Insight

IN-DEPTH DISCUSSION

MAY 2, 2016

Trade Secrets Finally Get Federal Law Protection

BY SCOTT MCDONALD AND JACKIE JOHNSON

UPDATE: On May 11, 2016, President Obama signed the Defend Trade Secrets Act into law.

On April 27, 2016, Congress passed the Defend Trade Secrets Act of 2016 (S.1890)[1] (DTSA) and sent it to President Obama, who has indicated he will sign it into law.[2] The DTSA, which will take effect on the day it is signed, will provide a new federal court civil remedy for acts of trade secret misappropriation occurring on or after the enactment date. The passage of the DTSA means trade secret owners finally have a truly uniform federal law under which to pursue trade secret misappropriation claims.

This article discusses trade secret misappropriation, outlines the provisions of this new law, and offers some practical takeaways for employers.

Trade Secret Misappropriation – How Big a Problem is it?

> *"There are only two categories of companies affected by trade-secret theft: those that know they've been compromised and those that don't know yet..."*
>
> *—Eric Holder, former U.S. Attorney General.*[3]

1 S. 1890, 114th Cong. (2016) (enacted), *available at* https://www.congress.gov/bill/114th-congress/senate-bill/1890.

2 The White House, Statement of Administration Policy, S. *1890 – Defend Trade Secrets Act of 2016*, (Apr. 4, 2016), *available at* https://www.whitehouse.gov/sites/default/files/omb/legislative/sap/114/saps1890s_20160404.pdf.

3 Brian Yeh, "Protection of Trade Secrets: Overview of Current Law and Legislation," The Congressional Research Service, April 22, 2016, *available at* https://www.fas.org/sgp/crs/secrecy/R43714.pdf.

The cost of intellectual property theft to American businesses has been estimated at more than $300 billion a year.[4] Trade secret theft by employees is a significant part of this problem. It is generally much easier for an employee with access to trade secrets in the course of employment to take and use a company's trade secrets for unauthorized purposes than it is for an outside party to do so. One recent survey indicated that 79% of employees leaving certain positions like finance, sales, and marketing, took data that belonged to their employer without permission, and 56% of the individuals surveyed did not believe there was anything criminal about using a competitor's trade secrets.[5] Statistics like these indicate the issue is one every employer with trade secrets to protect should pay close attention to.

While most states follow the Uniform Trade Secrets Act (UTSA), there are still significant variations in the law and how it is applied from state to state because the states were free to modify the model statute. Many have done so through language changes while others have simply interpreted it differently.[6] And, of even more significance, there are differences in evidentiary standards, discovery rules, and procedural mechanisms for pursuing trade secret claims from state to state.[7]

These differences in trade secret protections among states have created a complicated maze for employers to navigate. Further difficulties often arise when the parties or witnesses are in different states or the misappropriating party destroys the evidence of misappropriation or takes it out of the country.[8] The DTSA will provide a new route for trade secret owners that should help address many of these problems and give employers more options to consider.

The operative provision of the 2016 Defend Trade Secrets Act provides:

> 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.

The DTSA is an amendment to the Economic Espionage Act (EEA), 18 U.S.C. §1831, *et seq.*,[9] which has been around since 1996, but until now was primarily a criminal law enforcement statute that did not provide for a private right of civil action. The DTSA now provides for civil claims and original (but not exclusive) jurisdiction in federal court over claims brought under the statute.

There are several key features to the DTSA of particular interest to employers. The DTSA:

- Provides uniform definitions for "trade secrets" and "misappropriation" that are generally consistent with the Uniform Trade Secrets Act but with a few differences.

4 2013 U.S. Report of the Commission on the Theft of American Intellectual Property, *available at* http://www.ipcommission.org/report/ip_commission_report_052213.pdf.

5 Press Release, Symantec (Feb. 6, 2013), *available at* https://www.symantec.com/about/newsroom/press-releases/2013/symantec_0206_01.

6 The UTSA has been adopted in all states except New York, Massachusetts, and arguably North Carolina (which has adopted a very similar law); *see* Malsberger, *Trade Secrets: A State-by-State Survey* (BNA/ABA 5th Edition 2014).

