Re-evaluating companies' AI protection strategies

Artificial intelligence innovation is challenging to patent because of changes in US law, meaning trade secrets may be more appealing. **David A Prange** and **Alyssa N Lawson** examine how to approach AI asset protection

Once relegated to science fiction movies, artificial intelligence (AI) is hyped as being the "New Space Race" or having the potential to start World War III. But aside from the hype, developing AI to simplify or eliminate everyday human tasks is presently at the forefront of technological innovation. Companies are engaged in significant research and development that consumes substantial resources. While advancements in AI may continue to accelerate, companies should not move so quickly as to pass over the opportunity to protect these investments.

Traditional intellectual property theories may protect these AI assets, particularly if structured to complementarily protect different aspects of AI. A significant portion of AI innovation involves the design of algorithms and software architectures, and companies should understand the trade-offs for using different theories of protection. Obtaining and defending the validity of computer-implemented patents has become more difficult in recent years. Furthermore, the more stringent application of subject matter patentability and public disclosure requirements, and the fast pace of AI innovation and marketplace competition, means companies may find it less attractive to seek patent protection for a company's AI intellectual property. Accordingly, there is a growing recognition by companies to use trade secret theories to protect their AI innovations.

Trade secret law offers a complementary alternative to patents for protecting AI assets. Recent passage of the Defend Trade Secrets Act (DTSA) provides a federal cause of action for trade secret misappropriation claims, which may potentially lead to reducing uncertainty otherwise resulting from state-by-state variations in

1 MINUTE READ

Protecting AI innovation is a challenge. Software architectures and algorithms have become harder to patent as a result of recent changes in the law, most notably the Supreme Court's 2014 *Alice* decision. In patent prosecution, as many AI systems focus on source code and algorithms and replicating human activity, the challenge is how to claim it to be patent eligible. However, the USPTO has recognised that AI can be patentable by an express class designation, and at least two examining prior art units are specifically designated for reviewing patent applications directed toward AI algorithms. Companies may find more success by focusing on AI hardware innovations. A trade secret protection strategy is also well-suited for the rapidly developing and changing marketplace of AI innovations. Trade secret protection allows for more flexibility in what to protect with lower costs of establishing protection in comparison to patents. This flexibility may be beneficial in a rapidly evolving technology like AI.

The status of US law presents hurdles for companies seeking to protect these AI developments through patents. One of the fundamental challenges involves claiming subject matter that is patent eligible

trade secret law. As a result, trade secret law protections have become more attractive to companies wishing to protect their AI innovations. In view of the renewed focus on trade secrets, and the scrutiny on patents, this article considers some of the trade-offs between trade secrets and patents for protecting AI.

No longer science fiction; AI in everyday life

In the mid-1950s, John McCarthy, a computer scientist and one of the founding fathers of AI, first coined the term "artificial intelligence" as "the science and engineering of making intelligent machines, especially intelligent computer programs." AI is colloquially applied when a machine mimics "cognitive" functions of human minds, such as learning or problem solving. In computer science, however, AI is a broad and constantly evolving technical field that includes machine learning, natural language processing, speech processing, robotics, and machine vision. Presently, AI implementations understand human speech, autonomously drive cars, interpret complex data and images, or make strategic decisions. AI development has worked toward the goal of becoming an integral part of human life by expanding its proficiency into multiple platforms. In recent years, companies have accelerated investments in AI by adding AI features to existing products or creating new product offerings based entirely in AI. The digital age and its enormous quantities of data – referred to as "big data" – have created opportunities for companies to develop AI technology to use, process, and filter the large volumes of data that support machine learning.

The scope of AI complexity can vary dramatically. For, example, certain AI systems autonomously carry out entire complex processes based on past experience, while modifying processes as experience develops. This AI can turn the data into insights and insights into instructions and instructions ultimately into actions. An example of this type of AI is a self-driving car. Other AI systems have been modelled on human brain function. Several companies have developed software architectures consisting of artificial neural networks designed to process information by simulating the biological framework of the human brain. The architecture relies on layers of millions of clusters performing mathematic computations, similar to the connections between neurons in a brain. Such advances have led to increased accuracy of image and video processing and recognition, text analysis, and speech recognition. Yet other AI systems address the functional management of house appliances, such as smart refrigerators tracking product freshness. The broad implementation of AI across industries has led to market size predictions of at least $47 billion by 2020.

While AI implementations may vary in their complexity and scope, common to AI applications is their reliance on software architectures and algorithms. Software and algorithms may be protected to varying degrees based on the type of intellectual property legal framework used. A company desiring to maximise its protection of AI investments should develop an understanding of the complementary protections available; while historically the focus has been almost exclusively on patents, companies would be well served to develop at least trade secret protections in view of the increased scrutiny on software patents.

