PAUL HASTINGS

STAY CURRENT

May 2016

Follow @Paul_Hastings

There's a New Federal Trade Secrets Statute—Now What?

By Victoria A. Cundiff, Bradford K. Newman, Daniel Prince, Blair M. Jacobs, Jennifer S. Baldocchi & Carson H. Sullivan

The passage of the Defend Trade Secrets Act ("DTSA") underscores that trade secrets are critical economic assets and that protecting them and preparing to defend against claims for misappropriation need to be high on every company's agenda. Here are our lawyers' perspectives on what business should be focusing on now and in the future.

Quick Background

After years of proposals, counterproposals, hearings, and negotiations, Congress has finally enacted a federal private right of action for trade secrets misappropriation. The DTSA is the newest addition to the federal Economic Espionage Act, the 1996 federal criminal trade secrets statute.

Much of the DTSA will look familiar. Patterned on the Uniform Trade Secrets Act, which has been adopted in some variation in every state other than New York and Massachusetts, the DTSA permits the owner of a trade secret to bring a claim in federal court for the actual or threatened wrongful acquisition, use, and/or disclosure of a trade secret. The Act permits an award of actual damages, disgorgement of unjust gains, a reasonable royalty, and injunctive relief subject to limitations discussed below. In cases of willful and malicious misappropriation, or where claims are made or resisted in bad faith, exemplary damages of up to twice the actual damages and an award of attorney's fees may be available.

So Now What?

Some provisions of the DTSA are new. How courts will interpret them remains to be seen. That being said, the passage of the DTSA is a good occasion to review policies and strategies in effect and fine tune or upgrade as necessary. Here are our five takeaways:

I. The "Immunity" Provision Creates at Least Two Potential Hazards for Companies That Need to be Addressed Immediately

Notice to Employees About When It Is "OK" to "Spill" Trade Secrets. The DTSA immunizes employees, defined for these purposes to include contractors and consultants, from criminal or civil liability under any federal or state trade secret law for disclosing trade secrets in confidence to federal, state, or local governments solely for purposes of reporting or investigating a suspected violation of law or in complaints and filings in anti-retaliation lawsuits relating to such disclosures. This Immunity Provision is not a "get out of jail free" card for disgruntled employees: to qualify for the immunity, employees must file documents containing trade secrets under seal and not make further disclosures of the secrets absent court order. The statute further provides that an employer shall provide notice of the immunity in any contract or agreement with an employee entered into or amended after May 11, 2016 that governs the use of a trade secret or other confidential information or, alternatively, by providing a cross-reference to a policy document provided to the employee setting forth the employer's reporting policy for a suspected violation of law. ***If an employer does not comply with the notice requirement, it may not be awarded exemplary damages or attorney's fees in an action under the DTSA against an employee to whom notice was not provided.*** Since many companies use a variety of agreements to protect confidential information, including employment agreements, standalone confidentiality and inventions agreements, and separation agreements as well as handbooks and policy statements, an immediate review of these documents for compliance is key.

Here Comes the "Whistleblower" Defense. Because of the Immunity Provision, companies must be more vigilant than ever in protecting their trade secrets, while anticipating the DTSA's unintended effect will likely be to increase "whistleblower" claims by employees who engage in trade secret theft as an attempted defense under the DTSA.

II. Don't Forget About State Law

Other than in the whistleblower context, the DTSA does not preempt existing state law remedies. In many cases it will be the right fit for a particular trade secrets dispute. In other cases, state law will continue to provide more effective (or, possibly, the only available) tools for particular disputes. The information at issue may not be sufficiently connected to interstate commerce to qualify for protection under the DTSA. The aggrieved party may not have standing to sue under the DTSA. Or, state law may offer dispute-specific advantages that the DTSA does not. For example, some states have been willing to grant so-called "inevitable disclosure" injunctions on a proper showing to prohibit employees who know trade secrets but are not bound by post-employment contractual restrictions from entering into particular new employment relationships. The DTSA expressly bars such relief. As another example, some states provide a longer statute of limitations period for certain trade secrets disputes. Where state law offers a better option, litigants are still free to take it.

By the same token, the DTSA makes clear that it is not a "workaround" to state laws prohibiting post-employment restraints. The statute expressly provides that courts enforcing the DTSA have broad authority to grant injunctive relief, ***provided that the order does not otherwise conflict with an applicable state law prohibiting restraints on the practice of a lawful profession, trade, or business***.

Finally, DTSA claims do not have to be brought in federal court. Federal courts have original, but not exclusive, jurisdiction to hear DTSA claims. While in many cases federal courts will be the most attractive option, the caseload, experience, schedules, and courtroom practices of a particular forum or case-specific issues may make state court a better choice.

III. Be Prepared for Seizure Orders

The seizure provisions of the DTSA sparked much discussion during the drafting of the bill. Not surprisingly, Fourth Amendment concerns and other fears of wrongful seizure were raised and discussed on a number of occasions. Recognizing the potentially devastating consequences to the accused and to third parties, when issuing a seizure order, the Act expressly provides that it is important for the court to balance the need to prevent or remedy misappropriation with the need to avoid interrupting the legitimate interest(s) of the accused party, as well as the business of third parties.

