CONSIDERATIONS FOR USING PATENTS AND TRADE SECRETS TO PROTECT INNOVATIONS IN ARTIFICIAL INTELLIGENCE

Whether and to what extent technology in new and developing areas can or should be protected through patent, trade secret, or other areas of the law will depend, among other factors, on the objectives and resources of the innovator, the specifics of the technology at issue, and whether a particular legal doctrine is well-suited to protect the relevant technology. In the case of Artificial Intelligence,[1] significant investment from private enterprises and government agencies has accelerated the pace of innovation and expanded the reach of AI to the point where it no longer is a concept of science fiction or a niche technology in particular industries. Our ever-growing adoption of AI has implications for how we work, how we engage in commerce, and how we interact in our daily lives with each other.[2] At the same time, we are only starting to assess the implications AI may have on our legal relationships, and how we can best protect intellectual property interests in AI innovations. Of the forms of intellectual property available to protect AI, we focus here on patents and trade secrets. We provide an overview of those areas of the law and set forth factors one should weigh in assessing which of those protections (or a combination) may be available or preferable, including the nature of the technology, the risks involved, available budget, and overall business objectives.

Overview of Patents and Trade Secrets

Patents. A patent grants a patentee the legal right to exclude others from making, using, offering to sell, selling, and importing into the United States any invention claimed in the patent for a period of years. To be granted a patent, the patentee is required to file an application with the Patent and Trademark Office that, once published, publicly discloses the invention for which a patent is being sought whether or not the patent actually issues. The application process typically takes a minimum of 18 months, which does not include the time

[1] There is no generally accepted definition of AI. For purposes of this discussion, AI "can be understood as computer functionality that mimics cognitive functions associated with the human mind (e.g., the ability to learn)" U.S. Patent and Trademark Office, "Public Views on Artificial Intelligence and Intellectual Property Policy," at iii (October 2020), https://www.uspto.gov/sites/default/files/documents/USPTO_AI-Report_2020-10-07.pdf ("PTO Comments on AI") (footnote and citations omitted). AI may include various components, including the data used to train the system, the software algorithm that learns from the training data and that enables the technology to respond to new inputs, and processes, systems, and methods that implement the algorithm.

[2] AI is a widely used in various areas, including speech recognition, language translation, and visual detection. *See generally, e.g.*, U.S. Patent and Trademark Office, Chief Economist IP Data Highlights, "Inventing AI: Tracing the diffusion of artificial intelligence with U.S. Patents," at 2 (October 2020) (using AI system to provide an AI patent landscape, noting that "AI is poised to revolutionize the world on the scale of the steam engine and electricity."); *see also* Stanford Artificial Intelligence Index Rep. 2019, at 5 https://hai.stanford.edu/sites/default/files/ai_index_2019_report.pdf ("Globally, investment in AI startups continues its steady ascent. From a total of $1.3B raised in 2010 to over $40.4B in 2018 (with $37.4B in 2019 as of November 4th), funding has increased at an average annual growth rate of over 48%"); *id.* ("58% of large companies surveyed report adopting AI in at least one function or business unit in 2019, up from 47% in 2018"); *See* American Artificial Intelligence Initiative: Year One Annual Report (Feb. 2020) at 1 ("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.") https://www.whitehouse.gov/wp-content/uploads/2020/02/American-AI-Initiative-One-Year-Annual-Report.pdf; *See* http://vibrancy.aiindex.org/ (providing data on variety of parameters such as (but not limited to) research and development, education, publications, conferences, investment for countries all over the world).

and cost of drafting the application. If the application is granted, the patent issues publicly with the claims and disclosures approved by the Patent Office.

In order to have a patent issue, the patentee has to satisfy all of the requirements set forth in the patent statute and case law interpreting the statute. The specifics of those requirements and all of the hurdles one has to overcome to have a patent issue are beyond the scope of this discussion. At a high level, those requirements include that the invention[3] claimed in the patent has to be directed to patent-eligible subject matter, and it has to be novel, nonobvious, and useful. The patent has to include a disclosure that sufficiently describes the invention such that members of the public can discern what is patented. The disclosure also must at least enable one of ordinary skill in the relevant technology to be able to practice the invention without having to undertake undue experimentation. Put differently, your patent has to teach the very people you may be competing against how to practice your invention. Under current law and leaving aside technical matters that may affect the term of a patent, a utility patent expires 20 years after the filing of a non-provisional application.[4]

