Intellectual Property & Technology Law Journal

Edited by the Technology and Proprietary Rights Group of Weil, Gotshal & Manges LLP

VOLUME 28 • NUMBER 9 • SEPTEMBER 2016

What You Need to Know about the Defend Trade Secrets Act

By Joseph D. Mornin

The Defend Trade Secrets Act (DTSA) expands federal protections for trade secrets. Most notably, the DTSA creates a private federal cause of action for trade secret misappropriation. Other developments include an *ex parte* seizure provision, protections for whistleblowers, and employer notice requirements. This article explains the DTSA's key provisions and offers guidance to employers and trade secret practitioners.

Background

Until now, civil trade secret actions have been governed entirely by state law.[1] Forty-eight states have adopted versions of the Uniform Trade Secrets Act (UTSA), and the others recognize common law claims for trade secret misappropriation.

The DTSA does not preempt state law claims,[2] and it introduces several important distinctions, which are discussed in detail below. Trade secret plaintiffs can now pursue their claims under parallel state and federal regimes. Whether the DTSA will simplify trade secret litigation remains to be seen. On the one hand, a federal statutory regime should make trade secret litigation more uniform and predictable, since courts will apply the same standards regardless of the states in which they are located; on the other hand, because the DTSA explicitly does not preempt state laws, litigants will face competing and potentially conflicting legal frameworks.

The DTSA took effect on May 11, 2016.[3] It was passed with near-unanimous support in both the House and the Senate. It applies to acts of trade secret misappropriation that occur on or after the date of enactment. In addition, the employer notice provisions (discussed below) apply to employee agreements entered into or updated after the same date. The DTSA applies to misappropriation that occurs after May 11, 2016 or began before May 11, 2016 and continued after the act took effect; for instance, if an employee misappropriated an employer's trade secret before the DTSA and continued to do so after May 11, 2016, the employer could bring a claim in federal court.

Private Federal Cause of Action for Trade Secret Misappropriation

The most significant provision of the DTSA is a new federal cause of action for trade secret misappropriation:[4]

> An owner of a trade secret that is misappropriated may bring a civil action under this subsection if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce.

Joseph D. Mornin is an associate in the Intellectual Property Department of Winston & Strawn LLP's San Francisco office, focusing on Internet and technology law. He may be reached at *jmornin@winston.com*.

Federal courts now have original (but not exclusive) jurisdiction over trade secret misappropriation claims. Jurisdiction under the DTSA is as broad as the Commerce Clause allows. Critics have noted that the DTSA may increase the length and cost of litigation, because it takes time and money to prove that the trade secret at issue satisfies the jurisdictional requirements.[5] In practice, most trade secrets likely will qualify, as long as the trade secret is related to a good or service that was intended for use in interstate commerce. In any event, plaintiffs can still pursue claims in state court if they prefer.

A variety of remedies are available under the new provision.[6] First, monetary remedies are available, including damages for actual loss, restitution, or a reasonable royalty. If the trade secret is "willfully and maliciously appropriated," courts may award attorneys' fees and exemplary damages up to two times the award of actual damages. Courts also can award attorneys' fees if either party makes a showing of bad faith.

Second, injunctions are available "to prevent any actual or threatened misappropriation." However, courts will not issue injunctions to "prevent a person from entering into an employment relationship," and "conditions placed on such employment shall be based on evidence of threatened misappropriation and not merely on the information the person knows." This language prevents plaintiffs from pursuing "inevitable disclosure" claims, for instance, seeking to prevent a former employee from working for a competitor based only on the threat that the employee would inevitably disclose proprietary information.

Some states recognize the inevitable disclosure doctrine; others, notably California, promote employee mobility by limiting the doctrine. The DTSA requires "evidence of threatened misappropriation," that is, it requires an employer to show more than that a departing employee knows sensitive information. In this respect, state law will continue to play an important role in trade secret litigation.

Third, the DTSA allows *ex parte* seizures of misappropriated trade secrets. The next section explains this provision.

The DTSA establishes a three-year statute of limitations.[7] The limitations period begins when "the misappropriation … is discovered or by the exercise of reasonable diligence should have been discovered." Notably, the statute indicates that "a continuing misappropriation constitutes a single claim of misappropriation." This rule differs from the limitations periods in the patent and copyright contexts, where each infringing act begins a new limitations period.[8] Under the DTSA, the limitations period begins at the start of the misappropriation, regardless of how long it continues.

