

## The Rising Importance of Trade Secret Protection for AI-Related Intellectual Property

Artificial intelligence (AI) has quickly become one of the pillars of the modern economy. According to one widely cited study from 2017, AI could contribute up to \$15.7 trillion dollars to the global economy by 2030.<sup>1</sup> That prediction is already coming to fruition. According to a White House report on AI from February 2020, “AI is already having a substantial economic impact, not only for companies whose core business is AI, but also for nearly all other companies as they discover the need to adopt AI technologies to stay globally competitive.”<sup>2</sup> The recognition of the importance of AI is both broad and worldwide. Russia’s Vladimir Putin has gone as far as to state that “whoever becomes the leader in [AI] will become the ruler of the world.”<sup>3</sup>

It is thus no surprise that companies are heavily investing to protect the intellectual property generated from their investments in AI technology.<sup>4</sup> The question becomes how to best protect those investments in this critical space. For example, an autonomous driving company may be looking at its AI training data (i.e. records of previous test drives), the artificial neural network implementations generated from that training data (i.e., the software that helps the car drive itself), and assortments of other source code necessary to operate an autonomous car. For each of these elements, the company must examine what aspects are patentable, subject to trade secret protection—or both. The wrong decision on these topics could result in the company being left with no meaningful intellectual property protection for its most important research and development.

But patenting AI technology today can be difficult. Due to the prohibition on patenting abstract ideas, acquiring meaningful patents on artificial intelligence systems is not straightforward. Thus companies are increasingly turning to trade secret protection to protect their AI-related intellectual property. This article explores the tradeoffs between patents and trade secrets in the AI sector. It then describes how trade secrets have become essential tools for companies to protect their AI-related intellectual property. Finally, it concludes with practical guidance for in-house counsel on how to leverage both patents and trade secrets to best protect valuable intellectual property regarding AI.

### I. What is “artificial intelligence”?

First, a word on terminology. Like many popular technology areas, companies have been invoking the term “artificial intelligence” to describe their products at the earliest opportunity—even where the underlying technology does not fit within the established definition of artificial intelligence.

---

<sup>1</sup> See PwC’s Global Artificial Intelligence Study: Exploiting the AI Revolution at 3, <https://www.pwc.com/gx/en/issues/data-and-analytics/publications/artificial-intelligence-study.html>.

<sup>2</sup> American Artificial Intelligence Initiative: Year One Annual Report (February 2020) at 1, <https://www.whitehouse.gov/wp-content/uploads/2020/02/American-AI-Initiative-One-Year-Annual-Report.pdf>.

<sup>3</sup> “*Putin says the nation that leads in AI ‘will be the ruler of the world,’*” The Verge, (Sept. 4, 2017), available at <https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world>

<sup>4</sup> PwC MoneyTree Report (Q4 2018), <https://www.pwc.com/us/en/moneytree-report/moneytree-report-q4-2018.pdf>

For purposes of this article, artificial intelligence generally refers to technology that, in some sense, mimics human intelligence. In particular, AI under this definition permits computers to perform some task without being expressly programmed to do so. To that end, this article will focus on machine learning, neural networks, related training models, algorithms and data.

## II. Patents versus Trade Secrets – The Tradeoff of Public Disclosure

Patents confer a legal right to exclude others from making, using, selling, and importing the invention claimed for a number of years. But, in order to take advantage of this government-sanctioned monopoly, the inventor must disclose the invention to the public with enough detail such that the invention can be recreated by others in that field. This *quid-pro-quo*—a disclosure of the invention to the public in return for a limited-in-time monopoly on the invention—is one fundamental underlying policy objective of US patent law.

By contrast, trade secrets, as the name suggests, protect information that is “secret.” Trade secrets can provide protection for any information where the owner “has taken reasonable efforts to keep such information secret” and the information “derives independent economic value, actual or potential, from not being generally known” to other persons.<sup>5</sup> Both federal and state law provide protection for trade secrets. Historically, trade secret protection has been applied to a wide variety of subject matter, including compilations of public data,<sup>6</sup> source code,<sup>7</sup> schematics, diagrams, and customer lists—amongst many other pieces of information.