7 David S. Almeling, *Four Reasons to Enact a Federal Trade Secrets Act*, Fordham Intellectual Property, Media & Entertainment Law Journal XIX.3 (2009), at 774; see also, S. Rept. 114-220, at 2-3 ("Although the differences between State laws and the UTSA are generally relatively minor, they can prove case-dispositive: they may affect which party has the burden of establishing that a trade secret is not readily ascertainable, whether the owner has any rights against a party that innocently acquires a trade secret, the scope of information protectable as a trade secret, and what measures are necessary to satisfy the requirement that the owner employ "reasonable measures" to maintain secrecy of the information." *See also*, Yeh, "Protection of Trade Secrets: Overview of Current Law and Legislation," supra note 3, p.9.

8 Yeh, "Protection of Trade Secrets: Overview of Current Law and Legislation," *supra* note 3, p.22. (quoting Senator Coons' comment that "[f]ederal courts are better suited to working across state and national boundaries to facilitate discovery, serve defendants or witnesses, or prevent a party from leaving the country." News Release, *Senators Coons, Hatch Introduce Bill to Combat Theft of Trade Secrets and Protect Jobs* (Apr. 29, 2014.

9 The quoted provisions will be inserted in the EEA at 18 U.S.C. § 1836(b).

- Allows for a civil action in federal courts, providing a uniform set of procedural and evidentiary rules (the Federal Rules of Civil Procedure and Rules of Evidence).
- Allows for the seizure of trade secrets from an alleged misappropriator without notice or an evidentiary hearing in extraordinary circumstances.
- Provides for a variety of different remedies including injunctive relief (for actual and threatened misappropriation), damages (under a variety of different theories), and exemplary damages (up to two times the amount of damages).
- Limits injunctive relief that can be awarded to avoid conflicts with state law limitations regarding noncompete contracts and other restraints of trade.
- Allows a prevailing party to recover attorneys' fees under certain conditions.
- Provides protection from prosecution for whistleblowers and retaliation claimants.
- Requires that employers provide employees notice of the whistleblower protection in order to preserve the ability to recover attorneys' fees or exemplary damages.
- Does not preempt or eliminate state law claims and remedies related to trade secrets, or modify other federal laws on intellectual property or unauthorized computer access.
- Has a three-year statute of limitations that applies a discovery rule.
- Addresses ***international*** trade secret theft and economic espionage.

Uniform Definitions

The DTSA retains most of the definition of "trade secrets" used in the Economic Espionage Act, which generally follows the UTSA definition. Under this definition, the term "trade secrets" covers "all forms and types of" information, regardless of how stored, where:

> the owner thereof has taken reasonable measures to keep such information secret; and
>
> the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by another person who can obtain economic value from the disclosure or use of the information;...

The DTSA adds definitions for "misappropriation" and "improper means" to the Economic Espionage Act.

Under the DTSA definition, the term "misappropriation" tracks the UTSA and divides misappropriation into two categories: (1) improper acquisition and (2) improper use or disclosure. More specifically, it provides that "misappropriation" means:

1) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or
2) disclosure or use of a trade secret of another without express or implied consent by a person who
   a) used improper means to acquire knowledge of the trade secret; or
   b) at the time of disclosure or use, knew or had reason to know that his/her knowledge of the trade secret was
      i. derived from or through a person who had utilized improper means to acquire it;

ii. acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or

iii. derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or

c) before a material change of his or her position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.

The DTSA states that "improper means" includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means, but does not include reverse engineering, independent derivation, or any other lawful means of acquisition.

Uniform Procedures and Evidentiary Standards

The DTSA provides that the U.S. district courts have original jurisdiction over civil actions brought under the law. It is notable that this statement of jurisdiction is not exclusive. This may create issues as to whether pleading a claim under the DTSA is compulsory in certain circumstances if it is going to be preserved, even if the party is attempting to litigate only state law claims in state court.[10] This issue aside, employers will still have the ability to capitalize on uniformity advantages of the DTSA because as long as the action is brought in a federal court, the Federal Rules of Civil Procedure and Federal Rules of Evidence will control instead of state procedural and evidentiary rules.

