MAYER | BROWN
孖士打

Protecting Artificial Intelligence

Intellectual Property and Contractual Provisions

Brian W. Nolan
Partner
+1 212 506 2517
bnolan@mayerbrown.com

Allison M. Aviki
Partner
+1 212 506 2310
aaviki@mayerbrown.com

Lori Recker
Head of Global Business Operations
Aetion, Inc.
lori.recker@aetion.com

May 2023

What Is Artificial Intelligence?

- The “ability of computers to emulate human thoughts and perform tasks in real-world environments”
- Types of Artificial Intelligence (AI)
  - **Machine Learning (ML) is a subset of AI** that refers to the technologies and algorithms that allow a machine to identify patterns, make decisions, and improve based upon experience and data
  - **Deep Learning is a type of ML based on artificial neural networks** in which multiple layers of processing are used to extract progressively higher levels of features from data
  - **Neural Network** is modeled on the human brain and uses multiple interconnected nodes and a layered structure

The Components of AI to Consider Protecting

- Algorithms – codes and rules by which the AI operates
- Model – output of the ML algorithm based upon training data that includes the rules, numbers, and other algorithm-specific data structures
- Datasets
  - Training – data initially used to train the model
  - Validation – data that helps identify problems with the model
  - Test – unknown to the model and used to test the accuracy of the model
- Results – output of a model

Potential Protection Schemes for AI

- Patents
- Copyrights
- Trade Secrets
- Contracts

What AI Components Can Patents Protect and against What?

- Algorithms, models, and data structures
  - Potentially patentable if application transforms the device by enabling improvements in the process or the function of the computer
- Results
  - For certain results, e.g., new composition, device, method, or process, patenting may offer the strongest protection
- Protects the use of patented AI components by any third party

The Problems that AI Presents When Considering Inventorship

- U.S.A., U.K., Australia and EPO have held that AI cannot be listed as an inventor. South Africa and Saudi Arabia allowed AI as an inventor
  - *Thaler v. Vidal*, 43 F.4th 1207, 1210 (Fed. Cir. 2022) ("Here, there is no ambiguity: the Patent Act requires that inventors must be natural persons; that is, human beings"). Petition for *certiorari* denied April 24, 2023
- Ambiguity – what happens when AI makes a contribution that, if made by a human, would amount to joint inventorship?
  - USPTO request for comment published 2/14/23 (Question 3); *Thaler*, 43 F.4th at 1213

Determining AI Inventorship

- Consensus that AI cannot conceive of an invention just yet, so at most it can contribute to an invention, i.e., human involvement required
- Important to track contributions to development of algorithms and datasets to identify potential inventors
  - Contribution to AI components coupled with nexus to the drafted claims should support inventorship claim
  - Provided that a good faith effort is made to determine inventorship, then any incorrect inventorship will not affect patent validity

Issues that Arise When Determining Inventorship for AI

- Application of AI often requires expertise in different technical areas that do not reside within the same field
  - Result is that different entities often contribute to AI—potential for joint inventorship across unrelated entities
  - Joint inventors have equal rights to exploit the patent through use and licensing
- Missing inventor may request correction of inventorship under 35 U.S.C. § 256(b)
  - *Dana-Farber Cancer Institute, Inc. v. Ono Pharmaceutical Co., Ltd.*, 964 F.3d 1365, 1374 (Federal Circuit 2020)

The First Hurdle Is Showing Patent-Eligible Subject Matter

- Patents to algorithms or implementations of a process through a computer may be unpatentable as an abstract idea
- To avoid a finding of patent ineligible subject matter, focus on transformative aspect of AI, e.g.,
  - Improves computer functionality. *Enfish, LLC v. Microsoft*, 822 F.3d 1327, 1336 (Fed. Cir. 2016)
  - Improves the process in a specific application. *Thales Visionix, Inc. v. U.S.*, 850 F.3d 1343, 1348-1349 (Fed. Cir. 2017)
  - Claims limited to specific rules to create a desired result. *McRO, Inc. v. Bandai Namco Games America Inc.*, 837 F.3d 1299, 1315 (Fed. Cir. 2016)

Ambiguity in How Model Operates Makes Drafting Claims Difficult

- Difficult to comply with definiteness requirement
  - Insufficient details about algorithms may result in a conclusion that the claims do meet the definiteness requirement. See, e.g., *Rain Computing, Inc. v. Samsung Electronics America, Inc.*, 989 F.3d 1002, 1007-1008 (Fed. Cir. 2021)
- Difficult to draft claims that comply with patentability requirements while being sufficiently broad to identify potential infringers easily
  - A competitor is unlikely to describe its implementation of AI so claims with detailed limitations will be difficult to map on competitor’s AI

Uncertainty About the Model Could Make It Difficult to Comply with Patent Requirements

- Algorithms and results are known, but how the model developed by AI is operating to provide results may not be well understood
- Written Description & Enablement Requirements Hurdles
  - Ambiguity may present a difficulty in showing possession of and enabling claims directed towards the application of a trained machine learning model
  - Claiming by function achieved presents difficulty in showing sufficient examples representative of the ways to achieve the function
  - Important to include detailed description of human involvement, algorithms, training data, training procedure, model architecture, model results, data correlations, system integration of the model, and examples

AI Will Likely Disrupt the Traditional Obviousness Framework

- How to integrate the capabilities of AI into the concept of a person of ordinary skill in the art?
  - While we assume POSITA has available all relevant prior art, AI can access and understand all prior art across a broader field
- Does AI need a motivation to combine when it has the capabilities of considering all combinations?
  - Abilities of AI may make the concept of teaching away irrelevant because AI can look at all combinations
  - AI does not need a reasonable expectation of success because it may be able to predict the expected result

What AI Components Can Copyright Protect and against What?

