MAYER·BROWN

Legal Update
December 1, 2017

Protecting the Innovations That Protect Us—Intellectual Property Protection Strategies for Connected and Autonomous Vehicles

Introduction

The technologies necessary to fuel the development of connected and autonomous vehicles ("CAVs") are numerous and come from a number of different players. Traditional automotive companies and their suppliers are working with technology companies to combine and adapt existing technologies to the rigorous demands of the auto environment. In addition, substantial resources are being invested by all players to develop new capabilities and to integrate them into a cohesive product. These new technologies include sensor technologies, battery recharging and storage technologies, connectivity and security measures, computer processing capabilities, and software applications with artificial intelligence to continuously improve decision algorithms.

Both the breadth of capabilities and level of financial investment are substantial. Companies cannot rely on the traditional model of a supplier wholly funding the development of proprietary technology and selling a completely integrated system to the manufacturer while retaining all rights to the underlying IP. Nor can companies count on a manufacturer bearing all the costs of development, retaining all rights to the underlying IP created by a third-party supplier and preventing that supplier from leveraging that knowledge in other relationships. Neither model is sufficient to meet the incredible amount of investment required to bring the next generation of automobiles to market. It is not surprising, then, that there is a rise in co-development agreements, strategic partnerships, joint ventures and acquisitions of smaller technology companies by larger suppliers to provide a more integrated offering. With those models come new ways of protecting and allocating rights to IP that must:

i. reflect the allocation of design and development responsibilities and risks borne by each party to the collaboration, including overall integration responsibility, responsibility for design defects, costs of recall and product liability issues; and

ii. recognize the need for continued collaboration and future access to underlying components of the jointly developed product to enable continuing improvements and cybersecurity defense given the rapid change in both the technology itself and the regulatory environment that is still adapting to these new capabilities.

This more collaborative approach requires that the parties carefully negotiate both the sharing of costs and the sharing of rights to the developed technologies in a manner that meets their individual business requirements, is proportionate to the risks borne by each party and still allows sufficient sharing so that evolving technologies can continue to work seamlessly—both when initially integrated into the final product and as the resultant product is

improved to adapt to changing customer and regulatory requirements. To address those concerns effectively and to make sure that those carefully negotiated arrangements are enforceable, each party must have strategized in advance about how to best protect its underlying IP contributions.

Yet at the same time that the connected and autonomous vehicle industry has grown in prominence, changes in IP laws have created more uncertainty about the best way to protect new innovations. For example, patent protection for certain types of inventions—particularly those involving software—has become more difficult to secure. Meanwhile, new federal trade secret laws offer the potential for enhanced protection but remain relatively untested.

The best IP protection strategy for any given CAV development effort will thus depend both on the type of technology at issue and whether that technology was developed independently, collaboratively or as part of a joint venture. In addition, how each party's contribution is or can be protected will influence the parties' development of a sharing strategy. These concerns may impact terms such as whether rights to use the technology are transferable to third parties, whether information underpinning the resultant technology may be shared, and whether and at what cost rights to future derivative products created by one party after the collaboration has ended may be shared.

Patents: Despite Some Challenges, a Viable Means for the CAV Industry

Patents remain a strong option to protect many kinds of inventions. And because the allocation of patent rights can be agreed upon between the parties via contract, patents generally will offer the best form of protection in a collaborative environment. This is particularly true if requirements for extensive information sharing with a number of component suppliers, system integrators or regulators are present. Under such circumstances, the public disclosure requirements of the patent process impose few drawbacks, while trade secret protection may require confidentiality measures that are difficult to maintain in practice. Moreover, parties to a joint venture or collaboration agreement can precisely define what the expected contributions of each participant will be to the overall development effort and allocate patent rights accordingly.

Nevertheless, the parties should be careful in deciding how they will allocate patent rights flowing from their development efforts—especially when one contributor focuses on hardware development efforts and another focuses on software development efforts. As explained below, there are additional risks and hurdles associated with protecting software with patents. Companies seeking to protect software using the patent system should have a clear strategy in mind for addressing these challenges. Software companies should also recognize that the patent rights that they may receive from a collaboration may be of less value than the hardware-based patent rights stemming from the work of hardware developers. Accordingly, an allocation of patent rights based solely on who produced the patentable IP may not be appropriate and may not sufficiently compensate software developers for their contributions.

In such cases, the parties may need to consider other ways of sharing control and rights to patentable IP. A joint venture entity created to hold all rights in the co-developed property is one potential option. A joint venture will have the rights to grant licenses to each party to use, and potentially license, the joint venture's IP, thereby resolving the potentially unbalanced patent rights among individual contributors.