To avoid unnecessary disputes related to discovery protections, the statute expressly states that a court may ***not*** authorize or direct the disclosure of any information the owner asserts to be a trade secret unless the court allows the owner the opportunity to file a submission under seal that describes the interest of the owner in keeping the information confidential. And, providing information relating to a trade secret to the government or a court in connection with a prosecution under the DTSA constitutes no waiver of trade secret protection unless the trade secret owner expressly consents to such waiver.

Seizure Feature

A unique feature of the DTSA is its seizure of evidence provisions. The legislature recognized significant concerns over the potential for trade secrets to be compromised through use that destroys the value of its secret nature before an evidentiary hearing can be held, and the possibility of destruction of evidence or its removal from the country by a misappropriator as soon as the person or entity learns legal action is being taken. Consequently, the law provides for the ability of a party to, on an ex parte basis (meaning without notice to the opposing party), apply for and secure an order from a court to have the trade secret material seized by law enforcement authorities (state or federal) – thereby removing the trade secret information from the alleged misappropriator's possession until an evidentiary hearing can be held.

However, the DTSA also expressed the sense of Congress that it is important when applying this seizure mechanism to balance the need to prevent or remedy misappropriation against both (a) legitimate interests of the party accused of wrongdoing and (b) the need to avoid interrupting the business of third parties. The seizure

10 *See, e.g., Allied Erecting and Dismantling Co. v. Genesis Equipment & Manufacturing, Inc.*, 805 F.3d 701, 708-709 (6th Cir. 2015) ("A final judgment on the merits of an action precludes the parties or their privies from relitigating issues that were or *could have been* raised in that action.")(quoting *Federated Dep't Stores, Inc. v. Moitie*, 452 U.S. 394, 398, 101 S. Ct. 2424, 69 L.Ed. 2d 103 (1981)); Fed. R. Civ. P. 13(a)(1)–(a)(1)(A) ("A pleading must state as a counterclaim any claim that—*at the time of its service*—the pleader has against an opposing party if the claim: (A) arises out of the transaction or occurrence that is the subject matter of the opposing party's claim...." (emphasis added)).

mechanism is an extraordinary remedy and has several safeguards. These safeguards include the requirement to show "extraordinary circumstances" such as evidence that a normal court order would not be complied with by the alleged misappropriator, or that immediate irreparable injury will occur absent seizure, and that the risk of harm to the business is greater than that to the misappropriator or third parties. The entity alleging misappropriation must also show it is likely to prevail on the merits. In addition, the entity cannot have publicized the requested seizure.

The seizure order must contain provisions protecting the confidentiality of the information, provide guidance to law enforcement officials executing the seizure on their scope of authority, and require the applicant to post a bond or other security. An evidentiary hearing is then set to determine whether the seizure order should remain in place. The applicant must prove the elements to sustain the seizure.

The DTSA contains provisions prohibiting publicity of the seizure that might damage the alleged misappropriator. There are special provisions covering materials held in the custody of the court as well, such as rules regarding the storage medium, steps to be taken to protect the confidentiality of the materials seized, and appointment of a special master to handle logistical matters. And, a party or a person who claims to have an interest in the subject matter seized may make a motion at any time, which may be heard *ex parte*, to encrypt any material seized.

Abuse of the seizure mechanism has consequences. A party that can prove it was damaged by a wrongful or excessive seizure order can potentially obtain lost profits, costs of materials, loss of goodwill, punitive/exemplary damages and attorneys' fees.

Injunctive Relief Standards

The DTSA expressly provides for injunctive relief as a remedy to prevent any actual or threatened misappropriation "on such terms as the court deems reasonable." It allows for an injunction requiring a party to take affirmative actions to protect a trade secret. And, under exceptional circumstances that render an injunction inequitable, the future use of the trade secret can be conditioned on the payment of a reasonable royalty to the trade secret owner for as long a period of time as the misappropriators could have been prohibited from using the trade secret.

However, there are also some unique limitations to injunctive relief under the DTSA. The DTSA provides that an injunction under the statute may not prevent a person from entering into an employment relationship, and any conditions or limitations placed on an individual's employment as a result of an injunction must be based on evidence of threatened misappropriation and not "merely" the fact that the individual knows certain information. This signals a limitation on the use of the inevitable disclosure doctrine as it has been applied in some jurisdictions.

