts of training data, plaintiffs may struggle to identify the allegedly infringing works. Notably, however, some AI platforms, such as ChatGPT, expressly assign and convey output ownership to the user, thereby dramatically increasing their commercial appeal to users. Interestingly, the EU's proposed AI Act indicates that the creators of generative AI technologies may need to disclose the copyrighted materials used to train their AI technologies. Such disclosure requirement may provide copyright holders an opportunity to receive portions of the work's profits.

Liability for Harm

A major consideration, which will ultimately dramatically impact the commercial, use, and adoption potential of AI, is who bears the liability for harm caused by AI products or services. In the recent Supreme Court case *Twitter v. Taamneh*, the unanimous decision favored defendants Twitter, Google and Facebook, stating that the failure of the defendants to remove ISIS content from their platforms is not the same as intentionally providing substantial aid to ISIS under the Antiterrorism Act. *Twitter, Inc. v. Taamneh*, 143 S. Ct. 1206 (2023).

As a result, another terrorism liability case against Google based on Section 230 of the Communications Decency Act of 1996, which generally shields technology companies from liability for content published by users, was remanded by the Supreme Court indicating that the plaintiff's liability claims against Google are unlikely to survive. *Gonzalez v. Google LLC*, No. 21-1333., 2023 BL 169686, (U.S. May 18, 2023). However, the court acknowledged the challenges of applying Section 230 to today's internet landscape of highly complex algorithms.

The extent of liability of generative AI platform outputs are yet to be determined. Cases will likely turn the level of control, involvement and direction of the AI company and the actions and the responsibility of the users.

AI-enabled medical devices also raise new questions on the applicability of traditional tort theories, such as negligence, product liability, and strict liability, and whether AI/ML-based medical software would be litigated under medical malpractice or products liability. We can expect product liability to apply to developers and manufacturers across the AI distribution chain, and medical malpractice and other negligence liabilities to apply to health care providers from deviating from their standard of patient care. The standard applicable to AI-enabled medical devices will have to be developed over time.

Privacy

Privacy, civil rights, and algorithm bias are other major AI concerns. The White House published the Blueprint for an AI Bill of Rights to guide the design, use, and deployment of automated systems to protect the public from AI algorithm discrimination, abusive data practices that intrude on privacy, and inappropriate or irrelevant data use that can lead to harm.

The currently stalled federal American Data Protection and Privacy Act (ADPPA) provides rules on use of personal data. If passed, it would require covered entities and service providers to conduct algorithm design evaluations and impact assessments describing the algorithm's design, process, purpose, foreseeable uses, data inputs, and the outputs the algorithms generate. While the ADPPA is on pause, many states are pursuing, and some have passed, legislation relating to AI use and algorithm discrimination.

The EU's proposed AI Act also covers bans on intrusive and discriminatory uses of AI, such as predictive policing systems based on profiling and biometric surveillance. Other jurisdictions, such as Brazil and China, are working on their own bills to regulate AI.

Supplemental AI Due Diligence Checklist

Editor's Note: This supplemental M&A due diligence checklist proffers a list of due diligence requests designed to assist in assessing a target company's use of artificial intelligence (AI). These supplemental requests may be merged into a standard M&A due diligence checklist or may be used as a separate document.

Note that some requests may not be appropriate for all transactions; e.g., certain requests may only apply to a public company or private company, and certain equity and property documents may not be relevant in an asset purchase. Furthermore, these requests may be tailored to the specific transaction, including tightening or broadening the scope of the requests, to address the transaction's particular due diligence needs. In some instances, it may be useful to limit the scope of certain due diligence requests using lookback periods—e.g., "within the last five years"—or materiality standards, as appropriate.

For more information, see Overview - Transactional Guide to AI and Sample Clauses: Representations & Warranties – AI in Transactions.