Protecting AI innovation with patents

Artificial intelligence presents protection challenges based on its character alone: AI at its core involves computer-implemented inventions. For example, these inventions may be computer programming or hardware implementing mathematical models, algorithms or a neural network, or data consisting of generating raw data and the resulting analytic data output. Oftentimes the novelty in AI innovation is the application of a known technique underlying and applied to a new domain or problem. The status of US law presents hurdles for companies seeking to protect these AI developments through patents.

One of the fundamental challenges involves claiming subject matter that is patent eligible. Under Section 101 of the Patent Act, the subject matter of a patent claim must be directed to a "process, machine, manufacture or composition of matter." In *Diamond v Diehr*, 450 US 175 (1981), the US Supreme Court held that claims directed to nothing more than an abstract idea, such as a mathematical algorithm, are not eligible for patent protection. But although underlying mathematical algorithms have been recognized as unpatentable for some time, patent applicants have tried numerous different claiming techniques to claim software originating from algorithmic instructions. In 2014, the Supreme Court considered the patentability of software in *Alice Corp v CLS Bank International*, 134 S. Ct. 2347 (2014). The Court clarified the patent subject matter eligibility test for software patents to consider whether the claims (1) only encompass abstract ideas and (2) if encompassing an abstract idea, whether the claims include some additional inventive step showing an application of the abstract idea. The Supreme Court in *Alice* invalidated the patent at issue because it consisted of a computer-implemented business process for mitigating settlement risk for trades between financial institutions. According to the Court, the process could be done without the assistance of a computer and, thus, did not exhibit an additional inventive step.

A result of the *Alice* decision has been an increased examination of software patent eligibility and more aggressive challenges by patent infringement defendants. Federal court decisions applying the two-part *Alice* test demonstrate a stiffening inquiry to the patent eligibility requirement. Cases addressing patents directed to the manipulation of information using a computer

that may otherwise be done by hand, albeit more slowly, have generally found such types of patents invalid. For example, in *Purepredictive v H20.AI*, Case No. 17-cv-03049-WHO, 2017 US Dist LEXIS 139056, at *2-3 (Northern District of California August 29 2017), the court considered a patent addressed to a method and apparatus for performing predictive analytics, which included the steps of receiving data and generating "learned functions" or regressions from that data, evaluating the effectiveness of those learned functions at making accurate predictions based on the test data, and selecting the most effective learned functions and creating a rule set for additional data input. The court held the concept of manipulation of mathematical functions an abstract idea. The court went on to find that the claim did not demonstrate any inventive concept by demonstrating a specific application of that abstract idea.

Other cases have found the general manipulation and processing of data likewise unpatentable. *See, for example, OpenTV v Apple*, No. 14-cv-01622, 2015 US Dist LEXIS 44856 (Northern District of California April 6 2015). In general, since the 2014 *Alice* decision, the number of early patent subject matter eligibility challenges by early motion has increased dramatically, with nearly three-fourths of all motions brought being granted, and a success rate of 78% in 2016.

Patent prosecution has likewise become more difficult. The USPTO placed greater emphasis on the eligibility requirement through application of specific guidelines promulgated to patent examiners regarding best practices for formulating subject matter eligibility rejections in view of the changed legal landscape. As many AI systems focus on source code and algorithms and replicating human activity, the challenge is how to claim it to be patent eligible. An improperly drafted patent application directed to AI that does not describe more than mathematical algorithm, or that fails to define some additional inventive step, may not reach issuance. However, while patent protection may be more difficult to obtain, that is not to say that patent protection is unobtainable for artificial intelligence inventions. The USPTO has recognised that AI can be patentable by an express class designation – class 706: Data Processing – Artificial Intelligence. Furthermore, at least two examining prior art units are specifically designated for reviewing patent applications directed toward AI algorithms – Art Units 2121, 2129, and 2691.

Though protecting software AI innovations with patents has fundamental challenges, companies may find more success by focusing on AI hardware innovations. Characterising AI innovation in a hardware context, and beyond use of a general-purpose computer, may avoid having the innovation considered an abstract idea. For example, in *Thales Visionix v United States*, 850 F.3d 1343 (Federal Circuit 2017), the Federal Circuit found the challenged claims were patent-eligible where the claims addressed a configuration of sensors instead of the mathematical equations used to make the sensor calculations. On the other hand, the Federal Circuit in *Vehicle Intelligence and Safety v Mercedes-Benz USA*, 636 Fed. App. 914 (Federal Circuit 2015), found no patentable concept when the patent claimed use of an undefined expert system without providing a particular use or application of the system or any specific details as to how the systems provided a more efficient result. Thus, as guided by the *Alice* decision, one strategy to protecting AI innovations with patents is to claim AI in a way that transforms the abstract idea into patent-eligible physical subject matter. Similarly, inventions applying machine learning that requires some change or output in the physical world have a greater chance of surviving the eligibility requirements.