Distinguishing between patent-eligible subject matter and patent-ineligible subject matter has been a hotly litigated issue over the past several years. It is an important inquiry for purposes of determining whether to pursue a patent strategy to cover an innovation. The patent statute provides that patents can be granted to anyone who invents "any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof". 35 U.S.C. § 101. For an invention to be patentable, therefore, it has to be a process, machine, manufacture, or composition of matter. As a result, information that may be critical to the success of a commercial enterprise—like pure data—is not, standing alone, patentable because data, even if new, do not fall within one of those four categories. In addition, to determine patentability, one also has to determine whether the invention falls within the scope of a judicially-created exception to patentable subject matter. Those exceptions include abstract ideas (*e.g.*, concepts, mathematical algorithms, mental processes), laws of nature, and natural phenomenon. *See generally Alice Corp. v. CLS Bank International*, 573 U.S. 208, 221 (2014) ("generic computer implementation" failed to "transform" abstract idea of "intermediated settlement" into a patent-eligible invention); *Mayo Collaborative Servs. v. Prometheus Lab., Inc.*, 566 U.S. 66 (2012).[5] A full discussion of the current state of the law concerning patent eligibility is well beyond the scope of this presentation. We note here only that in assessing a strategy for protecting AI technology, attention must be paid to whether the technology concerns patent-eligible subject matter because software-based patents (and medical diagnostic technologies) have been materially impacted by decisions concerning patent-eligibility over the past several years. *See generally, e.g.,* Ben Hattenbach and Gavin Snyder, *Rethinking the Mental Steps Doctrine and Other Barriers to Patentability of Artificial Intelligence*, 19 Colum. Sci. & Tech. L. Rev. 313, 319–21 (2018) ("On a single day in September 2014, five different decisions invalidated software patents under *Alice*. There were as many or more invalidations

[3] Patents often claim more than one invention. For ease, we refer here to the invention as a singular term.

[4] We assume a utility patent filed after June 8, 1995. *See* 35 U.S.C. § 154 (term of utility patents). Design patents are not addressed here. *See* 35 U.S.C. § 173 (term of design patents).

[5] Under the framework set forth in *Alice/Mayo*, if in a first step the claims are found to be directed to patent-ineligible subject matter, the claims are reviewed in a second step to see if they contain an inventive concept sufficient to "transform" abstract idea into patent-eligible invention.

under § 101 on that one day than in any single *year* between 2007 and 2011. Since *Alice*, claims of more than 500 separate patents have been found invalid under § 101.") (emphasis in original)(footnotes omitted); *Purepredictive, Inc. v. H20.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) (invalidating patent directed to AI predictive technology because it covered "mental processes"); *Blue Spike, LLC v. Google Inc.*, No. 14-CV-01650-YGR, 2015 WL 5260506, at *1 (N.D. Cal. Sept. 8, 2015), *aff'd*, 669 F. App'x 575 (Fed. Cir. 2016) (dismissing claims concerning patent directed to AI for assessing whether music contained a cover of a copyrighted song, because patent claims involved mental process of "listening" to a song and recognizing it as a cover).

As a result, pursuing a patent strategy for the software component of AI if the claims are found to be unsustainable poses a risk that there will be public disclosure of anything described in the patent. Moreover, trade secret protection is unlikely to be available for the disclosed technology.

Notwithstanding the burden of satisfying patentability requirements, there are significant advantages to obtaining a patent. Indeed, in the area of AI, market participants plainly see the merit of obtaining patent protection. *E.g.*, U.S. Patent and Trademark Office, Chief Economist IP Data Highlights, "Inventing AI: Tracing the diffusion of artificial intelligence with U.S. Patents," (October 2020) (between 2002-2018, the number of AI patent applications increased by more than 100% and "the share of all patent applications that contain AI grew from 9% to nearly 16%); F. DeCosta and A. Carrano "Intellectual Property Protection for Artificial Intelligence," https://www.finnegan.com/en/insights/articles/intellectual-property-protection-for-artificial-intelligence.html (Aug. 30, 2017) (noting that in a five-year period, PTO saw a "500 percent increase" in "patents issuing to class 706, a classification exclusively designated for AI data processing systems.")

Significantly, patents provide strong protection if there is concern that others could independently derive the same invention or reverse engineer the invention. Reverse engineering or independent derivation are not defenses to a claim of patent infringement. A competitor will still infringe your patent as long as its product practices all of the limitations of at least one of your patent claims, even if the competitor independently developed its technology with no knowledge of your patent. A competitor's ignorance of a patent may negate a claim of willfulness, but it would not alleviate liability, which could result in recovery of damages or equitable relief, such as an order barring import of an infringing item.