Contributed by Harry Rubin and Michelle Park, Kramer Levin

[Subsection #]. Artificial Intelligence (AI) Concerns

Requested Item	Provided [or Public Filing Identified]	N/A	Comments
1. Identify any AI technology (including generative AI) used by the target company in any form or for any purpose.	☐	☐	
2. A list of any AI licenses or authorizations provided to, or obtained by, the target company and the terms under which such licenses were provided to or obtained by the target company. (a) For each of the licenses, describe how and for what purposes the AI is used, whether (i) internally or (ii) to generate outputs which are provided to or used by clients or other recipients.	☐	☐	
3. Describe the nature of the ownership (e.g., intellectual property) or identify the owner of the AI technology, inputs and outputs provided to the target company by a third-party provider. (a) Identify any contractual terms governing the ownership of the AI technology (if any), inputs or outputs.	☐	☐	
4. Describe the nature of the ownership and/or identify the owner of the AI outputs provided to clients or other recipients by the target company.	☐	☐	
5. Copies of the target company or AI provider's contracts, agreements and terms and conditions regarding the ownership of the information inputted into the AI technology by the target company's	☐	☐	

clients/users and the content generated by the AI technology in response to those inputs.			
6. Identify any AI technology that the target company develops, such as machine learning, deep learning or any others that may reasonably be considered as AI technology. (b) List and describe how each of these AI technology types work.	☐	☐	
7. Describe any type of data/information (content) used by the target company to train AI technology (i.e., training data). (a) A list of the sources of the training data	☐	☐	
8. A list of any licenses obtained from owners of the training data used by the target company to train AI technology.	☐	☐	
9. Describe how the target company obtains the training data, whether through lawful web scraping or otherwise. (a) Copies of any applicable web terms and conditions that are reviewed to ensure compliance.	☐	☐	
10. Copies of, and information on, any legal claims, suits, judgements, threats, fines or penalties against the target company for the unauthorized use of training data, violation of applicable laws, judgements or legal claims or suits arising from or relating to the company's use of AI.	☐	☐	
11. A list of any laws, rules, regulations and judicial decisions that apply to the target company's collection, use and processing of training data. (a) Describe how the target company ensures compliance with said laws, rules and regulations.	☐	☐	
12. Describe any known instances of past or ongoing unauthorized use of or access to the target company's AI.	☐	☐	
13. Describe any known or suspected violations of applicable laws and regulations by the use of the company's AI.	☐	☐	
14. Describe the material performance of the target company's AI as compared to its specifications and intended purpose.	☐	☐	

(a) Identify any material errors, defects, failures, or interruptions in the AI.			
15. A list of any commercially reasonable and industry conforming security safeguards and controls used by the target company, including proper access controls for the AI.	☐	☐	
16. Copies of any commercially reasonable insurance coverage held by the target company for claims or losses pertaining to AI.	☐	☐	
17. Describe and provide evidence of any steps taken by the target company to detect and remediate algorithm biases.	☐	☐	

Sample Clauses: Representations & Warranties - AI in Transactions (Annotated)

Editor's Note: Representations and warranties within an agreement are intended to mitigate risks. For any agreements governing transactions, such as M&A, asset acquisitions, JV's, collaborations and licensing and any others, involving artificial intelligence (AI), representations and warranties (RW) should be carefully drafted following a thorough due diligence assessment of the target AI where the due diligence assessment should identify the AI technologies and the relevant legal and contractual relationships.

RW's must be informed by and build upon the diligence exercise. RWs are designed to "smoke out" problems and identify the AI technologies and legal and contractual relationships pertinent to the target AI. Therefore, the scheduling contemplated by the RWs below is of particular importance—not just legally— but also for valuable business and technology information gathering.

The extent and granularity of the RW's should be proportionate to the particular risks arising from the transaction involving the target AI. If a transaction does not involve AI and a party wishes to ensure that the counterparty has not and will not use AI, the sample RW's prohibiting a counterparty's use of AI set forth below may be used.

For more information on how to carry out due diligence on AI in commercial transactions, see Overview - Transactional Guide to AI and Checklist - AI Due Diligence.

Contributed by Harry Rubin and Michelle Park, Kramer Levin

Sample Contractual Representations & Warranties

Definitions:

> **Comment:** Defining each of the terms used in the RW's of an agreement mitigates risks by adding certainty and reducing ambiguity. Furthermore, it is advisable to incorporate the defined term "AI" as part of the definition of "Intellectual Property." Reference to the word "Company" throughout this document refers to the counterparty.

"AI" collectively means the AI Inputs, AI Outputs and AI Technology.

"AI Inputs" means any and all of the following generated by or derived from AI Technology which are, in whole or in part, used or relied upon, or licensed, sold, otherwise provided or accessed, by or to the Company, including but not limited to, data, writings, works of authorship, graphics, pictures, recordings, any electronic or other information, text or numerals, audio or visual content, or materials of any nature or description.

