Published on *The National Law Review* https://natlawreview.com

Defend Trade Secrets Act. It's Coming: What You Need to Know

Article By:

Sara H. Jodka

Emma R. Wolfe

The Defend Trade Secrets Act ***(DTSA)*** is headed to President Barack Obama for his signature, and there is little doubt that President Obama will sign it into law. Below is a summary of what you need to know about this soon-to-be law, including what you should be talking to your employment law counsel about in terms of modifying employment contracts and agreements.

What is the DTSA?

The DTSA will effectively "federalize" trade secrets law and allow companies or individuals with trade secrets to file private civil lawsuits under the Federal Economic Espionage Act (the Espionage Act).

What does "federalizing" trade secrets law mean?

The federalization of trade secrets law is a game changer. Pre-DTSA, trade secrets law was a state law issue. While most states dealt with trade secrets by adopting some versions of the Uniform Trade Secrets Act, the laws (and court's interpretation of them) varied significantly from state to state. The variations led to many hotly contested procedural issues for example forum, venue and choice-of-law.

What is the purpose of the DTSA?

The DTSA's specified purpose is to create a nationwide law that tightens trade secrets protections to align them with those given to patents, copyrights, and trademarks. It makes the issue a federal one so that federal law and courts can control the subject area, which will provide more certainty for litigants in trade secrets cases.

What will the DTSA protect?

Federal law regarding intellectual property has been fought on three fronts: copyrights, patents, and trademarks. Now, trade secrets will enter the federal protection arena.

The DTSA will allow "[a]n owner of a trade secret that is misappropriated [to] bring a civil action…if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce." Oddly enough, however, the DTSA itself does not define "trade secret." The Espionage Act, however, does.

How will the DTSA protect trade secrets? *(Hint: Seizure provision)*

As set forth above, the DTSA will allow trade secret owners whose trade secrets have been misappropriated to file civil actions in federal court. It also provides for theft protections abroad, but much of this part of the law is yet to be determined.

In addition to allowing victims to be awarded damages for wrongful takings, the DTSA contains a seizure provision that allows for the seizure of stolen trade secrets in "extraordinary circumstances" upon an "ex parte application," and "affidavit or verified complaint." This seizure provision is something completely new in the trade secrets context, as no state law has ever provided a plaintiff with this remedy.

Although it is unclear what situations courts will eventually qualify as "extraordinary circumstances," the threshold appears to be slightly higher than that required to obtain a temporary restraining order under the Federal Rules of Civil Procedure. In fact, the first requirement for a court issuing a seizure order is the determination that "an order issued pursuant to Rule 65 of the Federal Rules of Civil Procedure or other form of equitable relief…[would] be inadequate…because the party to which the order would be issued would evade, avoid, or otherwise not comply with such an order." These additional requirements must also be met before the court will grant a seizure:

- an immediate and irreparable injury;
- the harm to the applicant outweighs the harm to the legitimate interest;
- a showing that the person misappropriated the trade secrets by improper means or conspired to misappropriate through improper means;
- a description (with reasonable particularity) of the matter to be seized and the location of the matter to be seized (if reasonable under the circumstance); and
- the person(s) against whom seizure would be ordered would destroy, move, hide or make the trade secrets inaccessible if they were provided notice of the application.

A seizure order is enforceable by federal law enforcement officials and the materials seized are to be deposited to the custody of the court.

While such seizures may be difficult when dealing with small bits of data or data that can be easily copied or disseminated, the DTSA provides something else no other trade secrets law offers: it allows the moving party to request that the seized information is encrypted in the custody of the court.

Is there anything else interesting about the DTSA? *(Hint: Whistleblower protection)*

Yes. It has an immunity protection for whistleblowers. That provision essentially provides that an individual, who reveals the disclosure of a trade secret in confidence to a federal, state, or local government official, or to an attorney, may not be held criminally or civilly liable under any federal or state trade secrets law.

Also, an individual who files a lawsuit for retaliation by an employee for reporting a suspected violation of law may disclose the trade secret to his or her attorney and use the trade secret information in the court proceeding.

What are the pros?

The advantage of the DTSA is that, for companies that operate across state and national borders and that have their trade secrets threatened by competitors across the world, state laws were previously insufficient to properly protect those companies. The DTSA will help shore up the protection of trade secrets, likely reduce jurisdictional court battles that are typical at the outset of trade secret litigation in state court, and provide litigants with federal jurisdiction.

What are the cons?

The DTSA does not preempt state trade secret laws. As such, while a litigant may bring a federal trade secrets lawsuit, that same litigant may also be able to bring a claim under state law as well. While it adds uniformity of trade secrets law at the federal level, it does nothing for the myriad of trade secrets laws at the state level. In reality, this means that a litigant is more likely to face a federal trade secrets misappropriations claim and similar state law claims. While this provides uniformity at the federal level, it does not to clarify the patchwork of state laws, and makes trade secret litigation more complex by providing more litigation options to trade secret holders. While some may see this as a good thing, because it provides multiple avenues for recovery, others prefer uniformity.

While it is not necessarily true that companies should expect to see more litigation, they should be prepared to litigate these cases on the federal stage, as well as remain up-to-date on all relevant state laws.

What should my company’s next steps be to ensure compliance and corporate readiness?

Internal Controls

Companies should check their internal controls to ensure they are properly protecting their trade secrets. Some beginning action items should include the following:

- Audit and Identify: Perform an audit of corporate assets to identify and designate trade secrets and determine where trade secrets are maintained and who has access to them.

- Protect: Take steps to properly and adequately protect trade secrets. For electronically available or accessible information, ensure trade secrets are username and password protected and only made available or accessible to those who need access. Encrypting electronic information will also reduce the chance that it can be taken, opened, read, and disseminated outside the company’s information systems. For tangible trade secrets, ensure trade secrets are physically locked or that physical access to them is password, keycard or otherwise protected and that only those who need access have it.

- Revise Agreements: Many companies allow third-parties access to the property, premises, data, networks, etc. Companies should review their vendor agreements, non-disclosure agreements, and other confidentiality and other non-disclosure-type agreements to ensure they are sufficient to identify and protect corporate trade secrets.

- Revise Policies: Companies should review their privacy policies, including corporate security and electronic use policies to ensure they are sufficient to identify and protect their corporate trade secrets. This includes reviewing non-compete, non-disclosure, and other privacy-related agreements and policies the company may have with its employees.

Dealing with Employees

The DTSA requires that employers provide notice of the DTSA's immunity "in any contract or agreement with an employee that governs the use of trade secret or other confidential information." Companies can comply with this requirement by cross-referencing a policy document provided to the employee that sets forth the employer's internal mechanism for reporting a suspected violation of law. If the employer fails to do this, the employer cannot be awarded exemplary damages or attorneys' fees in an action against an employee to whom notice was not provided. This is required for all contracts and agreements that are entered into or updated after the DTSA's enactment date.

The takeaway for this requirement is that companies with employees should sharpen their pencils because they have contracts and agreements to modify.

Dealing with Competitors

Companies can now act swiftly against a competitor attempting to misappropriate trade secrets. Under the appropriate "extraordinary circumstances," the ability to file an ex parte motion in federal court for the seizure of any misappropriated property provides companies with a way to actually keep these trade secrets, well, secret. In addition, the automatic access to federal courts provides companies with a forum that is often better suited to handle complex interstate and international litigation, not to mention complicated technical issues, and decreases initial costs related to procedural battles.

National Law Review, Volume VI, Number 124