In many ways, trade secret law can be broader or more flexible than patent law. Unlike patents, trade secret protection can be obtained without any application or registration—it arises automatically if the trade secret owner takes appropriate steps to ensure the information is secret and so long as it provides a competitive benefit. Trade secret protection can also theoretically last as long as the information is kept a secret. And trade secret law also “protects items which would not be proper subjects for consideration for patent protection under 35 U. S. C. § 101.” *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 482-3 (1974). For example, a list of customers could be protected as a trade secret, but certainly not as a patent.

But in other ways trade secret protection is weaker than patent law. Importantly, independent development is a defense to trade secret misappropriation, but not for patent infringement. As explained by the Supreme Court in *Kewanee* in 1974:

Trade secret law provides far weaker protection in many respects than the patent law. While trade secret law does not forbid the discovery of the trade secret by fair and honest means, e. g., independent creation or reverse engineering, patent law operates “against the world,” forbidding any use of the invention for whatever purpose for a significant length of time. The holder of a trade secret also takes a substantial risk that

---

<sup>5</sup> See, e.g., 18 U.S.C. 1839(3) (Federal Defend Trade Secrets Act, definition of “trade secret”); Cal. Civ. Code § 3426.1(d) (California Uniform Trade Secrets Act, definition of “trade secret”).

<sup>6</sup> See, e.g., *N. Am. Deer Registry, Inc. v. DNA Sols., Inc.*, 2017 WL 2402579, at \*7-8 (E.D. Tex. Jun. 2, 2017) (acknowledging that a novel or unique combination of publicly known elements may constitute a trade secret); *Strategic Direction Grp., Inc. v. Bristol-Myers Squibb Co.*, 293 F.3d 1062, 1065 (8th Cir. 2002).

<sup>7</sup> See, e.g., *People v. Wakefield*, 2019 WL 3819326, at \*5 (N.Y. App. Div. Aug. 15, 2019).

the secret will be passed on to his competitors, by theft or by breach of a confidential relationship, in a manner not easily susceptible of discovery or proof. Where patent law acts as a barrier, trade secret law functions relatively as a sieve.

*Kewanee*, 416 U.S. at 489-490 (footnote and citation omitted).

This view is not universal. One can ask whether Coca-Cola, the holder of one of the most famous trade secrets—the formula for Coca-Cola—would agree with this view.<sup>8</sup> More to the point, times have changed since the *Kewanee* decision in the 1970's. Under recent Supreme Court precedent, for certain types of innovations related to AI, the pendulum has swung away from patent protection towards trade secret protection.

### III. The Difficulties in Patenting AI – *Alice* and Abstract Ideas

Recent years have seen a rapid acceleration in the number of patent applications directed to inventions in the field of artificial intelligence. More than half of all AI-related patent applications have been published since 2013.<sup>9</sup> Within that time, applications related to machine learning have grown by an average of 28% each year, applications related to computer vision have grown by an average of 46% each year, and applications related to robotics and control methods have grown by an average of 55% each year.

Despite this surge in applications, however, there are potential pitfalls to seeking patent protection over AI-related inventions. In particular, to receive a patent, the patent must claim patent-eligible subject matter under 35 U.S.C. § 101. One category that is ineligible for patent protection is abstract ideas. Over the last 15 years, the clear trend in the case law is applying the prohibition on patenting abstract ideas more strictly to software-centric inventions.

The current law governing subject matter eligibility comes from the Supreme Court's 2014 decision in *Alice Corp. v. CLS Bank International*.<sup>10</sup> Under *Alice* and its progeny, courts are directed to “first determine whether the claims at issue are directed to one of those patent-ineligible concepts, and if so, then as what else there is in those claims.”<sup>11</sup> If they find the invention directed to a patent-ineligible concept (e.g., an abstract idea), a court “must examine the elements of the claim to determine whether it contains an inventive concept sufficient to transform the claimed abstract idea into a patent-eligible application.”<sup>12</sup>

Since almost all AI-related inventions are implemented through software processes running on computer hardware, patent eligibility for these inventions are generally governed by the same legal

---

<sup>8</sup> See *Coca-Cola Bottling Co. of Shreveport v. Coca-Cola Co.*, 107 F.R.D. 288, 294 (D. Del. 1985) (“The written version of the secret formula is kept in a security vault at the Trust Company Bank in Atlanta, and that vault can only be opened by a resolution from the Company's Board of Directors. It is the Company's policy that only two persons in the Company shall know the formula at any one time, and that only those persons may oversee the actual preparation of Merchandise 7X. The Company refuses to allow the identity of those persons to be disclosed or to allow those persons to fly on the same airplane at the same time.”).