Patents also can establish one as a market-leading innovator worthy of top talent and investors. Indeed, business partners may look to a patent portfolio as an indication that their investment in a venture is appropriately valued and has some level of protection.

Further, once a patent issues, the invention claimed in the patent is protected without having to undertake potentially considerable expenses in maintaining secrecy. While there are costs incurred in applying for a patent and periodic maintenance fees (*e.g.*, 37 C.F.R. 1.20(e)-(g)), those may pale in comparison to the significant expense and burden necessary to maintain secrecy of certain innovations. A disloyal employee, for example, may cause a variety of troubles, but taking already-patented technology would not risk the loss of the entire value of the intellectual property.

Trade Secrets. In contrast to patents, trade secrets do not have a subject matter eligibility requirement and there is no need to publicly disclose the trade secret vis-à-vis a lengthy and expensive application process. To the contrary, one must be vigilant in maintaining confidentiality in order to claim protection under trade secret laws. Indeed, there are only two requirements for information to be a "trade secret" under the Defend Trade Secrets Act: (i) the "owner" of the trade secret has to take "reasonable measures" to keep the information "secret;" and (ii) "the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information." 18 U.S.C. § 1839(3) (definitions, Defend Trade Secrets Act).[6] As long as—and ***as soon as***—those two requirements are met, any "forms and types of financial, business, scientific, technical, economic, or engineering information . . . whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing" can be a trade secret. *Id.* In short, the subject matter that is eligible for trade secret protections is vast and those protections can attach immediately.

Trade secret protection thus can apply to information that cannot be protected by patents (like customer lists and pure data). There is no requirement that information has to be novel in order for it to be a trade secret. And unlike patents, trade secrets do not expire after any particular time period. Rather, a trade secret "expires" when it is disclosed. Moreover, though one cannot obtain a patent by teaching the public only what does ***not*** work, that information may have economic value and thus may be protected as a trade secret, because competitors could use that information to save time and money in research and development. *See, e.g., Genentech, Inc. v. JHL Biotech, Inc.*, No. 18-CV -06582 WHA, 2019 WL 1045911, at *19 (N.D. Cal. Mar. 5, 2019) (acknowledging that "negative know-how" is viable as a trade secret because it could "confer [Defendants] the benefit of steering clear of fruitless development pathways, thereby saving precious time and resources."); *Cinebase Software, Inc. v. Media Guar. Tr., Inc.*, No. C98-1100 FMS, 1998 WL 661465, at *1 (N.D. Cal. Sept. 22, 1998) ("Negative research can be protectable as a trade secret," but finding Plaintiff's designation of what did and did not work "too nebulous . . . to qualify for trade secret protection").

That is not to say that trade secrets have no disadvantages or risks. There are three principal risks in relying on trade secret protection. First, failing to take "reasonable measures" to maintain confidentiality can cause one to lose trade secret protection. Second, even if one takes reasonable measures, there is the risk that disclosure will occur anyway, whether through inadvertence or misappropriation. Third, a critical risk to consider with respect to trade secret protections is whether a competitor will be able to "reveal" a trade secret through

[6] The effective date of the Defend Trade Secrets Act is May 11, 2016. The DTSA applies to misappropriation of a trade secret that occurred on or after that date, even if the trade secret came into existence beforehand. The statute defines "misappropriation" to include the "use of a trade secret" acquired through improper means, 18 U.S.C. § 1839(5). As a result, even if a trade secret was wrongfully acquired before May 11, 2016 but used after that date, one could allege a claim under the DTSA. In any event, because trade secret law is also a matter of state law under state versions of the Uniform Trade Secrets Act or the state's common law (*e.g.*, New York), practitioners should check individual state laws to assess the viability and advantages of pleading claims under state trade secret laws.

reverse engineering or independently derive the same protected information. If that occurs, the owner of the trade secret may have no remedy for trade secret misappropriation. *See, e.g.,* 18 U.S.C.A. § 1839 (6) (excluding from the definition of "improper means" in the context of misappropriation "reverse engineering, independent derivation, or any other lawful means of acquisition"); *KT Grp. Ltd. v. NCR Corp.*, No. 15 CIV. 7482 (PGG), 2018 WL 11213091, at *12 (S.D.N.Y. Sept. 29, 2018) ("'[T]rade 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 its development or manufacture.'") (quoting *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 476 (1974)).