In addition, the injunction cannot conflict with an applicable state law prohibiting restraints on the practice of a lawful profession, trade or business. This is clearly intended to create some deference to state noncompete statutes such as the law in California that would prohibit or put significant limits on actions that restrain an employee's employment options.[11]

11 Cal. Bus. & Prof. Code § 16600.

Whistleblower/Retaliation Claim Immunity Protections

The DTSA contains a provision designed to protect whistleblowers. Specifically, it provides that 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 that is made "in confidence" to a federal, state, or local government official, either directly or indirectly, or to an attorney, provided that: it is disclosed "solely for the purpose of" reporting or investigating a suspected violation of law, or is made in a complaint or other document filed in a lawsuit or other proceeding filed under seal so that it is not disclosed to the public.

The law also contains an anti-retaliation provision. Under the DTSA, an individual who files a lawsuit for retaliation stemming from the employer's suspected law violation may disclose the trade secret to his/her attorney and use the trade secret information in the court proceeding, provided the individual files any document containing the trade secret under seal, and does not disclose the trade secret, except pursuant to court order.

Notice Requirement

The DTSA provides that employers must give notice of the immunity provisions of the law described above in any contract or agreement with an employee that governs the use of a trade secret or other confidential information. An employer will be deemed to be in compliance with this notice requirement if it provides a cross-reference to a policy document provided to the employee that describes the employer's reporting policy for a suspected law violation.

If an employer does not comply with the notice requirement described above, the employer may not be awarded exemplary damages or attorneys' fees under the statute in an action against an employee who misappropriates trade secrets. The notice obligation for contracts applies only to contracts that are entered into or updated after the date of enactment of the DTSA. Consequently, the law does not require employers to replace existing contracts with new ones. However, for existing employees, even if an existing contract is not replaced or modified, notice of a policy amendment applicable to the employee that provides notice of the immunity protection is still advisable.

Notably, the DTSA's definition of "employee" for these protections is expansive. It defines employee to include not only ordinary employees but also "any individual performing work as a contractor or consultant for an employer." This suggests that there is a need to examine not only ordinary employee policy documents for purposes of the statutory notice but also independent contractor and consultant agreements.

No Preemptive Effect

The DTSA has no preemptive effect on other trade secret protection laws. It is part of the Economic Espionage Act, which already provides that it "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, or to affect the otherwise lawful disclosure of information by any Government employee under section 552 of title 5 (commonly known as the Freedom of Information Act)." The DTSA confirms that it retains this limitation by stating that "[n]othing in the amendments made by this section shall be construed to modify the rule of construction under section 1838 of title 18, United States Code, or to preempt any other provision of law."

The DTSA expressly provides that it will not be construed to be "a law pertaining to intellectual property" for purposes of any other act of Congress (presumably intended to distinguish it from federal patent, trademark,

and copyright laws). And, while there are whistleblower and retaliation claimant protections in the DTSA, the DTSA is also clear in stating that nothing in its protections will be construed to "authorize, or limit liability for, an act that is otherwise prohibited by law, such as unlawful access of matter by unauthorized means." This would presumably include conduct such as trespass, ordinary theft, or unauthorized access to a computer system that would violate the Federal Computer Fraud and Abuse Act.[12]

Statute of Limitations

A civil action under the DTSA may not be commenced later than three years after the date on which the misappropriation is discovered or by the exercise of reasonable diligence should have been discovered. For these purposes, "a continuing misappropriation constitutes a single claim of misappropriation."

This single-claim construction that triggers the running of the statute of limitations is the same construction used in the UTSA. Consequently, there is a considerable body of law to help guide employers on the timing issues it creates. However, this does not mean that the issue is without wrinkles. The knowledge and intent elements in the definition of "misappropriation" have created some difficult issues with the statute of limitations under the UTSA, and those will likely carry through to the DTSA.[13]

Enhanced Focus on International Trade Secret Theft

A significant part of the congressional focus on trade secret laws that gave birth to the DTSA was concern over international economic espionage.[14] There is no uniformly applicable international law or treaty that specifically addresses the protection of trade secrets, and the protections that do exist within the rules of the World Trade Organization and similar bodies have significant weaknesses.[15] Some have argued that "the United States has not consistently received cooperation from international jurisdictions in protecting trade secrets in part because it does not have its own federal civil statute to reference in encouraging the adoption and enforcement of similar legislation by its treaty partners."[16] The DTSA remedies this problem.

