Volume 6, No. 1 | January–February 2023

RAIL

The Journal of Robotics, Artificial Intelligence & Law

fastcase FULL COURT PRESS

RAIL The Journal of Robotics, Artificial Intelligence & Law

Volume 6, No. 1 | January–February 2023

THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW (ISSN 2575-5633 (print) /ISSN 2575-5617 (online) at $495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint. Copyright 2023 Fastcase, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. For customer support, please contact Fastcase, Inc., 711 D St. NW, Suite 200, Washington, D.C. 20004, 202.999.4777 (phone), 202.521.3462 (fax), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: Morgan Morrissette Wright
Production Editor: Sharon D. Ray
Cover Art Design: Juan Bustamante

Cite this publication as:

The Journal of Robotics, Artificial Intelligence & Law (Fastcase)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

711 D St. NW, Suite 200, Washington, D.C. 20004
https://www.fastcase.com/

POSTMASTER: Send address changes to THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW, 711 D St. NW, Suite 200, Washington, D.C. 20004.

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please contact:

Morgan Morrissette Wright, Publisher, Full Court Press at mwright@fastcase.com or at 202.999.4878

For questions or Sales and Customer Service:

Customer Service
Available 8 a.m.–8 p.m. Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)
ISSN 2575-5633 (print)
ISSN 2575-5617 (online)

Can Trade Secret Laws Protect Algorithm-Based Intellectual Property?

David J. Walton and Karen L. Odash*

The authors discuss the complications of traditional protections for algorithm-based intellectual property and how trade secret protections may be more appropriate in certain circumstances.

How do you protect algorithm-based intellectual property ("IP") when traditional protections, like patent protections and copyright, do not apply to abstract ideas? Resorting to trade secret protections may not only be the best option but the only option. But achieving these protections requires a skilled, thoughtful plan of execution, and enforcement—everything from enforceable employee agreements to protections against inadvertent disclosures to client disclosure to data security. What is algorithm-based IP and how can trade secret laws protect it?

Hey Alexa, Hey Echo, Hey Siri

Algorithm-based IP is part of our lives. The alarm clock that is activated at the ideal time in our sleep cycle; the housing thermostat that senses movement and knows to adjust the heat as we awake; the coffee maker that knows when to make the first cup of coffee; and the fridge that monitors consumption patterns, adding items to the grocery list as needed, are all part of the morning routine.

Leaving the home and heading into work, checking the real-time traffic, and adjusting the commute, maybe even checking the weather to determine what to wear.

Leaving work at the end of the day, the GPS makes recommendations of where it thinks the driver is headed. Haven't moved from your desk in a while? Don't worry, the device on your wrist is monitoring your heart rate, steps, and calories, letting you know when it is time to get up again to optimize the wearer's health.

Robotics, Artificial Intelligence & Law / January–February 2023, Vol. 6, No. 1, pp. 53–60.

ISSN 2575-5633 (print) /ISSN 2575-5617 (online)

During the workday, the use of background checks and credit scores can derive intelligence that may indicate what type of employee is being hired or student is being admitted into a college.

Algorithms are also used to analyze video interviews to search for verbal and non-verbal cues that shed light on an individual. Algorithm-based analytics can monitor system use and access to determine which employees are at risk for defection and if any confidential information is at risk for being taken when the employee departs.

These types of algorithms are highly valuable and worth protecting, but how?

Algorithms and Algorithm-Based Intellectual Properties

What is an algorithm? Understanding what an algorithm is needs to happen before determining how to protect one. However, there is no agreed upon definition for algorithm-based artificial intelligence ("AI"). AI is a broad and ever evolving set of technologies that simulates intelligent behaviors in machines, enabling machine intelligence to simulate or augment elements of human behaviors. AI technologies include machine learning, natural language processing, speech processing, robotics, machine vision, and technologies that learn from previous data gathered.

Simply put, algorithms are a set of rules used to solve for a particular problem. Algorithms consist of both AI and analytics. Collectively, algorithms enable computers to replicate cognitive abilities of humans to cause interactions that look and feel natural and responsive.

Generally, there are two types of learning algorithms—supervised and unsupervised. Supervised learning algorithms detect structures based on labelled inputs which is "tagged data," and desired outputs.[1] Unsupervised learning algorithms find hidden structures from unlabeled data sets, by grouping together data that is similar. These learning algorithms are used to make predictions—and these predictive algorithms are those most used by AI systems. There is incredible value in predictive algorithms. Algorithm-based IP can be protected in a variety of ways, including through copyright, patent, and trade secret.