<sup>9</sup> See WIPO Technology Trends 2019, Artificial Intelligence, [https://www.wipo.int/edocs/pubdocs/en/wipo\\_pub\\_1055.pdf](https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf) at 13.

<sup>10</sup> *Alice Corp. v. CLS Bank International*, 573 U.S. 208 (2014).

<sup>11</sup> *Id.* at 218.

<sup>12</sup> *Id.* at 221.

principles applied to other software patents. But in recent history, the application of patent eligibility standards to these kinds of software-based inventions has proven unpredictable.<sup>13</sup>

Some guidance has also recently emerged from the PTO, which has faced its own challenges implementing the post-*Alice* jurisprudence into its examination processes. Indeed, the PTO has acknowledged that “[p]roperly applying the *Alice/Mayo* test in a consistent manner has proven difficult, and has caused uncertainty in this area of the law.” The PTO recently instituted new guidance in 2019 regarding the application of this developing case law to pending patent applications, attempting to provide a more concrete framework for application of *Alice* and its progeny based on “enumerated groupings of abstract ideas.”<sup>14</sup> While this guidance is relatively new, initial review decisions since its introduction suggest a potentially friendlier environment for AI-related applications.<sup>15</sup>

Despite this guidance, there remain serious risks in seeking patent protection over AI-based inventions. Given the limitations articulated in *Alice* and its progeny, it is unclear how many of the AI-related patents that have made their way through the U.S. Patent Office would survive in eventual litigation. *Hyper Search, LLC v. Facebook, Inc.*, No. CV 17-1387-CFC-SRF, 2018 WL 6617143, at \*10 (D. Del. Dec. 17, 2018) illustrates how some courts are applying *Alice* to invalidate patents related to artificial intelligence:

Claim 1 of the ’412 patent recites generic computer functionality such as a “neural network module” and a “server.” (’412 patent, col. 19:49-67) Limiting the use of an abstract idea “to a particular technological environment” does not transform an abstract idea into a patent-eligible invention. *Alice*, 134 S. Ct. at 2358 (internal citations omitted). The specification states that neural networks were well-known in the art, and the inventors stated that the alleged invention is not limited to neural networks but rather to “any artificial intelligence agent.” (’412 patent, col. 7:45-8:5, 19:23-27) Courts have previously found that claims reciting neural networks to be unpatentable for failing to recite more than an abstract idea. See *Neochloris, Inc. v. Emerson Process Mgmt LLLP*, 140 F. Supp. 3d 763, 773 (N.D. Ill. 2015) (finding patent claims including “an artificial neural network module” invalid under § 101 because neural network modules were described as no more than “a central processing unit – a basic computer’s brain”).

---

<sup>13</sup> In the aftermath of *Alice* district courts and the Federal Circuit have expressed difficulty in consistently applying this framework. See, e.g., *Interval Licensing LLC v. AOL, Inc.*, 896 F.3d 1335, 1355 (Fed. Cir. 2018) (Plager, J., dissenting) (describing “uselessness of the abstract notion of ‘abstract ideas’ as a criterion for patent eligibility”); *Berkheimer v. HP Inc.*, 890 F.3d 1369, 1374 (Fed. Cir. 2018) (Lourie, J., concurring); see also Testimony of Hon. Paul R. Michel, *The State of Patent Eligibility in America, Part I: Hearing Before the Subcommittee on Intellectual Property of the S. Comm. On the Judiciary*, 116<sup>th</sup> Cong. 2 (June 4, 2019) (recording testimony of former Federal Circuit Judge Paul Michel that “recent cases are unclear, inconsistent with one another and confusing,” and that he “cannot reconcile” their outcomes or “predict outcomes in individual cases with any confidence.”).