Expanded Definition of "Trade Secret"

The DTSA definition of "trade secret" is broader than the UTSA definition. The UTSA definition is limited to specific types of trade secret information: "formula, pattern, compilation, program, device, method, technique, or process."[9] The DTSA adopts the broader definition of the Economic Espionage Act:[10]

> the term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing …

Under the DTSA, nearly any type of information can qualify as a trade secret, as long as the owner took reasonable steps to keep it a secret and the information derives economic value from its secrecy. This definition—"whether tangible or intangible, and whether or how stored"—potentially includes information that exists only in the mind of an employee. However, as discussed above, an employer cannot win an injunction against a departing employee based "merely on the information the person knows." Other definitions are generally the same; for instance, the DTSA definition of "misappropriation" is almost identical to the UTSA definition.

Ex Parte Seizures

The DTSA's most controversial provision allows a trade secret owner to seek a court order to seize misappropriated trade secrets:[11]

> Based on an affidavit or verified complaint satisfying the requirements of this paragraph,

> the court may, upon ex parte application but only in extraordinary circumstances, issue an order providing for the seizure of property necessary to prevent the propagation or dissemination of the trade secret that is the subject of the action.

The seizure provision is based on similar language in the Lanham Act.[12] In the trademark context, courts can order *ex parte* seizure of counterfeit goods. The party seeking the order must show that other remedies would be inadequate, the party would likely succeed on the merits, irreparable harm would otherwise occur, and that the counterfeit goods are located at a specific place.

No similar remedy exists under state laws for seizure of property to protect trade secrets. Under this provision, a plaintiff can have the government seize misappropriated property without advance notice to the defendant. There are several safeguards, for instance, the plaintiff must show that other remedies, such as a preliminary injunction, would not adequately protect the misappropriated trade secret. The court order must provide guidance to law enforcement on how the trade secret should be seized, including time of day and whether force may be used. When seized, the trade secrets must remain under the court's control, and cannot be accessible to the plaintiff before a seizure hearing.

Despite these safeguards, however, the seizure provision has been the most controversial part of the DTSA, in large part because the *ex parte* procedure does not allow the defendant to challenge the order before the property is seized.[13] Critics also have raised concerns about the expense of the process, which might encourage smaller defendants to capitulate rather than challenge the plaintiffs' claims. The seizure provision could open an avenue for trade secret trolling, that is, opportunistic plaintiffs might bring questionable suits for the purpose of extracting settlement payments from defendants, since it might be cheaper to settle than to mount a defense.

How the seizure provision will function in routine trade secret litigation remains to be seen. The DTSA requires the Federal Judicial Center to develop a set of best practices for seizing misappropriated information and securing it once it is seized. Its recommendations are due to be published by May 11, 2018.

Whistleblower Protections and Employer Notice Requirements

The DTSA protects whistleblowers from civil or criminal liability for disclosing trade secrets to the government or in a court filing.[14] The disclosure must be made "in confidence to a Federal, State, or local government official, either directly or indirectly, or to an attorney." The disclosure also must be made "solely for the purpose of reporting or investigating a suspected violation of law."

As of May 11, 2016, employers have a duty to notify employees of the whistleblower provisions "in any contract or agreement with an employee that governs the use of a trade secret or other confidential information."[15] The DTSA's definition of "employee" includes fulltime employees as well as "any individual performing work as a contractor or consultant," for instance, an independent contractor. Employers can meet this obligation by providing a cross-reference to a separate policy document describing the employer's policy for reporting suspected violations of law. If the employer fails to provide notice, it cannot win exemplary damages or attorneys' fees in an action against an employee for trade secret misappropriation.

In practice, employers now should include notice of the DTSA whistleblower provisions in nondisclosure agreements and other employment agreements that relate to trade secrets or confidential information. Employers must include the notice in agreements entered into or updated after May 11. The statute does not include a small-business exception, so employers of all sizes must provide notice.

The DTSA also includes rules to protect whistleblowers in anti-retaliation suits.[16] If a whistleblower sues an employer for retaliation for reporting a suspected violation of law, the DTSA allows the whistleblower to disclose trade secrets to his or her attorney and to use them in court proceedings. The plaintiff must file documents containing the trade secret under seal and must not otherwise disclose the trade secret, except by court order.

Other Provisions

First, the DTSA allows trade secret owners to maintain the secrecy of their trade secrets in court proceedings.[17] District courts must allow a trade secret owner to file a brief under seal arguing why the court should keep the information confidential. The language of the new rule does not limit its application to the DTSA or the Economic Espionage Act.