IP and Trade Secret Protections for Algorithm-Based Intellectual Properties

Patents are often thought to be the best form of protection for technological products. Thus, many people default to patent protection even for AI. For a technology to be patent eligible it must:

- Fall under a patent-eligible category,[2]
- Be novel,[3] and
- Be non-obvious.[4]

Additionally, the patent itself must include a written description of the invention, in such a manner that a person of ordinary skill would be able to create and use the invention.[5]

When someone or a company breaches a patent protection, a civil action is the best means to enforce and protect a patent.

If the patent protections are not the right fit for the algorithm-based technology, the best option may be trade secret protections. Trade secret protections can include the structure of the AI; the formulas used in the models; the training data, whether supervised or unsupervised; the output; the conversion of the output; and ultimately the end product, among other possibilities. Unlike other IP rights, a trade secret does not give the owner or licensee of the trade secret a complete monopoly over the subject of the trade secret. It simply protects it against misappropriation through various options like the Defend Trade Secrets Act (“DTSA”) or the Uniform Trade Secret Act (“UTSA”).

Trade secrets can be protected through the DTSA, which provides a private civil cause of action for victims of trade secret espionage or theft where a trade secret has been misappropriated. The DTSA requires that the trade secret be used in interstate commerce. It also requires that any conditions imposed on an employee be related to misappropriation—mere personal knowledge is not enough to show violation. The DTSA can result in civil and criminal penalties, particularly if the Economic Espionage Act is invoked.

The nearly identical UTSA, which has been adopted by 49 states, except New York, and the District of Columbia, allows trade secret misappropriation to be addressed at a state level. To be protected under the UTSA, a party must show that the information was secret and has actual or potential independent economic value due to its secrecy coupled with reasonable efforts to keep the information a secret. Additional steps include:

- The existence of a trade secret,
- An identified owner or licensee of the trade secret,
- Improper acquisition of the trade secret,
- Resulting in harm to the owner or licensee or unjust enrichment to another party, and
- The use, acquisition, or disclosure by the other party is a substantial factor in creating the harm or unjust enrichment, and are all necessary to prove a violation of the UTSA.

Civil actions for trade secret violations are similar to those available for copyright and patent infringement—everything from ceasing actions to returning information. Further, economic damages and moral prejudices are available as potential remedies.

Why Algorithms Are Harder to Protect Under Patent and Other Forms of IP Protection

In 2014, the U.S. Supreme Court looked at the ability to patent software in *Alice Corp. v. CLS Bank International.*[6] In its decision, the Court clarified the criteria for the eligibility test for software patents. Ultimately, the Court determined that patents covering certain computer-implemented transactions are abstract ideas and therefore not eligible under patent protections. To make an algorithm patentable, under *Alice*, requires converting an abstract idea into a method that is unique, novel, non-obvious, and useful. Even if an owner or licensee can overcome the hurdle of abstract ideas, the amount of time it takes to acquire IP protections frequently permits technology to outgrow the patent before the patent is even finalized.

Additionally, patents pertaining to AI technologies are hard to enforce. To obtain damages or acquire an injunction for a violation of a patent, the patent holder must establish infringement. Establishing infringement can put the patent at risk through defenses such as a prior use. AI technologies and the ability to detect them and their use in a competitor's product can also be difficult if not impossible. Finally, enforcement of a patent requires significant disclosure of the technology. If the competitor had not previously infringed on the patent, they may now possess significant insight into the patent holder's business and product.

Questions to consider on whether a patent or a trade secret protection makes the most sense include whether the algorithm-based AI is patent protectable, that is, does it meet the requirements of patent law? Does the algorithm-based AI consist of the type of information that can be kept secret by the company? If so, then patent protections may not be the best choice. Is the information likely to become generally known soon?

If the information is about to be generally known, either through use or disclosure, then trade secret laws will not protect it. Attempting to obtain a patent may make the most sense. Keeping in mind how quick the innovation becomes obsolete will also need to be considered. If it becomes obsolete quickly, or released to the public quickly, the process and expense of obtaining a patent may not be worth the benefit.

Finally, how hard is it to describe what the company is trying to protect? To obtain a patent, the filer must describe the invention to satisfy the obligation to disclose the technological knowledge on which the patent is based and to also demonstrate that the patentee is in possession of the invention. If it is difficult or time consuming to describe in the ways required to obtain a patent, a trade secret protection may make more sense.