To help strike that balance, the Act includes a number of key procedural safeguards, including: (i) any seizure order must "provide for the narrowest seizure of property necessary" and must be executed by law enforcement officials (although technical experts may accompany); (ii) the applicant is required to post a bond sufficient to cover damages should the seizure turn out to be wrongful or excessive; and (iii) the court is required to provide specific guidance to the officials executing the seizure that "clearly delineates" the scope of their authority and details how the seizure must be conducted.

Taken together, these safeguards, in combination with the seven-day post-seizure hearing requirement at which the claimant bears the burden of proof, can provide significant relief to a party exposed to a wrongful seizure order. Nevertheless, uncertainty exists regarding *how* the *ex parte* seizure provisions will be utilized and policed. If a seizure is ordered, federal law enforcement personnel may conduct an unannounced search at a facility or office location to secure physical and/or electronic information "*necessary to prevent propagation or dissemination of the trade secret that is the subject of the action*." While this may pose significant concerns with respect to one's own trade secrets or other confidential information, no matter how ill-founded the order may appear, the business team and/or technical personnel should consult counsel immediately and take great care not to interfere with the execution of a seizure order. Thinking about a response when the government is at the door may be too late; it is critical to develop internal and external response plans for properly handling the receipt of a seizure order.

IV. The DTSA is Not the Only Federal Remedy for Misappropriation

The International Trade Commission ("ITC") has previously entered exclusion orders as to goods shown to have been made through the misappropriation of trade secrets abroad, relying for its authority on what the Federal Circuit has dubbed a "federal common law" of trade secrets. The DTSA now gives the ITC another, arguably even stronger, foundation for issuing such orders. How the DTSA will impact the ITC's activity in this area remains to be seen.

While the DTSA gives private plaintiffs the right to bring civil claims under the amended Economic Espionage Act, it also increases the fines available for criminal theft of trade secrets by an organization from $5,000,000 to "the greater of $5,000,000 or three times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided," and expressly makes a violation a RICO predicate offense.

Finally, Executive Orders giving the Administration authority to address trade secrets theft and information-sharing about cyber security remain in effect and have recently been renewed.

The bottom line: Congress and the Administration have declared trade secrets protection a priority. Parties to trade secrets disputes now have additional tools for addressing them. Selecting and navigating these multiple approaches will take careful thought by both trade secrets claimants and those accused of misappropriation.

V. Focus on Facts, Not Simply Fears

The DTSA is filled with warnings for parties on both sides of trade secrets disputes that they act at their peril if they do not present evidence and facts to support their positions. A party seeking *ex parte* relief to seize property "necessary to prevent the propagation or dissemination of the trade secret" must make a detailed *factual* presentation to prevail, must post a bond, and is at risk of an action for damage for any wrongful or excessive seizure. A party seeking an injunction imposing conditions on employment activities by a former employee who knows trade secrets (as opposed to the unavailable ban on entering into an employment relationship) is expressly required to provide "*evidence* of threatened misappropriation," not simply assertions that the employee knows trade secrets and that they are therefore necessarily at risk. The Act provides that parties on either side who act in bad faith to seek or oppose relief may not only lose, but also be required to pay the other side's attorney's fees.

We Can Help

The DTSA is not the final word on trade secrets disputes. The Act mandates a continuing discussion between the Administration and Congress on best practices for implementing the Act, the need for potential additional legislation, and regular reports concerning the misappropriation of trade secrets abroad. This dialogue is part of worldwide attention to the importance of trade secrets in the world economy.

Every business has trade secrets. The passage of the DTSA underscores that every business must think about protecting trade secrets and guarding against successful claims for misappropriation.

To discuss these developments in more detail and to learn how Paul Hastings can assist, please contact members of our ***Litigation*** *department and* ***Employee Mobility and Trade Secrets*** *team.*

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Los Angeles

Daniel Prince
1.213.683.6169
danielprince@paulhastings.com

Jennifer S. Baldocchi
1.213.683.6133
jenniferbaldocchi@paulhastings.com

Thomas P. O'Brien
1.213.683.6146
thomasobrien@paulhastings.com

New York

Victoria A. Cundiff
1.212.318.6030
victoriacundiff@paulhastings.com

Palo Alto

Bradford K. Newman
1.650.320.1827
bradfordnewman@paulhastings.com

Seoul

Jong Han Kim
82.2.6321.3801
jonghankim@paulhastings.com

Washington D.C.

Blair M. Jacobs
1.202.551.1951
blairjacobs@paulhastings.com

Stephen Kinnaird
1.202.551.1842
stephenkinnaird@paulhastings.com

Jeff A. Pade
1.202.551.1814
jeffpade@paulhastings.com

Carson H. Sullivan
1.202.551.1809
carsonsullivan@paulhastings.com