"AI Outputs" means any and all services, products, data, writings, works of authorship, graphics, pictures, recordings, any electronic or other information, text or numerals, audio or visual content, or materials of any nature or description generated or derived by or on behalf of the Company, from any AI Technology or AI Inputs, where such outputs are licensed, sold, provided to, or otherwise made available or accessible by the Company to any third party.

"AI Technology" means any and all training, self-improving or machine learning software, algorithms, hardware or other artificial intelligence tools or aids of any kind.

Restricting a Counterparty's Use of AI

> **Comment:** A party seeking to ascertain that the counterparty has not and will not use any AI should insert the following language into the agreement:

The Company does not and will not access, procure, obtain, generate, use or rely on any AI, and the Company warrants that its products and services do not incorporate, are not based upon, nor derived from, any AI.

Representations & Warranties Related to AI

Reference to Schedule(s):

> ***Comment:*** The agreement should contain a schedule which stipulates at a minimum all AI relevant to the transaction, their owner(s), licensee(s), recipients and the agreements pursuant to which the Company uses or offers the AI and the following language may be inserted into the agreement to reference the schedule:

The parties acknowledge that Schedule [____] sets forth all (a) AI Technologies, the owners thereof, and the agreements pursuant to which Company obtains or accesses such AI Technologies; (b) AI Inputs, the owners thereof, and the agreements pursuant to which Company obtains or accesses such AI Inputs; and (c) Company AI Outputs, the recipients thereof, agreements pursuant to which each such recipient obtains or accesses the AI Outputs, and the means by which the AI Outputs have been provided to such recipient, including whether by remote access, SaaS or on premises.

General Representations & Warranties:

> ***Comment:*** The following sample clauses relating to the Company's use of AI may be incorporated into the general RW clause or incorporated into the relevant clauses within the appropriate transaction agreement—e.g., clause relating to intellectual property or technology—including mergers, asset acquisitions, collaborations, JV's, or licensing.

The Company hereby represents and warrants that:

(i)   the Company is not and will not be subject to any obligations that conflict with any terms contained herein which govern the Company's use of AI Inputs or AI Technology or its AI Outputs;

(ii)   the Company owns or possesses all legally requisite rights and licenses to use the AI Technology and AI Inputs and to generate the AI Outputs, all as currently used and generated AI Outputs in its business and reasonably anticipated to be used and generated post-closing;

(iii)   the Company's current and contemplated use of the AI, does not, and will not, infringe upon or violate any intellectual property rights, rights of likeness or publicity, or any other third-party right of any kind;

(iv)   the Company's use of AI complies with all laws and regulations (including those pertaining to data privacy and security, and financial or health care regulations) as applicable to the Company;

(v)   the Company's use of AI and generation of AI Outputs conform to prevalent industry standards and practices;

(vi)   the contemplated transaction will not adversely affect the Company's rights in or use of any AI, and the Company will be able to use the AI to the same extent prior to the effective date of the agreement as it has prior to the agreement.

Representations & Warranties Relating to Insurance:

> ***Comment:*** By requiring a counterparty to represent that it maintains insurance coverage in connection with the target AI at the time of the signing of the agreement, a party may be able to mitigate risks arising in connection with any disputes, judgments, fines or any other contentious matters relating to the AI. The following clause may be inserted into the agreement to mitigate risks concerning insurance coverage for AI:

The Company maintains and shall continue to maintain commercially reasonable insurance coverage for claims or losses pertaining to the AI. The Company warrants that the AI has not been subject to any claims, suits, demands, rulings, judgements, threats, fines, penalties, or a cease and desist letter asserted against, or brought by, the Company pertaining to intellectual property or any other rights violation or breach of any applicable law, rule or regulation.

Representations & Warranties Relating to Security:

> ***Comment:*** The following representations may be inserted as sub-clauses within the general representations and warranties clause of the agreement or as sub-clauses within any clause of the agreement relating to IT security. Clause (i) is designed to mitigate risk of the acquirer or licensee from any failures of the AI to adhere to its intended purpose and Clause (ii) is drafted to require the Company to maintain industry-standard security safeguards.

(i)   The Company hereby warrants and represents that there have been no material errors, defects, failures or interruptions in the AI or in the performance of its intended purpose, and the AI has materially performed in accordance with its specifications and intended purpose.

(ii)   The Company maintains and shall continue to maintain, if the deal so contemplates commercially reasonable and industry standard conforming security safeguards and controls, including proper access controls for the AI. There has been no unauthorized use of or access to AI and, to the best of Company's knowledge, no AI has been used in violation of any applicable laws and regulations.