Importantly, though there may not be the same upfront costs in securing trade secret protection as there is in securing a patent because there is no lengthy application process for trade secrets, costs can be considerable in maintaining a trade secret. "Reasonable measures" necessary to maintain secrecy over the "secret sauce" can vary depending on the circumstances, such as the technology involved, the resources of the owner of the trade secret, ways in which the trade secret can be accessed (*e.g*., electronically or only by passing physical barriers), and the number of individuals with access to the trade secret. Measures to protect the secrecy of the information could include physical or electronic means, limiting access through password-protected protocols or encryption, and ensuring that any transaction involving any trade secret include confidentiality/non-disclosure agreements. Remaining vigilant about eliminating or mitigating the risk of disclosure, and having a fluid and sizable workforce adopt that same vigilance, can tax even the most resourceful entities. One may not be aware that steps taken to protect the trade secret are insufficient—do not qualify as "reasonable measures"—until the issue is litigated and the trade secret is potentially lost through public disclosure in court documents.

Developing a Strategy For Protecting AI Using Patents and Trade Secrets

The advantages and disadvantages associated with protecting technology under patent and trade secret laws are particularly relevant with respect to software-based technology such as AI.[7] As noted above, to obtain a patent, one must satisfy several requirements, including patent eligibility, and important components of an AI system, like a set of data, are unlikely to be patentable. Moreover, AI-derived inventions may not be patentable because patent protection is limited to inventions made by natural persons.[8] To the extent an AI system itself assists in innovations, companies must exercise care in selecting the technology to patent and ensure proper identification of the correct (human) inventors who contributed to conception and reduction to practice of the invention. In contrast, trade secret protection is available to

[7] In the recently published PTO Comments on AI, half of the respondents indicated that existing intellectual property and other laws, including patent, trade secret, copyright, and contract were adequate to address issues relating to AI. https://www.uspto.gov/sites/default/files/documents/USPTO_AI-Report_2020-10-07.pdf. Though copyright laws are not addressed here, it should be noted that software also can be protected under copyright laws to the extent it includes an original expression. As with patents, under current copyright laws, "[t]o qualify as a work of 'authorship' a work must be created by a human being." Compendium of U.S. Copyright Office Practices, § 313.2 (3d ed. 2017). So works wholly created by AI are not copyrightable, though expressive aspects of the software and databases used in the AI system may be protectable under copyright.

[8] *See generally https://www.uspto.gov/sites/default/files/documents/16524350_22apr2020.pdf*; at 3-5.

the owner of the trade secret, who can be an entity or a natural person who takes reasonable measures to protect secrecy.

As indicated above, patent protection is a good candidate for covering technology that is certain or likely to be considered patent eligible, may be reverse engineered or independently derived, will take time to commercialize, will not be replaced in the short term, and/or that is important for attracting investors or business partners. For instance, hardware components of an AI system such as specialized sensors or innovations in computer processors are good candidates for a patent strategy because those components are not likely to raise a patent eligibility issue.[9] If there is a meaningful risk that a component of AI can be reverse engineered or independently derived, seeking patent protection may be the best option for protecting the innovation. Further, because patents have a 20-year term, they allow one to exclude others from using the technology during the time needed to establish sales or licensing. If a technology will soon be obsolete, it may not be worth going through the patent process, but if one has several years to build market share and recoup the investment made in developing the technology, obtaining a patent makes economic sense. Of course, if front-end capital is very limited, patenting may not be an option and trade secret protection may be the best or only option to protect the technology, at least in the first instance. The upfront patent costs one should consider in making this assessment include not only costs in applying in the U.S. but also in other key countries and regions as patents have jurisdictional limits and AI is being developed, implemented, and marketed all over the world.

Moreover, it may be more difficult for investors and other potential business partners to value a company's trade secrets as compared with a patent portfolio. Patents are publicly available and so investors and business partners can access and analyze the patents without taking on additional obligations through nondisclosure agreements and without the patent owner taking on additional risks of disclosure. It may be difficult for potential business partners to fully understand the contribution the trade secret makes to the business bottom line, and to gauge the risk that a future disclosure will occur or that a competitor will independently derive the same technology. By the same token, it may be difficult for the owner of the trade secret to bear the additional risk of disclosure arising from sharing the trade secret with potential business partners, even with non-disclosure agreements in place.

