

## Cos. Should Assess IP, Contractual Protections For Their AI

By **Lori Bennett, Brian Nolan and Allison Aviki** (June 16, 2020, 5:44 PM EDT)

The global COVID-19 pandemic has catalyzed our expectation that machine learning can unlock solutions today that otherwise would have remained available only in the distant future.

But artificial intelligence presents a confounding area for companies today: Often there can appear to be equal parts recognition of AI's growing importance alongside complete lack of visibility into what AI actually is and does within an organization.

One point that has drawn wide consensus is that AI is not something simply running in the background. Increasingly, it is at the forefront of development and central to intellectual property transactions and litigation alike. Yet in an acute way, the law is in peril of lagging far behind when it comes to AI.

This article addresses the various types of IP protection available to safeguard proprietary AI and lays out pros and cons for each, as well as tools for creating protections when statutory means fall short. It concludes with practical points and questions to focus client inquiries and achieve near-term and future goals.

### **Know what the client has.**

As a lawyer, whether in house or external, understanding the business operations and objectives of the client is always a best practice for providing effective counsel. When a client interacts with AI, such understanding becomes critical for developing the proper legal protections.

The presence and use of AI might be obvious or core to the client's operations, it might play a supporting role through internal processes, or it could be tangential in the way it interacts with software, hardware, data or other IP owned by third-party licensors. Identifying what needs protection and where the risks and potential liabilities hide requires an in-depth understanding of the client's technology and processes.

Specifically, successful counsel regarding AI requires close alignment with the engineering and product teams who understand at a technical level what the client's product contains or how it interacts with AI



Lori Bennett



Brian Nolan



Allison Aviki

through a full life cycle.

If AI is essential to the client's product, it also requires thorough understanding of what customers value when they purchase the product and how they expect to derive a return on investment. This can only come from regular and in-depth conversation with the business and customer engagement teams who have the most direct relationship with how the product is used, and desired to be used, in the market.

Armed with a complete understanding of a client's AI universe, the next challenge is building out the rest of the picture: how does this AI interact with other potentially proprietary information or material? AI by nature seeks to evolve, so what happens to the client's proprietary rights, and those of its transaction partners, as this happens?

### **Figure out what the client needs.**

The value of AI resides in different components associated with a client's product. These components include datasets, algorithms, models, hardware systems and results. Each requires consideration of the type of IP that will provide the best protection for that component.

Further complicating the selection of IP protection is whether the client's asset resides in the AI or the results it produces. Early in AI development, stakeholders should assess the benefits associated with patents, trade secrets, copyrights, contracts and open source to determine which will best position the client to maximize the value associated with each AI component.

### **Patent**

Patents offer a well-established means of protecting an asset. The familiarity with patents may allow a client to use the issuance of a patent to tout its AI and pursue investments or partners. The value associated with a patent flows from the owner's ability to exclude others from practicing the technology for a defined period of time. But the time it takes to obtain a patent may reduce its value to AI. AI may have moved on before a patent issues.

A decision to use patents as a means of protecting AI requires consideration of multiple facets of patent law. It starts with a basic question: Who is the inventor when AI generates aspects of an invention? Both the U.S. Patent and Trademark Office[1] and the European Patent Office[2] have held that an AI system cannot be named as an inventor on a patent application — inventors are limited to humans. So from the outset, a client should track contributions to the AI to provide a mechanism for identifying the inventors.

A decision as to whether patents offer the best form of protection for AI requires consideration of its individual components. Certain components such as algorithms or databases may not qualify as patent-eligible subject matter under Title 35 of the U.S. Code, Section 101. Patent protection may be more appropriate for AI systems or the results produced by AI, e.g., a new chemical compound or method of using existing compounds.

Other considerations include the ever-changing nature of AI. To properly describe and enable an invention, a patent specification may need to provide the algorithms, relationships or models the AI uses. If the AI continues to develop or modify the algorithms used, relationships in the data or model implemented to achieve the end result, the original description may fail to describe or enable the changing AI. Similar issues arise with drafting claims that define the right to exclude.

As AI, the claims as issued may become irrelevant to how the AI operates. The right to exclude others from practicing the claims may diminish in value as the AI develops. The law will continue to develop to deal with these and other issues. For example, what should be considered obvious when AI can review massive amounts of combinations, not just those a person of ordinary skill in the art is motivated to pursue and which have a reasonable expectation of success?

## **Trade Secret**

While patents will continue to be valuable assets protecting aspects of AI such as the systems and results generated by AI, it is uncertain whether patents will protect other components of AI. Trade secrets may offer a way to obtain protection for these components. A trade secret applies to information that derives value from not being publicly known. As long as an entity takes reasonable steps to maintain the confidentiality of the information, the trade secret exists.