There are also a number of features in the DTSA (beyond the importance of its existence as a ***federal*** law protecting trade secrets) that are designed to help focus on and address the international theft issue. The seizure feature is expressly designed to be used "in instances in which a defendant is seeking to flee the country…", as well as in other circumstances.[17] And, the DTSA requires the Attorney General to make a biannual report to the House and Senate Judiciary Committees on international trade secret theft affecting U.S. companies. The report is to include recommendations for legislative and executive actions to address the problem along with educational material for U.S. companies to help protect themselves and to provide a means for U.S. companies to report any theft occurring outside the United States.

---

12 18 U.S.C §1030, *et. seq.*

13 *See e.g., Cypress Semiconductor Corp. v. Superior Court*, 163 Cal. App. 4th 575 (2008).

14 *See* Yeh, "Protection of Trade Secrets: Overview of Current Law and Legislation," *supra* note 3, p. 1 (citing *Cyber Espionage and the Theft of U.S. Intellectual Property and Technology: Hearings Before the House Energy & Commerce Comm., Subcomm. on Oversight and Investigations*, 113th Cong. 1st Sess. (2013); *Economic Espionage and Trade Secret Theft: Are Our Laws Adequate for Today's Threats?: Hearings Before the Senate Judiciary Comm., Subcomm. on Crime and Terrorism*, 113th Cong. 2d Sess. (2014); *Trade Secrets: Promoting and Protecting American Innovation, Competitiveness and Market Access in Foreign Markets: Hearings Before the House Judiciary Comm., Subcomm. on Courts, Intellectual Property and Internet*, 113th Cong. 2d Sess. (2014)).

15 *Id.* at 11-15, 16-18 (discussing current administration initiatives to address the international problem).

16 *Trade Secrets: Promoting and Protecting American Innovation, Competitiveness and Market Access in Foreign Markets: Hearings Before the House Judiciary Comm., Subcomm. on Courts, Intellectual Property and Internet*, 113th Cong. 2d Sess. (2014) (statement of Thaddeus Burns, Senior Counsel, General Electric, on behalf of the Intellectual Property Owners Association), see also, Yeh, "Protection of Trade Secrets: Overview of Current Law and Legislation," p. 20.

17 S. Rept. 114-220, at 6.

Practical Takeaways

Employers looking to take advantage of the new options provided under the DTSA should consider the following practical measures:

1. Examine contracts and confidential information protection policies with employees and independent contractors to evaluate the need for notice language regarding the DTSA whistleblower and retaliation claimant protections. Inclusion of this language can help preserve remedies for misappropriation.
2. Examine contracts covering confidential information and/or trade secrets and consider the use of savings clause language to help safeguard rights provided under the DTSA.
3. Examine applicable state law options in the most likely states for a legal action involving your company (e.g., the location of the principal place of business), and identify in advance any substantive and procedural advantages of the state law versus the new federal law (DTSA) so that a decision on which option to pursue (state or federal court action) can be made more quickly when need for injunctive relief arises.
4. Examine hiring and on-boarding procedures to make sure that reasonable steps are being taken to avoid newly hired employees bringing trade secrets of a prior employer into the workplace or using them.
5. Examine employee termination and exit processing procedures to ensure appropriate protocols are in place to secure the return of confidential and trade secret information that might be in a departing employee's possession or control, and to identify criteria indicative of the possible need to pursue a seizure order.
6. Consider establishing an identification process to flag in advance trade secret information that is of the highest priority to protect, and that might require the pursuit of a seizure order if misappropriated.
7. If international theft is a concern, monitor the biannual reports from the Attorney General to Congress and the recommendations and educational materials generated by this process, and evaluate reporting options to be pursued so that the company's industry is appropriately represented in any future congressional evaluations and developments on the issue.