Trade secret protection is an attractive option where the technology cannot be patented and where reverse engineering or independent derivation is not possible or is cost-prohibitive. In addition, if there is rapid development in the relevant field such that the technology of today will be replaced by tomorrow, the long-term coverage provided by patents may be of little value. Under those circumstances, the better option may be to protect what is economically valuable now as a trade secret and replace or supplement it as new innovations develop.

[9] AI systems can comprise several different technologies. *See* USPTO Office of the Chief Economist, IP Data Highlights, "Inventing AI: Tracing the diffusion of artificial intelligence with U.S. Patents," at 3-4 (October 2020) (describing eight component technologies that can comprise an AI system, including knowledge processing, speech recognition, hardware, evolutionary computation, natural language processing, machine learning, vision/image recognition, and planning and control).

Importantly, taking "reasonable measures" to maintain secrecy may be particularly difficult in areas involving software development, like AI. Technology employees and independent contractors who work on software development are highly skilled and may leave to work for a competitor. In addition, software can be copied or downloaded without the need for specialized equipment. Further, it may take years to discover that a breach has occurred, and even after detecting a misappropriation, obtaining relief can be challenging, including if it will be difficult to describe the trade secret with sufficient specificity. *See*, *e.g*., *Zirvi v. Flatley*, 433 F. Supp. 3d 448, 465 (S.D.N.Y. 2020) (dismissing misappropriation claim because plaintiffs "failed to identify their alleged secrets with 'sufficient particularity' in order to apprise the defendants and the Court what information contained in the alleged negative trade secrets is truly secret and what information is not."); *AlterG, Inc. v. Boost Treadmills LLC*, 388 F. Supp. 3d 1133, 1146 (N.D. Cal. 2019) (allegations failed to "describe the subject matter of the trade secret with sufficient particularity to separate it from matters of general knowledge in the trade or of special persons who are skilled in the trade."). As part of a trade secret strategy, owners of trade secrets should consider identifying their trade secrets in the ordinary course, not just when litigation arises. In addition to keeping the trade secret owner prepared for litigation, such a practice also will allow for consistent notice to employees as to which information requires particular care.

For all of the foregoing reasons, and given the fact that AI systems can comprise different technologies (*see above*, note 9), AI developers may find a strategy that uses patents ***and*** trade secrets—and other protections, such as copyright and contract—particularly useful: [10]

First, AI systems are likely to be quite difficult to reverse engineer in their entirety, as the algorithm can be a "black box," though that risk may increase as computing power increases. As a result, trade secret protection remains an option for important aspects of AI technology.

Second, trade secret is particularly attractive for aspects of AI that may not be patent-eligible, like the data used to train the system. A patent can still cover significant aspects of AI technology (like the hardware, processes, and methods used by the AI system), while trade secrets can continue to cover ongoing and undisclosed research and know-how.

