



## Trade secret law: A brief guide for in-house counsel

Here are three basic features of trade secret law that every in-house counsel should know.

BY BEN BERKOWITZ, BRIGGS MATHESON  
AUGUST 18, 2016

Nearly every in-house lawyer will, at some point during his or her career, have to deal with issues surrounding confidential company information.

Understanding *when* information qualifies for **trade secret** protection, and *what* conduct amounts to actionable trade secret misappropriation, is critical to protecting the value of your company's intellectual property. Here are three basic features of trade secret law that every in-house counsel should know.

### What information does trade secret law protect?

---

Forty-seven states have adopted some form of the [Uniform Trade Secrets Act](#) ("UTSA"), with New York, Massachusetts, and North Carolina as the only exceptions. Under the UTSA, there is a two-prong test for determining whether information may be subject to trade secret protection. First, trade secret information must be information that "derive[s] independent economic value" from not being publicly known (*See, e.g.*, Cal. Civ. Code § 3426.1(d)). That is, the information is valuable *because* it is a secret that others, including competitors, do not possess. Second, the information must be "the subject of efforts that are reasonable under the circumstances to maintain its secrecy." (*Id.*) "The determination of whether 'reasonable efforts' have been taken is quintessentially fact-specific," and "'depends on a balancing of costs and benefits that will vary from case to case.'" (*Rockwell Graphic Systems, Inc. v. DEV Industries, Inc.*) "Reasonable efforts" may include adopting confidentiality policies, entering into non-disclosure agreements, and establishing digital and physical security infrastructure. (*Religious Tech. Ctr. Netcom On-Line Commc'n Servs.*)

The "information" eligible for protection under the UTSA can be almost anything, including any "formula, pattern, compilation program, device, method, technique, or process." Unlike information eligible for patent or copyright protection, which must fall into certain statutorily

defined categories, “any particular class or kind of matter” may qualify for trade secret protection, so long as it satisfies the two definitional requirements described above. (*Altavion, Inc. v. Konica Minolta Sys. Lab. Inc.*)

Even a combination of publicly available elements can qualify for trade secret protection, so long as the idea for that combination is valuable because it is unknown to others *and* reasonable efforts have been taken to keep it secret.

## What does trade secret law protect against?

---

Suppose you have reason to believe someone (a former employee, a competitor’s employee, etc.) is in possession of your company’s proprietary information that satisfies the two-pronged test described above. When will courts intervene to protect your company’s trade secret information?

The first question is whether that person or entity *misappropriated* your company’s trade secret. In states that have adopted the UTSA, a plaintiff asserting trade secret theft must show that the person alleged to have stolen a trade secret “acquired, disclosed, or used” the information at issue “through improper means.” (*Brocade Communications Sys., Inc. v. A10 Networks, Inc.*) To “use” a trade secret, one must “directly exploit” the information at issue “for one’s own advantage.” (*Silvaco Data Systems v. Intel Corp.*)

Simply possessing or taking advantage of something else (e.g., a software program or device) that was made *using* the secret is not enough.

“Improper means” may include “theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means.” (Cal. Civ. Code § 3426.1.) And in most cases, to prove trade secret misappropriation, a plaintiff will have to show that the defendant had “knowledge of the trade secret,” or at least “reason to know” about it. That is not to say that a defendant must have “comprehended” the trade secret.

But inadvertent possession is not trade secret misappropriation. Nor does legitimate reverse engineering or independent invention amount to trade secret misappropriation. The key question in such cases is whether the invention was truly independent, or if the engineering process was tainted in any way that suggests improper appropriation or use. (*Brocade Comms.; Faiveley Transp. v. Wabtec Corp.*)

In some jurisdictions, as an alternative to proof of actual or threatened misappropriation, a plaintiff asserting trade secret theft may seek relief under the “doctrine of inevitable

disclosure.” (*Whyte v. Schlage Lock Co.*) Claims under this doctrine typically arise in situations in which an employee leaves one company to work for a competitor, and the employee’s “new employment will inevitably lead him to rely on the plaintiff’s trade secrets.” (*PepsiCo, Inc. v. Redmond*) Note, however, that several jurisdictions, including California, have rejected this doctrine. (*Whyte*).

## What other legal claims may arise in trade secret cases?

Although there is some disagreement among UTSA jurisdictions over the extent to which the Act preempts other theories of recovery, nearly all agree that, at the very least, the UTSA displaces *stort claims* that are based on misappropriation of trade secrets. (*First Advantage Background Servs. Corp. v. Private Eyes, Inc.*) However, *breach of contract claims* are *not* preempted by the UTSA, even if they are partially based on the misappropriation of trade secrets. (*Angelica Textile Servs., Inc. v. Park*) Indeed, breach of contract claims, when available, can enable claims for misappropriation that otherwise falls short of trade secret protection. Such breach of contract claims, however, can raise their own unique issues.

For example, in California, most non-compete agreements — as may be found in employment contracts or termination agreements — are void under the state’s Business and Professions Code section 16600 as illegal restraints on employee mobility. At the same time, courts in California have held that section 16600 does *not* invalidate agreements that seek to protect an employer’s trade secrets. (*Latona v. Aetna U.S. Healthcare Inc.*) Other jurisdictions permit “reasonable” non-compete agreements, though the permissible scope varies from state to state.

In addition, in May, President Obama signed into law the Defend Trade Secrets Act of 2016 (“DTSA”), which creates a new *federal* civil cause of action for trade secret misappropriation. Although the DTSA is largely modeled on the UTSA, the new federal law gives plaintiffs the option to sue in federal court, and includes some potentially significant variations on existing trade secret law.

Most notably, the DTSA allows a plaintiff to seek an *ex parte* order “for the seizure of property necessary to prevent the propagation or dissemination of the trade secret.” While this provision only applies in “extraordinary circumstances,” it is a new and potentially potent remedy of which company counsel should be aware.