Insights, News & Events

CAN TRADE SECRET LAWS PROTECT ALGORITHM-BASED INTELLECTUAL PROPERTY? 6 STEPS FOR EMPLOYERS TO CONSIDER

Insights
Dec 16, 2022

How do you protect algorithm-based intellectual property 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. Achieving these protections, however, requires a skilled, thoughtful plan of execution and enforcement – you'll need to consider everything from enforceable employee agreements to protections against inadvertent leaks to client disclosures to data security. Traditional protections for algorithm-based intellectual property are complicated and trade secret protections may be more appropriate in certain circumstances. So, what is algorithm-based intellectual property, and how can trade secret laws protect it? Here are six steps that employers should consider in this area.

Hey Alexa, Hey Echo, Hey Siri

Algorithm-based intellectual property is part of our daily lives:

- Our morning routine includes 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 and adds items to the grocery list as needed.
- Leaving the home and heading into work, we check the real-time traffic and adjust the commute, maybe even

Related People

Karen L. Odash

Associate

610.230.2165

David J. Walton, AIGP, CIPP/US

Partner

610.230.6105

check 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 health.

Employers also regularly turn to such technology. The use of background checks and credit scores at work 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? You need to understand what an algorithm is before you can determine how to protect one. However, there is no agreed upon definition for algorithm-based artificial intelligence. Artificial intelligence (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 previously gathered data.

Simply put, algorithms are a set of rules used to solve for a particular problem. Algorithms consist of both AI and analytics. Collectively, they 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 labeled inputs — which are known as "tagged data" — and desired outputs. *Unsupervised learning algorithms* find hidden structures

Service Focus

AI, Data, and Analytics

Counseling and Advice

Privacy and Cyber

Resource Hubs

AI Governance Hub

from unlabeled datasets 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 under U.S. law it must: (1) fall under a patent-eligible category; (2) be novel; and (3) be non-obvious. 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. When someone 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 Secrets 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. 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 (all but 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: (1) the existence of a trade secret; (2) an identified owner or licensee of the trade secret; (3) improper acquisition of the trade secret; (4) resulting in harm to the owner or licensee or unjust enrichment to another party; and (5) 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 remedies 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*, 134 S.Ct. 2347 (2014). 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. In other words, 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. Keep in mind how quickly the innovation becomes obsolete. If it becomes obsolete quickly or is 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 the 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. The information may, however, be protected as trade secrets. Trade secret laws can protect your company’s data and models and also protect how the company intends to use the information.

You may also be able to protect knowledge about what does not work. Companies create a valuable base of knowledge from failed actions. Notably, failed knowledge is not eligible for patent protection, but it is eligible to be protected under trade secret as a "negative trade secret." 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" — rather than passive actions — taken to protect a trade secret, that trade secret can take effect immediately. "Active actions" could include obtaining a non-disclosure or non-compete agreement, but it may be as simple as marketing in a way that prevents disclosure.

6 Steps to Help You Protect a Trade Secret

1. **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 the information was a trade secret. Incorporate such trainings during the life cycle of 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. You should also consider how to handle the return of all trade secret information, laptops, printed paperwork, work product, and data sets.

2. **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.

3. **Be ready to enforce**. Know what the trade secret is that needs to be enforced and why it matters. In additional to knowing that a former employee took the information or misappropriated it, you should know why it matters that the information has left the bubble of secrecy.

4. **Monitor and measure employee engagement.** You can use algorithm-based AI to check for changes in activities of employees, looking for potential departures or filtering of trade secret information.

5. **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 inadvertently disclose such information 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.

6. **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

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

We will continue to monitor developments regarding artificial intelligence, so make sure you are subscribed to Fisher Phillips' Insight system to keep up with the most up-to-date information. Please contact your Fisher Phillips attorney, the authors of this Insight, or any attorney in our Privacy and Cyber Practice Group should you have any questions.

Note: A version of this article was originally published in the January-February 2023 edition of The Journal of Robotics, Artificial Intelligence & Law.