As a result, parties may invoke this provision in a wide variety of litigation involving trade secrets.

Second, the DTSA directs the Attorney General to publish a bi-annual report on trade secret thefts that occur outside the United States.[18] The reports will include recommendations for legislative and executive action to protect trade secrets abroad.

Third, the DTSA modifies the RICO statute to add violations of the Economic Espionage Act to the list of predicate offenses that constitute "racketeering activity."[19]

Conclusion

Congress passed the DTSA largely in response to fears of misappropriation of U.S. trade secrets by foreign actors.[20] As enacted, however, the DTSA provides no tools beyond what is allowed by state law to pursue claims for misappropriation that occurs abroad. Instead, the DTSA establishes a federal regime for trade secret protection that will operate alongside a variety of existing state frameworks. The DTSA is broader than state laws in some ways (*e.g.*, its seizure provisions and its broader definition of "trade secret") and narrower in others (*e.g.*, its rejection of the inevitable disclosure doctrine, which some states recognize). How the DTSA will affect trade secret protection strategies remains unclear, but it is likely to have a major impact on litigation.

Notes

1. The Economic Espionage Act provides for a federal criminal cause of action for acts of economic espionage, including trade secret misappropriation. *See* 18 U.S.C. § 1831 ("Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly [commits an act of economic espionage] shall, except as provided in subsection (b), be fined not more than $5,000,000 or imprisoned not more than 15 years, or both.").
2. 18 U.S.C. § 1838 ("Except as provided in section 1833(b), this chapter shall not be construed to preempt or displace any other remedies, whether civil or criminal, provided by United States Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret…").
3. DTSA § 2(e) ("The amendments made by this section shall apply with respect to any misappropriation of a trade secret (as defined in section 1839 of title 18, United States Code, as amended by this section) for which any act occurs on or after the date of the enactment of this Act."). President Obama signed the DTSA into law on May 11, 2016.
4. 18 U.S.C. § 1836(b)(1).
5. Professors' Letter in Opposition to the Defend Trade Secrets Act of 2015, at 6, available at *https://cyberlaw.stanford.edu/files/blogs/2015%20Professors%20Letter%20in%20Opposition%20to%20DTSA%20FINAL.pdf*.
6. Remedies are described in 18 U.S.C. § 1836(b)(3).
7. 18 U.S.C. § 1836(d).
8. *See, e.g.*, Stone v. Williams, 970 F.2d 1043, 1049 (2d Cir. 1992) ("Each act of infringement is a distinct harm giving rise to an independent claim for relief.").
9. *See, e.g.*, Cal. Civ. Code § 3426.1(d).
10. 18 U.S.C. § 1839(2).
11. 18 U.S.C. § 1836(b).
12. 15 U.S.C. § 1116(d) ("with respect to a violation that consists of using a counterfeit mark in connection with the sale, offering for sale, or distribution of goods or services, the court may, upon *ex parte* application, grant an order under subsection (a) of this section pursuant to this subsection providing for the seizure of goods and counterfeit marks involved in such violation and the means of making such marks, and records documenting the manufacture, sale, or receipt of things involved in such violation.").
13. Professors' Letter in Opposition to the Defend Trade Secrets Act of 2015, *supra* n.5 at 3-4
14. 18 U.S.C. § 1833 (b) ("An individual shall not be held criminally or civilly liable under any Federal or State trade secret law for the disclosure of a trade secret" under the specified circumstances.).
15. 18 U.S.C. § 1833(b)(3).
16. 18 U.S.C. § 1833(b)(2).
17. 18 U.S.C. § 1835.
18. DTSA § 4 ("Not later than 1 year after the date of enactment of this Act, and biannually thereafter, the Attorney General, in consultation with the Intellectual Property Enforcement Coordinator, the Director, and the heads of other appropriate agencies, shall submit to the Committees on the Judiciary of the House of Representatives and the Senate, and make publicly available on the Web site of the Department of Justice and disseminate to the public through such other means as the Attorney General may identify, a report on the following…").
19. 18 U.S.C. § 1961(1)(B) ("any act which is indictable under any of the following provisions of title 18, United States Code:… sections 1831 and 1832 (relating to economic espionage and theft of trade secrets)….").
20. *See, e.g.*, DTSA § 5 ("It is the sense of Congress that… trade secret theft occurs in the United States and around the world [and] trade secret theft, wherever it occurs, harms the companies that own the trade secrets and the employees of the companies….").