<sup>14</sup> See <https://www.govinfo.gov/content/pkg/FR-2019-01-07/pdf/2018-28282.pdf>. Note that while these guidelines do not have the force of law, they are themselves based on a distillation of post-*Alice* cases.

<sup>15</sup> See, e.g., <https://e-foia.uspto.gov/Foia/RetrievePdf?system=BPAI&flNm=fd2018007443-10-10-2019-0> (reversing rejection of claims that “recite monitoring operation of machines using neural networks, logic decisions trees, confidence assessments, fuzzy logic, smart agent profiling, and case-based reasoning” on the grounds that using “neural networks” in the context of monitoring a machine did not qualify as an abstract method of organizing human activity and that this “computational complexity” removed the claims from the realm of abstract mental processes).

*Id.* at \*10. After making these findings, the Court then held the asserted patent invalid as improperly claiming only abstract ideas. *Id.*

Similarly, in *Purepredictive, Inc. v. H2O.AI, Inc.*, No. 17-CV-03049-WHO, 2017 WL 3721480, at \*5 (N.D. Cal. Aug. 29, 2017), *aff'd sub nom. Purepredictive, Inc. v. H2O.ai, Inc.*, 741 F. App'x 802 (Fed. Cir. 2018), the Court invalidated an asserted patent directed to automating predictive analytics:

Turning to this case, I agree with H2O that PPI's claims are directed to a mental process and the abstract concept of using mathematical algorithms to perform predictive analytics. The method of the predictive analytics factory is directed towards collecting and analyzing information. The first step, generating learned functions or regressions from data—the basic mathematical process of, for example, regression modeling, or running data through an algorithm—is not a patentable concept. *See DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 1256 (Fed. Cir. 2014) (“We know that mathematical algorithms, including those executed on a generic computer, are abstract ideas.”). That the “function generator module” described in the '446 Patent “may generate hundreds, thousands, or millions of learned functions, or more,” '446 Patent at 9:55–57, does not change this conclusion.

*Id.* at \*5.

While each of these patents stand on their own and the decisions do not indicate that any future AI-related patents are necessarily invalid (or valid), they stand as guideposts that companies should be mindful of when considering patenting artificial intelligence inventions. *Compare id. with SRI International, Inc. v. Cisco Systems, Inc.*, 930 F.3d 1295 (Fed. Cir. 2019) (finding patent claiming “detecting, ...suspicious network activity based on analysis of network traffic data” directed towards patentable subject matter).

Finally, some AI-related innovations are simply not eligible to receive patent protection in the first place. For example, raw data collected for use in machine learning algorithms is not patentable in and of itself. That raw data combined with a conventional and well-known machine learning algorithm, also may not be patentable even though the result may be incredibly valuable to the company. Considering these limits and potential risks, many companies are turning to alternatives means to protect their valuable intellectual property in the AI space—namely, trade secrets.

## **IV. Trade Secrets – An Apt Tool for Protection AI Intellectual Property**

While it's hard to track the exact number of trade secrets related to AI that are being closely held by organizations around the world—as they are by their nature secret—it is likely that most intellectual property generated in the United States today related to AI is being protected through the use of trade secrets. While specific details remain confidential in light of strict confidentiality procedures, courts have already indicated that certain areas of information related to AI are protected

as trade secrets, such as algorithms, source code, and the way a business utilizes AI to implement machine learning.<sup>16</sup>

There are certain distinct advantages to trade secrets—no filings fees, protection in real-time, theoretically unlimited length of protection, and broadly eligible subject matter. For AI in particular, there are several reasons why trade secrets are particularly valuable and suitable for intellectual property protection as compared to patents:

- AI technology is rapidly developing and improving<sup>17</sup> at a rate the patent system is not designed to keep up with.
- Companies can create highly valuable intellectual property by understanding and creating a knowledge base about what technology does **not** work. While this knowledge does not qualify for patent protection, it can be protected as a “negative trade secret.”<sup>18</sup> If another company were to misappropriate this information, it could short circuit the need for years of research and development going down the wrong path.
- Some of the most important technology in AI is implementation know-how that is not suitable for patent protection. For example, because autonomous cars are not yet widely on the market, some companies have kept their technology secret from their competitors to gain an advantage.<sup>19</sup>
- As discussed, many AI developments are software-based, making patents more difficult to obtain under *Alice*.