A company should also consider the extent to which technologies may be incorporated into standard-essential technologies. If development efforts in the industry lead to a standardized technical specification, a company will need to consider the pros and cons of contributing to

those technical standards. If a company decides to join a standard setting organization and make contributions to a proposed standard, it generally must agree to license its standard essential patents on fair, reasonable and non-discriminatory ("FRAND") terms. These obligations may require a company to license its standard essential patents to anyone interested in the technology—including competitors—at potentially very low rates.[1] The decision is further complicated by the fact that whether a patent is in fact "standard essential" is frequently a matter of dispute. The question is usually answered definitively only after protracted patent infringement litigation. Nevertheless, for technologies that are expected to become widely adopted, participation in standard-setting organizations may be preferable as it allows a company to have a voice in how the industry standards are developed and implemented.

PATENT SUBJECT-MATTER ELIGIBILITY CONCERNS FOR SOFTWARE TECHNOLOGIES

The poor grant rate for software-based patents at the USPTO, and the large number of "Section 101" challenges[2] to patents in district court, have prompted many to reconsider the use of patent protection, particularly for software algorithms designed to replicate a standard human response to object detection, as such concepts are easily framed as "abstract ideas." While patent protection remains a strong option for innovations that might be easily reverse engineered or that cannot be kept confidential due to regulatory requirements, trade secrets may be the better alternative to protect software algorithms. However, here too, a decision to seek, and a strategy to preserve, trade secret protection must be well-planned and executed in advance.

Trade Secret Protection for CAV Technologies

For companies developing software-based technology independently, trade secrets are an excellent alternative to patent protection. While patents require public disclosure, trade secrets protect intellectual property by obscuring technical developments. And where patents require years of back-and-forth discussions with the USPTO to obtain rights, trade secret rights can be obtained without any government involvement.

Trade secret protection applies to "information, including a formula, pattern, compilation, program, device, method, technique, or process."[3] The secrecy must generate "independent economic value," and the owner of a trade secret must take "efforts that are reasonable under the circumstances to maintain its secrecy."[4]

Unlike other forms of IP protection, which require registration before a government agency like the USPTO or the Copyright Office, trade secret protection can be claimed independently. For example, if a company's software meets the trade secret requirements, then the company can sue for trade secret misappropriation against an individual that acquires or discloses the trade secret under "improper means."[5]

Indeed, the recent enactment of the federal Defend Trade Secrets Act (DTSA) makes trade secret protection more attractive than ever by providing a federal cause of action for trade secret misappropriation that implicates interstate or foreign commerce.[6]

The DTSA allows for recovery of actual losses and for any unjust enrichment caused by the misappropriation or recovery of a reasonable royalty for any unauthorized disclosure of the trade secret.[7] Additional remedies include

injunctive relief,[8] exemplary damages for willful or malicious misappropriation,[9] and (under certain circumstances) attorneys' fees.[10]

Companies in the connected and autonomous vehicles industry have already begun to use the DTSA. For example, a self-driving car start-up filed suit in the Northern District of California against a ride-sharing service seeking to develop its own autonomous vehicle program alleging violations of the DTSA and the California Uniform Trade Secrets Act.[11] The case involves the supposed theft of over 14,000 highly confidential documents related to the start-up's LiDAR technology.[12]

ADVICE FOR TRADE SECRET PROTECTION

Although there is no formal process for registering or applying for trade secret protection, companies should create and adhere to a detailed protocol for identifying trade secrets and the steps to protect them. Thus, companies should craft a comprehensive trade secret portfolio management plan similar to what many companies already have in place for other IP assets such as patents and trademarks. The plan should outline a protocol for clearly identifying each trade secret and the steps taken to protect it, with systems in place to collect and catalog evidence of this protection.

Companies should think carefully about what procedures to put into place for protecting trade secrets. For example, consider requiring employees and third parties with access to confidential information, such as source code, to sign a confidentiality agreement.[13] Also consider limiting access to confidential information by requiring password access and by keeping track of any hard copies of confidential information.[14]

DRAWBACKS TO A TRADE SECRET-BASED STRATEGY

Trade secret protection offers an alternative path for companies that view the patent process as unappealing either because it is ill-suited for their technology or too expensive and time-consuming to pursue. Preparing a trade secret protection strategy at the outset of a project is critical, however, and companies may not be successful if they wait until litigation begins to claim that a particular piece of confidential information is a trade secret.