A company has a cause of action for misappropriation of trade secret against any person or entity that improperly obtains the information, such as a former employee failing to comply with confidentiality obligations or a new employer failing to take reasonable steps to prevent the disclosure.

The creation of a federal cause of action by the Defend Trade Secrets Act enhances trade secrets as a potential mechanism to protect components of AI. As federal courts have the opportunity to interpret the DTSA, more clarity should develop, which will provide a better understanding of the scope of trade secret protection for AI.

Trade secrets should offer a viable means to protect aspects of AI such as algorithms, datasets and identified relationships. They offer the benefit of immediate protection that exists as long as the information remains confidential.

Drawbacks are that they do not prevent a competitor from using information that it independently develops or reverse engineers from another's product and that trade secrets are more difficult to evaluate and value when considering potential transactions.

Unlike patents or copyrights, the owner of a trade secret is unlikely to disclose its existence or may apply conditions to the disclosure to parties in a transaction. AI companies needing to partner with third parties to effectively implement their AI should consider these limitations before deciding on trade secret protection for AI.

## **Copyright**

Like patent law, copyright law offers well-established asset protection through which companies obtain exclusive rights in exchange for public disclosure. Federal copyright registration offers the added benefit of a comparatively low cost and rapid means of staking a claim. Even so, some similar basic questions arise. While copyright protects original works of authorship under Title 17 of the U.S. Code, Section 102(a), what does authorship mean in the context of AI?

The U.S. Copyright Office articulated this concern early and well in its 1965 annual report:

The crucial question appears to be whether the 'work' is basically one of human authorship, with the computer merely being an assisting instrument, or whether the traditional elements of authorship in the work ... were actually conceived and executed not by man but by a machine.[3]

While recent decision-making abroad points to countries such as China taking a more expansive approach in recognizing copyright protection for AI-generated work, the U.S. Copyright Office stated earlier this year that it will only register original works of authorship created by a human being.[4]

The workhorse power of AI presents another basic question, this one arising under U.S. common law. The merger doctrine instructs that for ideas that can only be expressed in a limited number of ways, ideas and expression merge, such that the expression "cannot be protected, lest one author own the idea itself." [5]

As AI enables fixation of permutations of idea expression at levels previously unimaginable, does that computational output itself shrink the realm of copyrightable expression? Clear answers will only take shape with time.

## **Contract**

When traditional or statutory language for creation and invention fail to fully capture reality, contracts become critical as a means of defining and protecting or leveraging the proprietary elements of an AI product. With respect to AI, laws, regulations and legal precedent, as always, lag behind the speed of invention, pushing lawyers to innovate at the rate of their tech counterparts.

The flexibility of a contract often makes it the best legal tool to accomplish this, allowing for tailored definition and protection of the related proprietary rights, and/or ensuring a client is receiving adequate rights to use AI in the intended way.

First and foremost is to fully understand the applicable AI universe and where a client needs protection or permission. When the client identifies its AI as proprietary, then a contract provides the opportunity not only to detail ownership, but to obtain acknowledgment and agreement by the other party that the client owns what it says it owns.

The contract can and should also describe in detail how the AI may be used or restricted. This could prove critical when the law is not clear or fails to adequately address a proprietary element at all.

From there, contract sections feel relatively traditional: definition of IP, statement of rights, description of how and to what extent those rights are being shared with the other party, and then a list of restrictions on the other party's use. However, each of these sections can be used in nontraditional ways to craft a holistic picture of permissions and protections, while also laying the proper foundation for further business opportunities.

For example, if a customer is clearly restricted in the contract from using a client's product in connection with machine learning and natural language processing, then the client can negotiate different financial terms if the customer wants that restriction removed.

Alternatively, when representing the customer, the reviewing attorney needs to understand how these restricted functions might fit into the buyer's plan and whether the restriction diminishes the overall value. This demonstrates why it is so important to be aligned with internal teams on what generates new or additional value so that it can be legally distinguished.

Risk and liability mitigation are separate but equally important components of the contract governing

use of or creation with AI. Here again the law has not yet been developed to answer the question directly, so start by asking what law applies and how it might be applied in the relevant situation. Is it IP law? Manufacturing? Product liability? Privacy? Depending on which space a client traditionally occupies, its standard contracts or boilerplate provisions may not adequately address some of these potential liabilities.

Uncertainty remains around how the law will apply traditional implied warranties, so it is important to be clear about what the client is not warranting. Identify the broadest scope of potentially applicable law, review the statutory and case law elements in play, and then address them appropriately in the contract. A client is in a much better position to argue that its contracting partner knew and agreed to forgo product liability protections, for example, if this is conspicuously identified and disclaimed in the contract.

