Trade Secrets: Practical Considerations

by Chad G. Clark | Aug 19, 2021 | Patents, Trade Secrets

In the final scene of *Raiders of the Lost Ark*, a worker wheels perhaps the greatest archaeological find in human history into an enormous government warehouse, where it is stashed among thousands of other crates, perhaps never to be seen again. Unlike the *Ark*, trade secrets that businesses are seeking to protect can't just be hidden away in a vault.

Trade secrets are often central to a company's value and, therefore must be used. This means they must be shared with employees and vendors, embedded in software, disclosed to regulators, and included in products. The fundamental dilemma of trade secrets is that while they derive their value from secrecy, at some point they must be disclosed, at least selectively. Thus, protection of trade secrets is not something to be undertaken lightly. It requires planning, strategic thinking, and a multi-dimensional approach. First, however, it's important to understand what a "trade secret" is.

What Is a Trade Secret?

For states adopting the *Uniform Trade Secrets Act* framework, a trade secret is defined as information that 1) "derives independent economic value" from not being generally known or readily ascertainable, and 2) is subject to "reasonable" efforts to maintain secrecy. As to this latter provision, the holder of a trade secret cannot pursue legal remedies unless reasonable steps have first been taken to prevent disclosure, and "reasonable" is determined in light of that secret's value to the holder.

For example, asking a court to award substantial damages or an injunction when the trade secret was maintained on an open network (or where the password used was "password") will likely net little more than an eye roll and a dismissal from the judge.

The NDA Trap

One of the first interactions a business has with a prospective vendor, investor, or collaboration partner is often a non-disclosure agreement (NDA). However, use of a standard NDA - without addressing trade secret aspects, specifically - may result in inadvertent trade secret disclosures.

To be enforceable, NDAs are usually tied to an expiration date, often 3-5 years after termination, after which the obligation to protect disclosed information ends. Some courts have ruled that allowing an NDA to expire is evidence that reasonable efforts to protect trade secrets have likewise expired. Fortunately, contracting parties can prevent this with language requiring the indefinite survival of obligations to protect trade secrets.

Employees and Data Security

A company is only as good as its people, and its trade secrets are only as secure as its data security practices. While trade secrets must be disclosed to certain employees, contractors or agents, people are fallible: employees leave, send emails, chat online, brag to friends at the bar, and lose their laptops. Thus, data security must be a cornerstone of trade secret protection, and employees should be steeped in security practices from Day One until their departure from the company.

Further, employment agreements and independent contractor agreements should contain robust, enforceable confidentiality clauses. And personnel should receive data security training early and often. This should include, a minimum, device control and password procedures; treatment of confidential information in internal and external communications; and hacking or data-mining risks and responses.

Supervisors at every level must be empowered to explain and enforce data security. Moreover, when an employee, contractor or agent leaves the company, they should be counseled on their continuing confidentiality obligations, to include their non-expiring obligations to protect trade secrets, as well as the requirement to surrender any trade secret or other confidential information in their possession. Finally, companies should employ compartmentalization methods to control disclosure risks when the inevitable happens and an employee loses their phone or has their account hacked.

Regulatory Potholes

Government contractors should be aware that the federal government may require the disclosure of certain trade secrets, putting these at risk of disclosure to third parties. For example, government agencies often require companies competing for defense contracts to detail their technical capabilities, disclose technical data and personnel qualifications, and justify their costs. These trade secrets may inadvertently be disclosed through the bidding process, or may even be subject to *Freedom of Information Act* (FOIA) requests.

To counter such risks, companies *must* label their trade secrets as such and include express declarations along with those labels that these trade secrets are exempt from such requests. Beyond these measures, however, FOIA disclosures must also be monitored for potential disclosure of trade

secret-related material, and those requests for FOIA-based disclosures must be opposed in court. The government's acquisition of certain data rights may also result in the inadvertent disclosure of trade secrets, so companies must think strategically about accepting government funding for their core technologies.

Similarly, for medical device or drug approval processes, the FDA requires manufacturing steps and processes, vendor lists and drug formulas all to be documented and disclosed. Accordingly, trade secrets that form a part of any regulatory filing must be identified up front, carefully grouped, and appropriately labeled. Trade secrets should not be threaded throughout a regulatory filing, but rather, kept in key technical sections, if possible. Those sections likely to be disclosed, such as those addressing safety and efficacy, should contain no trade secrets. Government-published summary documents should also be scrutinized for any trade secrets that may have been copied from confidential sections.

Trade Secrets and Patents

Unlike trade secret rights, patent protections are premised on public disclosure. It is therefore no surprise that the two are largely mutually exclusive means to protect an invention. However, further complications may arise if a company initially keeps an invention as a trade secret and then later opts for patent protection.

The novelty requirement for patent protection is key. Under patent law, prior art is anything in the public domain that discloses the invention, including a sale of (or in some cases even a confidential offer to sell) the invention. Such a prior art disclosure can include a company's *own* activity. This means that a product including that invention and sold to the public is considered prior art to a patent application filed for that invention.

Any sale (or offer to sell) marks the date from which a one-year window extends during which the company's own activities will not be considered prior art, so a patent application can be filed. However, if a trade secret is inadvertently disclosed by an employee or a government agency, this, too, starts the "clock," and the company has one year to get a patent application on file or else forfeits its ability to do so. Because of these factors, companies must carefully weigh whether trade secret protection is superior to patent protection for certain intellectual property (IP).

Conclusion

Maintaining trade secret protections may be one of the most complicated and crucial tasks facing companies. Moreover, trade secrets should not be considered in a vacuum, but contemplated as a part of a comprehensive IP strategy that evaluates the likely disclosure requirements and risks, the means to protect those secrets, and their relationship to patents and other forms of IP protection.

Contact:
Chad G. Clark
chad@martensenip.com
220-201-0051
Download vCard