Breaking down AI and machine learning systems into three stages, we can see the benefits of trade secret protection available at each one:

**Stage 1: Data Collection and Training** – Training data itself may not be protectable as a patent, but a collection of data—even where that data comprises otherwise public

---

<sup>16</sup> See e.g., *LivePerson, Inc. v. 24/7 Customer, Inc.*, 83 F. Supp. 3d 501, 514 (S.D.N.Y. 2015) (finding algorithms based on artificial intelligence eligible for trade secret protection).

<sup>17</sup> See “Nine charts that really bring home just how fast AI is growing,” MIT Technology Review (Dec. 12, 2018), available at <https://www.technologyreview.com/s/612582/data-that-illuminates-the-ai-boom/> (describing how “the state of the art is improving fast” in AI).

<sup>18</sup> Cal. Civ. Code § 3426.1(d); accord *XpertUniverse, Inc. v. Cisco Sys., Inc.*, No. CIV.A. 09-157-RGA, 2013 WL 867640, at \*2 (D. Del. Mar. 8, 2013), aff’d (Jan. 21, 2015) (“The definition [of a trade secret in Cal. Civ. Code § 3426.1(d)] includes information that has commercial value from a negative viewpoint, for example the results of lengthy and expensive research which proves that a certain process will not work could be of great value to a competitor.”).

<sup>19</sup> The implementation know-how must have potential or actual economic value to qualify as a trade secret. “Proprietary ways of doing the same thing that others in the same field do are not trade secrets.” *Agency Solutions.Com, LLC v. TriZetto Grp., Inc.*, 819 F. Supp. 2d 1001, 1017, 1021 (E.D. Cal. 2011)). If particular functionality of software is known or knowable without resort to clandestine means, then some aspects of the code may not comprise a trade secret even though the associated source code may itself be kept secret. But see *id.* (“Note, however, that while the way something is done is not a trade secret, some discrete fact concerning that way could conceivably be a trade secret.”).



information—can be protected as a trade secret.<sup>20</sup> This data can be highly valuable. According to *The Economist*, “[t]he world’s most valuable resource is no longer oil, but data.”<sup>21</sup>

**Stage 2: Neural Networks and Algorithms** – There may be difficulty patenting algorithms alone under *Alice*. But the algorithm or neural network design and implementation are eligible for trade secret protection if the statutory requirements are satisfied.

**Stage 3: Output of AI System** – Output data is potentially protectable as a trade secret if the relevant information is sufficiently secret and not generally known.

While trade secrets are increasingly important for AI companies, there is one major drawback in utilizing trade secrets: protection is only afforded to the extent the intellectual property can be kept secret. Keeping software a “secret” can be challenging and operationally taxing for several reasons: (1) given the turnover at technology companies, strong employment agreements are needed to ensure departing employees are legally required to keep trade secrets secret; (2) given the ease of “stealing” software—which can be as easy as downloading code to a USB drive—strong cybersecurity policies need to be created and enforced;<sup>22</sup> (3) because reverse engineering can be a defense to trade secret appropriation,<sup>23</sup> software needs to be designed and deployed in a way to ensure reverse engineering is not possible; and (4) in order to conduct business, it is often necessary to share technology widely with employees and partners, which increases the risk that a trade secret could be disclosed publicly.<sup>24</sup>

In light of these concerns, maintaining trade secret protection can incur meaningful costs for a company and requires significant ongoing vigilance. Companies relying on trade secret protection can take the following steps to help ensure the protection of their AI innovations:

- (1) Require third parties to sign non-disclosure agreements and restrictive licenses so they cannot disseminate trade secret information in unauthorized ways;<sup>25</sup>
- (2) Appropriately label company confidential information;

---

<sup>20</sup> See *N. Am. Deer Registry, Inc. v. DNA Sols., Inc.*, No. 4:17-CV-00062, 2017 WL 2402579, at \*8 (E.D. Tex. Jun. 2, 2017).