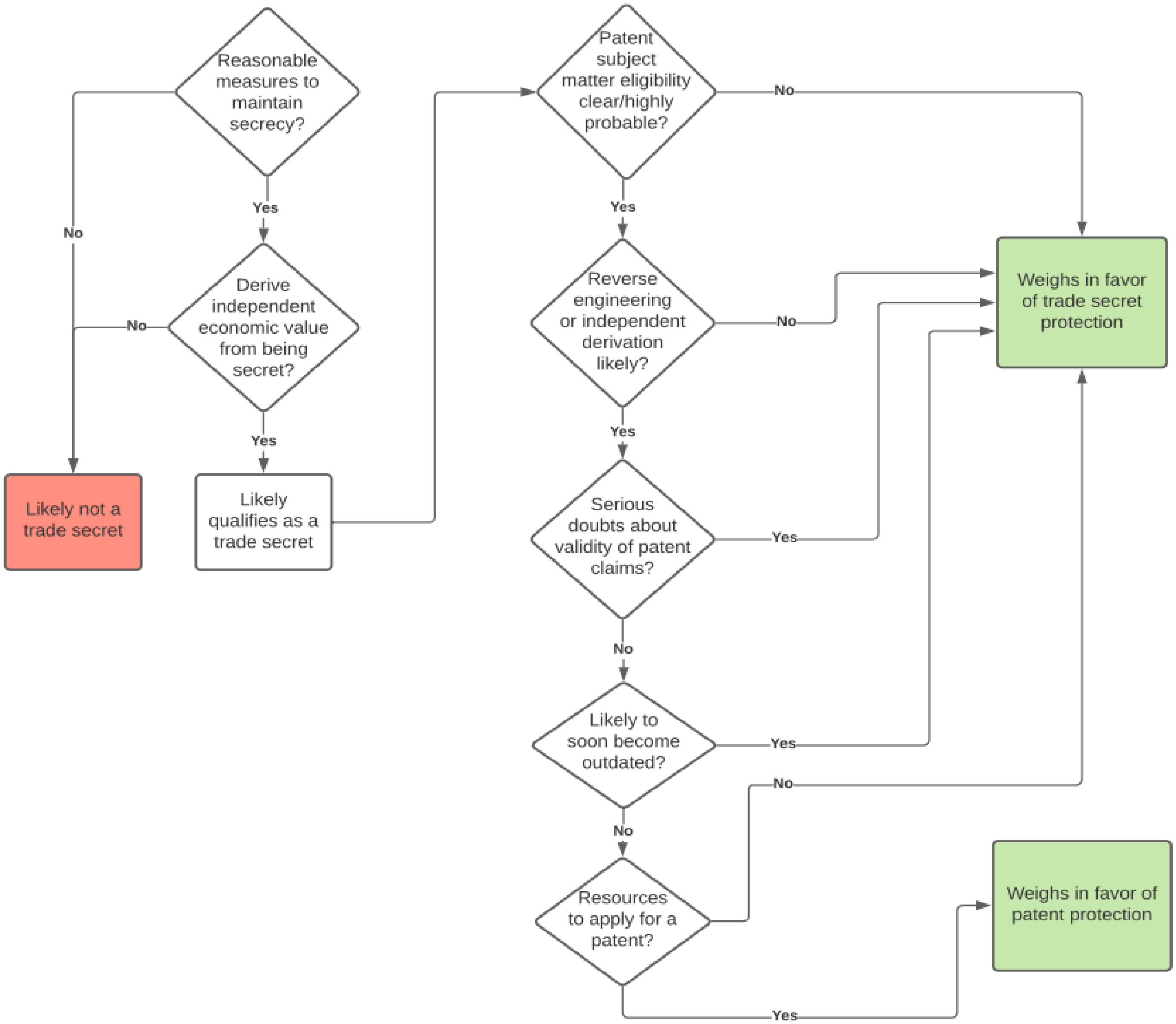
Third, even if one chooses to focus on a patenting strategy, trade secret protection is still highly relevant. Prior to filing a patent application, research supporting the application may be protected as a trade secret. After filing the patent application, trade secret protection still is useful for covering anything that was not disclosed in the application and any ongoing research that may contribute to additional patents.

Fourth, there is likely to continue to be rapid development of AI technology and therefore the innovation today may be replaced or obsolete by tomorrow. Thus, obtaining patent protection for all aspects of an AI product may not be worthwhile and taking steps to treat innovations as trade secrets as soon as they develop is a sensible way to protect and potentially quickly monetize the technology.

[10] For additional discussion of these issues, *see also*, *e.g.*, https://www.jdsupra.com/legalnews/april-2020-the-increasing-importance-of-64465/; "Protecting Artificial Intelligence IP: Patents, Trade Secrets, or Copyrights?" https://www.jonesday.com/en/insights/2018/01/protecting-artificial-intelligence-ip-patents-trad (Jan. 2018).

Fifth, if one does not have the resources needed to patent an invention (which may require filing several patent applications in different countries), taking steps to keep the innovation secret can provide some measure of protection in the first instance.

In sum, determining whether to protect an innovation through patent or as a trade secret is heavily dependent on the circumstances. We have identified some factors to consider in choosing an appropriate strategy. For ease of review, we have included the following diagram to capture some of the considerations in an accessible format. However, particular cases may involve other factors. Each decision point in the diagram includes complex assessments that are beyond the scope of this presentation. Finally, the diagram is not intended to prescribe a specific order in which to consider each factor. Rather, factors may be considered simultaneously or at different stages—for example, as a practical matter one may consider the risk of independent derivation at the same time as, or before, considering patent subject matter eligibility:


Reasonable measures to maintain secrecy?
No
Yes
Derive independent economic value from being secret?
No
Yes
Likely not a trade secret
Likely qualifies as a trade secret
Patent subject matter eligibility clear/highly probable?
No
Yes
Reverse engineering or independent derivation likely?
No
Yes
Serious doubts about validity of patent claims?
Yes
No
Likely to soon become outdated?
Yes
No
Resources to apply for a patent?
No
Yes
Weighs in favor of trade secret protection
Weighs in favor of patent protection