While patent protection may be more difficult to obtain, that is not to say that patent protection is unobtainable for artificial intelligence inventions. The USPTO has recognised that AI can be patentable by an express class designation

While there are still opportunities to obtain patent protection related to artificial intelligence (as it will depend on the proposed claim language), other patenting requirements should also be considered. For example, a patent application should provide an adequate written description of the invention. To adequately support the claims, this may require disclosing the algorithms and specific software code for the application. This disclosure is generally made at the time of filing the patent application. However, while providing details can help support the claims written description and avoid abstraction, it can also severely narrow the scope of protection and publish to the public all previously proprietary details. Thus, a company seeking patent protection for its artificial intelligence innovations may arrive at the unenviable position of disclosing to the public an asset with significant underlying investment yet still not obtain any or all of the requested patent protection for it. This trade-off of public disclosure for patent ownership with maintaining secrecy of AI innovations that will now face heightened review as to whether the innovation is patent eligible suggests that companies should revisit and strengthen trade secret protection plans if innovation secrecy is the primary concern.

AI innovations as trade secrets

Trade secret protection theories can protect a broader group of competitive assets than what can be protected by a patent. Unlike a patent, information protectable as a trade secret does not need to be a novel or nonobvious improvement over what is generally known. Further, statutes defining the scope of what types of information may qualify for trade secret protection broadly include almost any type of business-related information provided that it meets other requirements, including that the business takes reasonable measures to keep the information secret and that the information has independent value in not being generally known in the industry. Thus, while it may be a challenge to obtain patent protection for mathematical algorithms and abstract ideas, companies can protect their investments in developed AI processes by keeping them secret. Moreover, the broad scope of what may be a trade secret po-

A trade secret protection strategy is also well-suited for the rapidly developing and changing marketplace of AI innovations

tentially allows for the protection of data sets that underlie the machine learning of AI.

A trade secret protection strategy is also well-suited for the rapidly developing and changing marketplace of AI innovations. Patent prosecution can take years to complete and requires detailed public disclosure of the invention, including an immediate and potentially substantial hurdle of demonstrating the invention is patent eligible subject matter. Trade secret protection, on the other hand, offers the advantage of gaining immediate protection (provided one can substantiate the requirements for demonstrating that information is a trade secret) while avoiding the need for public disclosure. There is no application process, no government approval, and no patent prosecution costs or fees. A company does not need to determine that an invention should be patented or take any internal position on whether the information may be patentable. Further, if the marketplace shifts or an AI technology developed by a company proves unsuccessful, using a trade secret protection plan, instead of seeking patents, reduces the investment loss that may otherwise be incurred from pursuing patent protection and paying related patent prosecution expenses.

Relatively recent changes in trade secrets law, namely passage of the DTSA, potentially make protection of AI assets with trade secret theories more appealing. To the extent that state-by-state variations in trade secret law created uncertainty and complications in the assertion of trade secret claims throughout the country, the DTSA federal framework now provides a common claim for assertion. Further, and while there is not much debate that state trade secrets laws are broad enough to cover algorithms and data compilations, the federal framework expressly contemplates protecting computer source code as a trade secret.

Nonetheless, trade secret protection has limits in comparison to patent protection. Appropriate defences to a claim for trade secret misappropriation include legitimate reverse engineering or that the information does not have independent economic value. Similarly, independent development of what a company claims as a trade secret may also be a viable defence to a claim of trade secret misappropriation. In comparison, reverse engineering and use of the gained knowledge is not a defence to patent infringement. Further, one may infringe a patent regardless of the economic value that the patent provides to the patent owner's business. Thus, while trade secret protection may more easily accommodate the subject matter for protection – source code and algorithms – the trade-off in litigation is the requirement to demonstrate that the information claimed to be a trade secret should be protected as such.

Take a holistic approach

Protecting AI innovation has no easy solution – patent protection is more difficult to obtain and trade secret protection has been characterised as needing "eternal vigilance" to police secrecy. Businesses investing in AI face increasing uncertainty following the erosion of patent protection for computer-implemented inventions and the detailed disclosure requirements and elongated timeline for patent protection in a fast-pace marketplace. While trade secret law offers an alternative avenue for protection of these assets, there are separate associated challenges. The better course is to approach the AI asset protection challenge holistically, using patents, trade secrets, and in addition copyrights and contractual protections, to protect different aspects of these company investments.

David A Prange

Alyssa N Lawson

 Prange is a partner at Robins Kaplan and leads the trade secrets subpractice. Lawson is a trial lawyer at Robins Kaplan, practicing in the intellectual property and technology group. Both are based in Minneapolis