Trade Secrets Can Offer Protections to Guard Algorithm-Based Intellectual Property

Algorithm-based AI is well-suited for trade secret protections. It can be difficult to reverse engineer AI. Additionally, protections afforded by patent law are not necessarily the best option due to length of time required to achieve protections. Rather, consider trade secret protections. They last as long as the secret remains a secret. Simply put, a license can continue indefinitely without an expiration date so long as the conditions of the license remain a trade secret.

Certain aspects of algorithm-based AI, such as raw data, is not patent eligible. Similarly, information and data sets used for machine-based learning or training models is also not protectable under patent law. They may, however, be protected as trade secrets. Trade secret laws can protect a business not only by protecting the data and the models but also by protecting what and how the company intends to use the information. Protection of the knowledge regarding what does not work is also available.

Companies create a valuable base of knowledge from failed actions and what does not work. Failed knowledge is not eligible for patent protection, but it is eligible to be protected under trade secret as a "negative trade secret."[7] Think of a negative trade secret as the knowledge of what does not work. If another company were to obtain and utilize such knowledge, it would allow them to potentially omit years of research and development, as the correct path of what works would be readily available to the competitor.

Trade secret protections also take immediate effect. There is no lengthy process or specific amount of time or expense required to protect a trade secret. So long as there are active actions taken to protect a trade secret, that trade secret can take effect immediately. Active actions could include things such as a nondisclosure or noncompete agreement, but it may be as simple as marketing in a way that prevents disclosure.

What Steps Should Be Taken to Protect a Trade Secret?

Employee Training

Training is key to protect a trade secret. Education of employees on what is a trade secret helps reduce the theft of trade secrets. It also prevents an argument later that the employee did not know that it was a trade secret. Incorporate such trainings during the life cycle of the employment—immediately upon hire, annually, and at terminations. Frequently, companies focus on getting the keys to the office and the fob for the elevator back at termination; instead, incorporate into the process the return of all trade secret information, laptops, printed paperwork, work product, and data sets.

Label Confidential Items

Label things confidential that are truly confidential. Label things for internal use only if they should not be seen or utilized by non-employees. Limit audiences to individuals who need to know the information obtained. Limit access to systems to those that need the access. Do not go overboard and just label everything confidential but be thoughtful on what is confidential and why.

Be Ready to Enforce

Know what the trade secret is that needs to be enforced and why it matters. Enforcement is not as simple as a former employee took the information or the former employee misappropriated the information. The company needs to know why it matters that the information has left the bubble of secrecy.

Monitor and Measure Employee Engagement

Companies can use algorithm-based AI to check for changes in activities of employees, looking for potential departures or filtering of trade secret information.

Avoid Disclosure to Customers

When marketing your products to customers, make sure that this is done without disclosing the trade secret. It's not uncommon to make an inadvertent disclosure to a consumer during the marketing process. Additionally, consider a nondisclosure agreement for third parties who need to obtain trade secret information in order to fulfill their obligations.

Look at Data Security

Limit access as needed. Implement the use of passcodes. Restrict technology to prevent the use of downloads or storage on external devices. Implement hacking protections to reduce the unintended disclosure of the trade secret information. Make sure to review cyber security policies to limit potential unauthorized access.

Conclusion

If, after careful review, trade secret protections make more sense for algorithm-based IP than traditional IP protections, it is important to take steps from the beginning to ensure that the AI is protected as a trade secret. Most important, when there is a trade secret theft, act quickly to gather relevant information and connect with appropriate legal representation to assist in any potential enforcement action. And now your fridge just notified you that your milk has spoiled, so it is time to ask Alexa to place a grocery order.

Notes

[*] David J. Walton, a partner in the Philadelphia office of Fisher Phillips, focuses his practice on trade secrets, restrictive covenants, and employment litigation. He may be contacted at dwalton@fisherphillips.com. Karen L. Odash, an associate in the firm's Philadelphia office, assists clients with a range of labor and employment matters, including counseling on restrictive covenants and trade secrets. She may be contacted at kodash@fisherphillips.com.

[1] Datailsynet, "AI and Privacy Report" (2018) 8-9.

[2] 35 U.S.C. § 35.

[3] 35 U.S.C. § 102.

[4] 35 U.S.C. § 103.

[5] 35 U.S.C. § 112(a).

[6] *Alice Corp. v. CLS Bank International*, 134 S.Ct. 2347 (2014).

[7] Cal. Civ. Code § 3246.1(d); *accord XpertUniverse, Inc. v. Cisco Sys., Inc.*, No. CIV. A. 09-157-RGA, 2013 WL 867640, at *2 (D. Del. Mar. 8, 2103), *aff'd* (Jan. 21, 2015).