- USCO recently launched its “AI Initiative”
  - New guidance on copyrightability and registration issued last month
  - Cancellation Decision re: Zarya of the Dawn (Feb. 21, 2023)
- Courts will be weighing in
  - *Thaler v. Perlmutter*, 1:22-cv-01564 (D.D.C.)

When Copyright May Be the Best Choice

- Instances where the company must disseminate work externally, particularly where there is high potential for reverse engineering
- Works with "sufficient human authorship," e.g.,
  - Inputs: prompts
  - Outputs: Human compilation or modification of AI-generated material
- Disclosure is the watchword

What AI Components Can Trade Secrets Protect and against What?

- Each component can be protected provided the following:
  - The company makes reasonable efforts to keep the information secret
  - The information derives independent economic value from not being generally known
- May offer best method of protection for the components individually
  - Algorithm by itself likely only protectable as a trade secret
  - Unique collection of data probably best protected by trade secrets
- Prevents the use of the components by any third party that obtains the information by improper means

Should a Company Rely upon Trade Secrets Over Patents?

Benefits	**Detractions**
• Trade secrets avoid the barriers of patent protection	• Do not provide a monopoly against all competitors
• Trade secret's immediacy helpful in rapidly developing technology	• Independent development and reverse engineering defenses
• Unlimited term provided secrecy remains	• May be difficult to detect trade secret misappropriation

Recent Software Trade Secret Damage Awards Show the Value of Trade Secret Protection

- Appian Corp. awarded $2.04 billion against Pegasystems Inc. in Virginia state court action
- Epic Systems Corp. awarded $940 million against Tata Consultancy by Wisconsin court based upon “avoided cost” damages theory
  - Judge reduced to award $420 million and appellate court affirmed award of $280 million
- Versata Software awarded $104 million against Ford Motor Co. by Michigan district court
  - Judge overturned jury’s trade secret damage award as speculation

Important to Implement Protocols that Ensure Confidentiality

- Internal education and policies regarding nature, importance, and treatment of IP
- Employee turnover may present issues
  - Federal actions show disfavor of non-compete agreements, so key will be non-disclosure and invention assignment agreements. This is especially true for global companies with employees outside the U.S. (where non-competes may be even less favored or enforceable).
- Algorithms and source code are easily transferable
  - Must police access, prevent copying to portable drives, implement strong cybersecurity policies and data loss prevention (DLP) mechanisms
  - Open-source policy and procedure for use, perhaps third-party monitoring of use
- Detailed contracts necessary for collaboration and oversight for compliance of collaborator with contractual obligations
  - Require collaborator use company equipment and conduct any work for the collaboration inside company systems (to ensure adequate protection, monitoring, DLP, etc.)
  - Otherwise ensure that algorithms and code don’t leave the company’s secure environment

What AI Components Can Contracts Protect and against What?

- All components of AI
- Protection limited to the parties to the contract and any subsidiaries or third parties included in the protections
- Discuss questions of ownership and use rights for algorithms, datasets, and models; clearly and fully outline this in the contract

Take the Time to Understand All the Inputs and Outputs Before Drafting Terms

- Is this a service provider model, or more collaborative venture?

Service Provider Model

- How is AI used by the service provider?
- What are the service provider's intentions regarding how customers use their product?
  - What is the service provider pricing model in connection with use of AI?
- How does the customer intend to use the service provider product?
- Are there any third-party rights involved with the AI components, e.g., rights in training data?
- What rights will the customer require to accomplish its objectives?
- What rights will each party have in the components of the AI at the conclusion of the transaction?

Collaboration

- What are the ultimate objectives of the collaboration? And how will AI be used by the parties to obtain them?
- What components of AI will each party bring to the transaction?
- Are there any third-party rights involved with the AI components, e.g., rights in training data?
- How will the parties deal with the dataset if a party expands dataset by adding proprietary data?
- How will parties share potential liabilities, e.g., personal information in datasets, potential bias in datasets?
- What rights will each need to complete its tasks during the transaction?
- What rights will each party have in the components of the AI at the conclusion of the transaction?

What Rights Will the Parties Have in the Algorithm and Trained Model?

- Ownership of algorithms likely to stay with party supplying algorithm
- Trained model is a result of the algorithms along with the datasets and use cases experienced during training
  - Contract provisions key to defining rights
    - Field-of-use limitations – what can it be used for?
    - Permitted use and/or limitations on use – how can it be used?
    - Ability to use with or license to other parties
    - Governance requirements around how it is used to ensure contract compliance
    - Audit rights to allow parties to understand whether the parties are complying with the agreement
    - Obligations to provide updates to AI as model continues to develop after implementation

What Rights Will the Parties Have in the Datasets?

Protective contracts clearly address in detail:

- Which entity owns the input data and the output data
- Ownership issues for improvements or changes to the dataset over the life of the project
- Ownership questions regarding derivatives of the dataset
- How the parties will treat intellectual property in outputs generated by multiple inputs (with different input ownership)

Disclaimer

- These materials are provided by Mayer Brown and Aetion, Inc. and reflect information as of the date of presentation.
- The contents are intended to provide a general guide to the subject matter only and should not be treated as a substitute for specific advice concerning individual situations.
- You may not copy or modify the materials or use them for any purpose without our express prior written permission.

Americas | Asia | Europe | Middle East

mayerbrown.com