<sup>21</sup> See “The world’s most valuable resource is no longer oil, but data.” *The Economist* (May 6, 2017), available at <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>

<sup>22</sup> Several high-profile cases have involved so-called “insider threats” where an employees has taken software or trade secret data to use at a competitor.

<sup>23</sup> See, e.g., *Sargent Fletcher, Inc. v. Able Corp.*, 110 Cal. App. 4th 1658, 1670 (2003) (“Evidence of independent derivation or reverse engineering directly refutes the element of use through improper means.”); *N. Am. Deer Registry, Inc. v. DNA Sols., Inc.*, 2017 WL 2402579, at \*7 (E.D. Tex. June 2, 2017) (trade secret is not misappropriated if there is reverse engineering or independent derivation).

<sup>24</sup> See *LivePerson, Inc. v. 24/7 Customer, Inc.*, 83 F. Supp. 3d 501, 514 (S.D.N.Y. 2015) (denying motion to dismiss trade secret claim where plaintiff demonstrated that it included confidentiality provisions and prohibitions against reverse engineering, infringing, or disrupting its technology, as well as confidentiality and limited-use license restrictions in its client agreements).

<sup>25</sup> Note that certain jurisdiction, notably California, place considerable restrictions on the terms of such agreements as part of prohibitions on non-compete clauses. See, e.g., Cal. Bus. & Prof. Code § 16600.

- (3) Review cybersecurity policies to limit the potential for unauthorized access to information that constitutes a trade secret; and
- (4) Ensure any departing employees have returned company materials and removed any sensitive information from personal devices.<sup>26</sup>

Ultimately, a trade secret is only protected so long as it remains a secret. Even with strict regulations in place, companies always run the risk that the information will become public.

## V. Patent vs. Trade Secret: Making the Right Decision for AI-Related Inventions

Even though trade secrets are important to protect AI-related intellectual property, there remain different advantages and drawbacks for both patents and trade secrets. The decision whether to patent or keep as a trade secret a given innovation thus represents an important strategic decision for any company.

As an initial matter, the decision between patents and trade secrets can be, but is not always, mutually exclusive. In some instances a company can file a patent on the public-facing part of a product, which cannot be kept as a trade secret because it is not secret. At the same time, the company can maintain as a trade secret certain manufacturing techniques or other innovations within the product that are not generally known.<sup>27</sup> In another strategy, the company may keep technology as a trade secret while simultaneously applying for patent protection by seeking non-publication of its patent application.<sup>28</sup> In this scenario, the invention could have trade secret protection for the period of time during patent prosecution, and then patent protection once the patent issues. Of course, the company would then be limited to the claims of the patent only.

For some AI-related inventions, it may be possible to either apply for a patent or keep the intellectual property as a trade secret. Here are some guiding factors to consider when making these kinds of critical decisions:

- (1) ***Is the innovation eligible for patent protection?*** Does the innovation satisfy the requirements of the Patent Act, including being patent-eligible subject matter under 35 U.S.C. § 101? If not, then patents are unavailable and trade secret protection is the best option. As discussed throughout this article, that can be the case with many AI-related innovations and technology.
- (2) ***Does the innovation comprise the type of information that can be kept secret as part of your business?*** If the innovation is readily discernable from the product itself or by other appropriate means, trade secret protection would be

---

<sup>26</sup> Conversely, to avoid trade secret liability, best practices must be observed when hiring and/or onboarding new employees who formerly worked for competitors.

<sup>27</sup> One potential pitfall to avoid in this instance is the requirement under patent law to enable one to practice the claimed invention. If knowledge of the contemplated trade secret is essential to practice what is claimed, then it likely needs to be disclosed in the patent application or it risks invalidity for lack of enablement under 35 U.S.C. § 112.

<sup>28</sup> See 35 U.S.C. 122 (describing circumstances where patent applicant can request its application not be published).



