MARCH 2023

DEVOTED TO LEADERS IN THE INTELLECTUAL PROPERTY AND ENTERTAINMENT COMMUNITY

VOLUME 43 • NUMBER 3

THE Licensing Journal®

Edited by Gregory J. Battersby and Charles W. Grimes

Wolters Kluwer

Praxis

Business Tech

Eugene Mar and Tom Pardini

Failures Are Valuable IP: Protect Your Startup's Negative Trade Secrets

Technology companies and start-ups are familiar with protecting inventions with patents, and protecting their secret formulas, source code, and algorithms as trade secrets. But tech companies may not be aware of another powerful form of IP protection in California known as "negative trade secrets," which are intended to protect a company's secret know-how gained from extensive research investment about what does *not* work.

Consider Thomas Edison's quote about his lightbulb experiments: "I haven't failed, I've just found 10,000 ways that won't work." Imagine that Edison's assistant quit and was hired by a competitor. The former assistant's "negative know-how" from Edison's 10,000 failed attempts would allow his new employer to start on attempt 10,001. But while a trade secret is a company's intellectual property, an employee's general knowledge, skill, and experience acquired in his or her former employment is not. Where does one draw this line? Does Edison's former assistant really have to re-try all 10,000 prior failures that he knows won't work? In a high-profile intellectual property case regarding self-driving technology (*Waymo v. Uber*), Judge Alsup asked rhetorically, "Is an engineer really supposed to get a frontal lobotomy before they go to the next job?" The answer to this question is obviously no—but companies have other ways to protect this information beyond employee lobotomies. Companies and employees should bear in mind some general best practices when protecting and navigating around negative trade secrets.

First, courts sometimes scrutinize the breadth of alleged negative trade secrets to determine if they prevent others from competing in a particular field altogether. The broader it is and the greater the preemptive effect, the more likely a court will refuse to recognize that negative trade secret. In one case, a court found that "Plaintiff's designation of 'technical know-how' regarding what does and does not work in . . . digital media management software is simply too nebulous a category of information to qualify for trade secret protection." The court criticized the plaintiff for failing to "identify any specific design routes," but seeking instead to prevent defendants from designing any software at all. Therefore, any company seeking to protect this type of IP should sufficiently narrow the negative trade secret's breadth so it doesn't overlap with an entire field or industry.

Second, negative trade secret claims most often succeed where a company can identify specific documents or data that was taken that includes negative knowledge. This specificity is likely what allowed Genentech's claims to go forward in a recent pharmaceutical case. Genentech included specific allegations that the defendants "downloaded and provided to JHL hundreds of confidential Genentech documents filled with proprietary negative know-how." JHL argued that its protocols differed from Genentech's, but the court said this did not foreclose JHL's possible use of Genentech's negative trade secrets. This negative know-how "would confer JHL the benefit of steering clear of fruitless development pathways, thereby saving precious time and resources." This means if a pharmaceutical manufacturer can identify data that was taken, which contained failed formulas, those failed formulas could be protectable negative trade secrets. And in a software context, claims for negative know-how misappropriation may require specific examples of the failed code that was taken.

Third, companies should bear in mind that courts sometimes enforce a negative trade secret as the flip side of a positive trade secret. In a case where a customer list was misappropriated, a court stated that "[i]f a customer list is acquired by lengthy and expensive efforts, which, from a negative viewpoint, indicate those entities that have not subscribed to plaintiff's services, it deserves protection as a trade secret." The court meant that by acquiring a list of those who *had* purchased, defendants had "acquire[d] a list which has already screened out uninterested consumers and thereby saved 'themselves comparable efforts in screening out those entities who declined [their] patronage . . .'" In other words, the

defendants acquired a customer list and could now avoid calling uninterested people—which the court characterized as a negative trade secret.

Below, we provide a list of general trade secret best practices with specific ones for negative trade secrets. Combining these lists can improve a company's chances of maximizing its IP protection.

General Trade Secret Tips

- Like the rules laid out by Tyler Durden in the movie *Fight Club*, the first and second rule of protecting a trade secret is "You do not talk about [the trade secret]." Keep it secret. Circulate trade secret information only on a need-to-know basis among employees or internal teams. Avoid distributing the trade secret to anyone who doesn't need to know about it, especially anyone outside the company.
- Prepare an information security policy, documenting basic policies regarding when employees may share confidential information outside the company and in what format. Define categories of information, such as public information, internal information, confidential information, and strictly confidential information.
- Conduct organized and formal trainings with employees on the meaning of trade secrets, how the company protects them from public disclosure, and how employees are obligated to help protect them. It is best practice to do this when onboarding new employees and to provide periodic reminders (at least annually) either individually or in group settings. It is also a good practice to provide documentation that the employees can sign to assert that they attended and understood the training.
- Add Confidential or Highly Confidential legends on internal documents that describe or reference trade secrets. Do not overuse these labels on documents that don't warrant them; such overuse can cause employees to ignore the label entirely and can cause courts to discount their significance.
- Implement a company VPN network so employees are working with copies on company servers and not storing anything locally. VPNs also typically add a layer of encryption to transmission and can log access.
- Technology companies should use tools such as Github that log the key developments of their product, including versions of their source code. Ideally, this information should include what those developments are, when they happened, and who designed them.
- When onboarding employees, have employees certify that they are not bringing any trade secrets from their former employer, and train them in the company's information security policies, which should usually include signing a Non-Disclosure Agreement.
- Conduct exit interviews with departing employees, ensuring that all their equipment and documentation has been returned and that access to company databases has been revoked. Include a termination certification in employment agreements that is signed during the exit interview. The certification should state that the employee has not taken any confidential information or company devices, and that personal devices have been reviewed and cleared of all company trade secrets and confidential information (although such information should never be on personal devices regardless).
- If considering a merger or partnership with another company, try to limit the initial information to financial information, and only provide sensitive technical information if the potential partnership has progressed significantly. Always use a well-written Non-Disclosure Agreement.

Negative Trade Secret Tips

- Have a general practice of documenting all attempts, so that failed formulas, code, or implementation are documented along with successful ones. Include who worked on it and why it failed. Ensure any such documentation is well-protected within the company.
- Include a clause regarding the protection of negative trade secrets in any Non-Disclosure Agreement that your company signs—whether with an onboarding employee or a potential partner company.
- Include the concept of negative trade secrets in organized trainings, so employees understand that their obligation to keep proprietary information secret extends not

only to positive know-how, but negative know-how.

- If litigation occurs, describe the negative trade secret in specific terms. It's also a good idea to couple any negative trade secret with a positive formulation of the secret—if at all possible. For example, if trying to protect years of unproductive sales calls with potential customers who were not interested in your product, you should also choose to protect the customer list of those who *were* interested in the product. If the court looks askance at the negative secret, the positive one can be a great alternative.

This article was originally published on TechCrunch.

Eugene Y. Mar is a partner with Farella Braun + Martel LLP in San Francisco, leading the firm's Technology Industry Group. Eugene represents technology companies in intellectual property litigation, advising emerging companies on strategies for building and diversifying their intellectual property portfolios, and counseling clients on IP licensing and best practices for trade secret protection.

Thomas J. Pardini is a senior associate with Farella Braun + Martel LLP in San Francisco, representing clients in intellectual property litigation and other commercial disputes, with a focus on trade secret and patent infringement matters.