Today's GENERAL COUNSEL

DEC/JAN 2015 VOLUME 11/NUMBER 6 TODAYSGENERALCOUNSEL.COM

DISCLOSURE AND NONDISCLOSURE

ISSN: 2326-5000

View our digital edition: digital.todaysgeneralcounsel.com


TOP SECRET

Protecting Trade Secrets with a Solid Nondisclosure Agreement

By Jake M. Holdreith and David A. Prange

Trade secret protection of company information has seen a popular resurgence, as patent protection has become less certain and patent enforcement more expensive. Courts are struggling to define what qualifies for patent protection, particularly in technologies such as computer software, biologics and biosimilars, and business methods. The uncertainty and additional investment that a company must make to secure and protect its patent rights may mean it is simpler and safer to protect its technology by keeping it secret.

A company must take "reasonable" steps to protect a trade secret in order to qualify for protection under the Uniform Trade Secret Act (UTSA), which is adopted in some form by almost all states. Recent case law suggests that reasonableness for a sophisticated company may require it to establish contractual obligations of secrecy with those who use or receive its trade secrets.

For example, in a 2012 Seventh Circuit case, *Fail Safe, LLC v. A.O. Smith Corporation*, the court suggested that sophisticated businesses should, at a minimum, use written disclosures to identify communicated trade secrets. According to the court, absent a written agreement and identification, a sophisticated business should not have an expectation that shared trade secrets will remain secret.

This development reinforces the importance of a specific written nondisclosure agreement if a company is disclosing its trade secrets or confidential information to others outside the company. Using a nondisclosure agreement is nothing new, but there are pitfalls, and the balance of this article provides suggestions for drafting to provide more certain protection.

Greater certainty leads to more predictability in the relationship. It also may lead to more effective enforcement should the relationship sour.

These suggestions are malleable, and how they can be applied depends on the relative bargaining positions of the parties, including their size and desire to share or receive confidential information.

In general, for greater certainty be more specific in defining the confidential information. Many times a party disclosing confidential information will define the scope broadly, believing that will provide more flexibility to protect its rights. But broadly defined rights may lead to confusion about what information is actually protected. This confusion may lead to a misstep in using that information. Instead, a company should consider a more narrow and specific definition, so people using the information understand what is protected.

Vague or ambiguous terms used to define the scope of a trade secret can compromise its protection.

The good reasons for specificity must be balanced against any difficulty in identifying each trade secret with particularity, especially when the agreement concerns information that may be in development and may change and grow over time. A best practice will attempt to define the protected information comprehensively, by category, and will also itemize specific known trade secrets to the extent practicable.

People providing and receiving confidential information are more likely to comply with an obligation to protect that information if they understand the obligation. A specific definition allows people to determine permissible uses for received information, and it gives a judge or jury comfort in imposing sanctions when it is clear that an actor should have known what was prohibited. By contrast, a broad definition may sweep in public information and can lead to confusion regarding what is and is not confidential information. This can be problematic when enforcing a breached obligation.

This confusion can also lead to accidentally disclosing confidential information without appropriate protection. Using a specific definition to identify confidential information allows all involved to recognize and use that information with greater certainty. Parties who are forthcoming in their treatment of information have a relationship that is not plagued by confidentiality questions. Clarity minimizes disputes.

If a dispute arises, a court (and a jury) is more likely to recognize and enforce confidentiality rights if those rights are specific. A broad definition invites an argument that the contract is unenforceable. Under the UTSA, as modified by the states, information may be a trade secret only if that information is not generally known (in other words, not public). There may be an argument that a broad term does not clearly identify the trade secret because it also captures public information. A court faced with a broad term that overreaches on a party's statutory right of protection may find the contract unenforceable because it is too vague or ambiguous.

In addition, a company may have greater difficulty convincing a jury that it has a protectable trade secret if the definition is overly broad. A broad definition of confidential information coupled with over-designation on the part of the disclosing company can, in the hands of good opposing counsel, be used to instill doubt that the asserted confidential information should be protected. A defendant can argue that the company seeking enforcement is trying to take from the public what should be rightfully available to all market participants. A defendant could also argue that it did not and could not have understood the obligations. Such arguments may appeal to a jury and create greater skepticism regarding whether any trade secret or confidentiality exists.

A lawsuit premised on a contract with a specific definition can also help to contain litigation costs when a company turns to enforce its rights. Several jurisdictions now require a plaintiff asserting trade secret claims to identify its asserted trade secrets early in the case. In California, for example, a plaintiff must identify its trade secrets with specificity before other discovery can commence. Early disclosure requirements are easier to enforce and comply with, and may result in fewer discovery disputes, if a party can rely on a specific definition based on the written agreement. A consistent identification of the trade secret or confidential information, from written agreement to litigation, can also protect a plaintiff from unnecessary discovery.

For greater certainty, also be specific about how long the information must be kept secret. The parties should agree to a period for protection based on how long it is actually needed, and that will depend on the industry and technology involved. For example, technology that advances rapidly may dictate a shorter nondisclosure period, while technology that relates to national security may require a longer period. Having a fixed period provides certainty to both parties. The disclosing party knows how long it has to keep track of its information that is in the hands of another party, and the receiving party knows how long it must be careful with the information that it has received.

The nondisclosure agreement should also address how information that a party considers confidential is identified as confidential. A first method for doing that is by category. A second is by labeling information exchanged as confidential with a brand or other legend.

Both methods have a related problem. Defining confidential information by categories can lead to a disagreement about whether a document's content is within one of the categories, and branding exchanged information is problematic because verbally conveyed information is hard to label, and compliance is not always perfect. A better practice is to identify protected information by category and a specific label. An agreement should include designated categories of information protected as confidential before the parties exchange documents or have discussions covered by the agreement. In addition, parties should consider including a labeling clause covering documents and communications. Documents, and each page of multiple-page documents, should be branded in some form (e.g. "Confidential information of [Party]").

Parties should discuss the applicability of any nondisclosure agreement at the beginning of any meeting, and after the meeting the disclosing party should consider providing a written identification of the confidential information disclosed during the meeting. This additional notice may eliminate ambiguity about whether discussions are confidential.

A company enforcing a nondisclosure agreement also will benefit in litigation by following the agreement's marking provisions. A defending party may challenge a claim that the plaintiff intended for the information to be confidential at the time of conveyance, and this claim is more easily rebutted if the conveying party labeled the information as confidential.

For greater certainty, include statements regarding the purpose for exchanging information, how the information may be used, or limits on who may review it. Including these terms provides guidance for a receiving company on how to maintain confidentiality. Identifying who may review confidential information, for example, allows a receiving company to establish barriers that prevent employees who have received confidential information from sharing it with other employees, thus potentially avoiding a claim that a person who received confidential information later used it improperly.

In summary, improving specificity in a nondisclosure agreement leads to greater predictability in the parties' relationship with regard to how information is handled, and in litigation if the relationship sours. The level of specificity necessarily is affected by the relative bargaining positions of the parties at the time they enter into a nondisclosure agreement, but in general more specificity allows parties to evaluate risk, a potential breach and whether subsequent litigation is prudent. ■

Jake Holdreith is a partner at Robins, Kaplan, Miller & Ciresi LLP. He counsels clients and tries complex lawsuits in areas including intellectual property, regulatory matters and constitutional issues. He handles cases in the United States, Europe and Asia.
jmholdreith@rkmc.com

David Prange is a trial lawyer and registered patent attorney at Robins, Kaplan, Miller & Ciresi LLP. He focuses on complex business litigation with an emphasis on intellectual property, including patents, trademarks, and trade secrets.
daprange@rkmc.com