- unavailable. The trade secret in that instance would not be “secret.” Thus, patent protection would be the best option.
- (3) ***Is the innovation likely to become generally known soon?*** Trade secrets only protect information that is not generally known. If the innovation is one that competitors or academia is likely to be making public relatively soon, then trade secret protection is sub-optimal. Instead patent protection may be the best option.
  - (4) ***How likely is the patent able to withstand an attack in litigation?*** Even if the patent may be approved by the patent office, if you believe the patent is unlikely to withstand an attack in litigation, it may be better to keep the innovation as a trade secret so the underlying intellectual property does not have to be disclosed to the public.
  - (5) ***How hard would it be to determine that another company is practicing your invention?*** The purpose of a patent is to prevent others from practicing your invention. But if the invention is for an AI algorithm that runs on a server that cannot be observed by the public, it may be impossible to tell which, if any, competitors are infringing on the technology. This would make a patent less valuable. On the other hand, if it is possible to completely reverse engineer the invention, then a competitor can use that as a defense to any claims of trade secret misappropriation.<sup>29</sup>
  - (6) ***How quickly will the invention become obsolete?*** If the invention will become obsolete quickly, the length of protection that patents provide (and the cost and effort to file the patent), may not be worth the benefit.
  - (7) ***How quickly can the invention be commercialized?*** Conversely, if the invention will take a long period of time to monetize, the length of protection afforded by a patent will allow time for long-term investment and capitalization.
  - (8) ***How hard is to describe the invention?*** In order to be issued a patent, the filer needs to describe the invention which serves both to “satisfy the inventor’s obligation to disclose the technologic knowledge upon which the patent is based, and to demonstrate that the patentee was in possession of the invention that is claimed.” If an invention would be difficult or time consuming to describe in a way that would satisfy the patent requirements, a trade secret may be more appropriate.

---

<sup>29</sup> See e.g., *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470 (1974) (“A trade secret law ... does not offer protection against discovery by fair and honest means, such as by independent invention, accidental disclosure, or by so-called reverse engineering, that is, by starting with the known product and working backward to divine the process which aided in its development or manufacture.”). Different courts and jurisdictions have applied this so-called “reverse engineering” defense differently: some courts have not considered the time, expense, or effort needed to reverse engineer the trade secret while other courts have only allowed a reverse-engineering defense where the trade secret was “readily ascertainable through...reverse engineering.” Compare *Barr-Mullin, Inc. v. Browning*, 424 S.E.2d 226 (N.C. Ct. App. 1993) to *Midland-Ross Corp. v. Sunbeam Equipment Corp.*, 316 F. Supp. 171, 173 (W.D. Pa. 1970).

- (9) *Is the innovation worth patenting?* Patents cost time and money to prosecute and obtain. Not all innovations are worth that effort. For certain types of know-how, it may be more practical to utilize trade secrets to protect the innovation rather than filing a patent.

Trade secrets are a powerful tool for protecting AI-related innovations and are particularly well-suited to the field. But both patents and trade secrets offer powerful ways for companies to protect their intellectual property. Each can be effective in certain circumstances. In most cases, optimal protection strategies will involve a thoughtful use of both regimes.

\*\*\*

If you have any questions about the issues addressed in this memorandum, or if you would like a copy of any of the materials mentioned in it, please do not hesitate to reach out to:

**Jordan R. Jaffe**

Email: [jordanjaffe@quinnemanuel.com](mailto:jordanjaffe@quinnemanuel.com)

Phone: +1 415-875-6315

**Jared Newton**

Email: [jarednewton@quinnemanuel.com](mailto:jarednewton@quinnemanuel.com)

Phone: +1 202-538-8108

**Patrick Curran**

Email: [patrickcurran@quinnemanuel.com](mailto:patrickcurran@quinnemanuel.com)

Phone: +1 617-712-7103

**Anil Makhijani**

Email: [anilmakhijani@quinnemanuel.com](mailto:anilmakhijani@quinnemanuel.com)

Phone: +1 212-849-7334

**Zack Flood**

Email: [zackflood@quinnemanuel.com](mailto:zackflood@quinnemanuel.com)

Phone: +1 415-875-6419