Trade secret protection will generally be of minimal value for technology that could be easily reverse engineered by a competitor without reliance on confidential information. Thus, companies focusing on hardware developments may find trade secret protection less valuable than patent protection. Trade secret protection also may not be suitable for innovations that require extensive disclosures to collaborators, or public disclosure to regulators or other government agencies. For these cases, patent protection may be the preferred option.

Furthermore, it will likely not be possible to seek both patent and trade secret protection for the same innovative concept. The public disclosure required in the patent application process sits in uneasy tension with the strict confidentiality requirements of trade secret law.[15] Therefore, companies should choose between a patent strategy and a trade secret strategy for each of their innovations.

In addition, the ability to protect IP as a trade secret is premised on maintaining confidentiality that may be in contrast to a practical need to share certain development characteristics with other third parties to be able to integrate the jointly developed product with other third-party-provided components, and the parties will need to agree on who can share, for what purposes and with whom. In the event that the control over the IP is to be shared, contribution to a joint venture that asserts trade secret protection and controls decisions regarding the IP may again be a solution.

The below matrix provides generalized guidance as to which IP strategy may be most appropriate for a given scenario:

Scenario	Software Technology	Hardware Technology
Independent Development	Trade secret protection may be more appropriate	Individualized analysis needed to determine best strategy
Joint Development	Individualized analysis needed to determine best strategy	Patent protection may be more appropriate

Conclusion

Intellectual property protections for the innovations driving many of the recent advances in CAVs are in a state of flux. The best intellectual property strategy to protect those developments will depend not just on the type of technology at issue but also on whether the technology was developed independently or as part of a collaborative effort. Nevertheless, with appropriate planning, a company or group of companies may successfully employ an intellectual property protection strategy involving both patents and trade secrets that maximizes its chances of protecting its innovations. In addition, when the technology is developed as part of a collaboration and for a use case that will require ongoing maintenance and development of the jointly developed technologies, a group of companies will need to consider structuring their relationship in a way that maintains protection but does not prohibit each party's continued development of its contributions to the joint product.

For more information about the topics raised in this Legal Update, please contact any of the following authors.

Clinton H. Brannon
+1 202 263 3440
cbrannon@mayerbrown.com

Bryan C. Nese
+1 202 263 3266
bnese@mayerbrown.com

Marjorie H. Loeb
+1 312 701 8833
mloeb@mayerbrown.com

The authors also wish to thank summer associate Marie Rehg for her research contributions to this article.

Endnotes

1 *See, e.g.,* IEEE-SA Standards Board Bylaws § 6.2 (stating that licenses are to be made available "to an unrestricted number of Applicants on a worldwide basis without compensation or at Reasonable Rates").
2 An alleged infringer may assert that a patent is invalid pursuant to 35 U.S.C. § 101 for failing to claim patentable subject matter. For example, a patent claim is invalid pursuant to Section 101 if it merely claims an abstract idea, even if the use of the abstract idea is limited to a particular technological environment. *See Alice Corp. v. CLS Bank Int'l.,* 134 S. Ct. 2347, 2352 (2014).
3 UTSA § 1(4) (Unif. Law Comm'n 1985).
4 UTSA § 1(4); 18 U.S.C. § 1839 (2012).
5 18 U.S.C. § 1839(5); UTSA § 1(2). But reverse engineering is not considered an "improper means." 18 U.S.C. § 1839(6)(B); UTSA § 1, cmt. 2.
6 18 U.S.C. § 1836(b)(1).
7 18 U.S.C. § 1836(b)(3)(B).
8 18 U.S.C. § 1836(b)(3)(A).
9 18 U.S.C. § 1836(b)(3)(C).
10 18 U.S.C. § 1836(b)(3)(D).
11 *Waymo LLC v. Uber Techs., Inc.*, No 3:17-cv-00939 (N.D. Cal. Feb. 23, 2017) (ECF No. 1).

[12] *Id.*

[13] *See Cortz, Inc. v. Doheny Enterprises, Inc.*, 2017 WL 2958071 (N.D. Ill. July 11, 2017); *Liberty American*, 199 F. Supp. 2d at 1286.

[14] *See Arcor, Inc. v. Haas*, 842 N.E.2d 265, 271 (Ill. App. Ct. 2005) (finding measures beyond a confidentiality agreement, "such as limiting access to its customer information by computer password or keeping track of the hard copies of the information" might have led to a ruling that the plaintiff took reasonable efforts to keep information secret).

[15] *See Wellogix, Inc.*, 716 F.3d at 875 ("[A] patent destroys the secrecy necessary to maintain a trade secret only when the patent and the trade secret 'both cover the same subject matter.'").