Liability with respect to AI also provides the opportunity to innovate and negotiate based on client priorities. AI in a commercial setting is often interdependent on the IP of others, e.g., using third party data to improve/evolve AI software.

That fact coupled with existing ambiguities across jurisdictions as to whether or not liability can adhere to AI-driven decision-making counsels in favor of contracting parties taking a thoughtful approach about who is responsible for what actions, and, perhaps where it is reasonable, agreement on shared liability.[6]

## **Open Source**

Stepping away from historically closed IP models, some companies, including many of the leading tech companies, have opted instead to release open source frameworks and machine learning libraries in order to extend the type of collaborative sharing and building ushered in by the open-source software movement. This theory of a so-called virtuous circle — through which public availability leads to faster development and better products — is a now-familiar one.

Going open source with AI does not require that companies abandon goals of monetizing their innovation or ceding downstream control. Quite the contrary. Open source provides a menu of options for clients attracted to what it has to offer — though perhaps even more so than with more traditional forms of protection, serious front-end conversations about business goals and rights preservation are key.

## **Conclusion**

The AI landscape is evolving as quickly as the machine capabilities underlying it. Even so, a few practical points guide IP considerations in this space:

1. There is no one-size-fits-all solution. Like the organizations that are deploying and relying on AI, AI is dynamic. The right IP for any company's AI is the IP that meets the client's current — as well as future — goals. Particularly given the legal uncertainties outlined above, it is important to consult with experienced AI IP counsel to ensure goals are met.
2. Consider overlapping IP protection. IP regimes are not mutually exclusive, though some dovetail more neatly than others. Mapping out what IP regime best corresponds to each asset is a good exercise and one worth repeating at different points in time.

3. Ask the important questions, and ask them early. At a minimum, attorneys should consider the below, and recognize that the client's answers may prompt additional questions:

- What are the AI's inputs? In other words, where do the data sets originate and what proprietary claim do others have to those data sets?
- Who are the company stakeholders and how early are key internal drivers such as engineers being engaged in the IP conversation?
- Is this bet-the-company AI or does the AI prompt a more defense-minded move in order to ameliorate risks?
- Who are the intersecting rightsholders? Variations on this question include: are there any licensing limitations? Do others have access to evolving algorithms? Is there any joint development occurring?
- How, in terms as specific as can be stated, does the client intend to reap the benefits of the AI asset?

---

*Lori Bennett is general counsel at Aetion Inc.*

*Brian W. Nolan is a partner and Allison Aviki is an associate at Mayer Brown LLP.*

*The opinions expressed are those of the author(s) and do not necessarily reflect the views of the organization or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.*

[1] U.S. Patent and Trademark Office, Decision on Petition In re Application of Application No. 16/524,350, available at [https://www.uspto.gov/sites/default/files/documents/16524350\\_22apr2020.pdf](https://www.uspto.gov/sites/default/files/documents/16524350_22apr2020.pdf).

[2] European Patent Office, "EPO refuses DABUS patent applications designating a machine inventor" (Dec. 20, 2019), available at <https://www.epo.org/news-events/news/2019/20191220.html>.

[3] U.S. Copyright Office, "Sixty-Eighth Annual Report of the Register of Copyrights for the Fiscal year Ending June 30, 1965" (1966), available at <https://www.copyright.gov/reports/annual/archive/ar-1965.pdf>.

[4] U.S. Copyright Office, "Comments of the United States Copyright Office to the World Intellectual Property Organization Impact of Artificial Intelligence on IP Policy: Call for Comments" (Feb. 14, 2020), available at [https://www.wipo.int/export/sites/www/about-ip/en/artificial\\_intelligence/call\\_for\\_comments/pdf/ms\\_usa\\_usco.pdf](https://www.wipo.int/export/sites/www/about-ip/en/artificial_intelligence/call_for_comments/pdf/ms_usa_usco.pdf).

[5] *Zaleski v. Cicero Builder Dev., Inc.*, 754 F.3d 95, 102-03 (2d Cir. 2014).

[6] See, e.g., Iria Giuffrida, Liability for AI Decision-Making: Some Legal and Ethical Considerations, 88 Fordham L. Rev. 439 (2019), available at <https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=5627&context=flr>; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Art. 22, available at <https://eur-lex.europa.eu/eli/reg/2016/679/oj#d1e2838-1-1>; European Commission, "Ethics guidelines for trustworthy AI" (Apr. 8, 2019), available at <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>.