HOW THE NEWLY ENACTED "DEFEND TRADE SECRETS ACT" HAS CHANGED THE LANDSCAPE OF TRADE SECRET LAW

BY: ELISABETH GRAY

On May 11, 2016, the federal government enacted a new tool for responding to the theft of valuable company information: a federal claim for trade secret misappropriation, the Defend Trade Secrets Act of 2016 ("DTSA"), codified at 18 U.S.C. § 1836(b). The DTSA creates, for the first time, a federal private right of action for trade secret misappropriation. According to the Senate Report for the DTSA, the goal of the DTSA was to "provide a single, national standard for trade secret misappropriation with clear rules and predictability for everyone involved."[1] While the enactment of the DTSA has now provided a federal cause of action, the DTSA does not preempt state trade secret laws and is simply an additional avenue for relief.[2]

The DTSA was overwhelmingly passed by Congress and then signed by President Obama on May 11, 2016.[3] The DTSA applies to any act that occurs on or after this date. Recent judicial decisions have found that a DTSA claim may accrue as long as any of the alleged acts of misappropriation occur after May 11, 2016.[4] The statute of limitations under the DTSA is three (3) years from the date on which the misappropriation was, or should have been, discovered.[5] However, the continued misappropriation does not toll the statute of limitations, and the statute of limitations begins to run once the misappropriation was, or should have been, first discovered.[6]

Prior to the DTSA's enactment, private causes of action for trade secret misappropriation were only authorized by state law. Forty-eight states, including Kentucky, have adopted the Uniform Trade Secrets Act ("UTSA"). However, even under the UTSA, there are many inconsistencies amongst the states. For instance, the statute of limitations varies from state to state.[7] Further, businesses are typically limited to the state court systems to enforce a UTSA claim unless there is an independent basis for federal jurisdiction.

To address those shortcomings, the new DTSA provides that a person or entity may bring a civil action in federal court, under federal law, against a person or entity who improperly acquired or disclosed a trade secret. Arguably, the definition of a "trade secret" under the DTSA is broader than the one contained in the UTSA, focusing on whether the public (as opposed to other persons) can obtain economic value from the trade secret's disclosure. To qualify for trade secret protection under the DTSA, any purported trade secret must (i) in fact be secret; (ii) derive actual or potential independent economic value from not being

generally known to or readily ascertainable through proper means by another person who could obtain economic value from the disclosure or use of the information; and (iii) have been consistently subject to efforts reasonable under the circumstances to protect its secrecy.[8] This definition of "trade secret" under the DTSA broadens the UTSA's definition of a "trade secret" by now including "all forms and types of financial, business, scientific, technical, economic, or engineering information, . . . whether tangible or intangible" regardless of how, where, or even whether they are stored at all.[9]

"Misappropriation" under the DTSA includes the wrongful acquisition of a trade secret, *i.e.*, the acquisition of a trade secret by a person who knows or has reason to know that the acquisition was made by improper means, and the wrongful use or disclosure of a trade secret, use or disclosure by one who (i) used improper means to acquire the secret or (ii) knew or had reason to know that the secret was (a) derived from a person who used improper means to acquire it, (b) acquired under circumstances giving rise to a duty to maintain its secrecy, or (c) derived from or through a person who owed a duty to the owner to maintain its secrecy.[10]

Moreover, "improper means" under the DTSA includes "theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means." However, in a departure from the UTSA that is nonetheless consistent with general trade secret practice, the DTSA expressly provides that reverse engineering, independent derivation and any other lawful means of acquisition are excluded from the definition of "improper means."[11] The DTSA speaks in terms of the "owner" of a trade secret, but the term "owner" is defined to include not only the legal owner, the party with legal title to the trade secret, but also an equitable title holder and a licensee of the trade secret.[12] Because the DTSA is a federal cause of action, the DTSA also has an "interstate commerce" requirement and provides standing to pursue a trade secret claim only where the trade secret is "related to a product or service used in, or intended for use in, interstate or foreign commerce."[13]

The DTSA does not authorize injunctions to restrain a person from entering into an employment relationship, but expressly allows courts to impose certain restrictions on employment where there is actual evidence of threatened misappropriation.[14] Moreover, the DTSA bars injunctive relief if it would otherwise conflict with state law prohibiting restraint on the practice of a lawful profession, trade or business.[15]

Further, the DTSA allows for whistleblower immunity to employees, contractors or consultants if they disclose the alleged trade secret to investigate or report a suspected violation of law.[16] Before a federal court will award punitive damages or attorney's fees to an employer in an action against an employee under the DTSA, such whistleblower immunity must be disclosed to all employees in any agreement or policy that addresses trade secrets or "other confidential information" that is entered into or updated after May 11, 2016.[17] Whistleblower immunity does not extend to any otherwise improper acts by the employee, such as hacking information in violation of the Computer Fraud and Abuse Act.[18]

The new law also provides more nimble remedies. In addition to injunctive relief and an award of actual damages, the statute provides that the court may award unjust enrichment (defendant's profits), or alternatively, a reasonable royalty for unauthorized use (where other remedies are unavailable).[19] The DTSA also permits an award of exemplary damages up to two (2) times the amount awarded as compensatory damages in the case of willful and malicious misappropriation.[20] In addition, with the appropriate notice as outlined above, the DTSA provides for reasonable attorney's fees to the prevailing party upon a showing of bad faith or willful misconduct, or when a motion to terminate an injunction is made or opposed in bad faith.[21]

Notably, the DTSA also provides a new form of relief, an *ex parte* seizure order, authorizing law enforcement to seize stolen property and bring it into the custody of the court until the parties can be heard (which must occur within seven (7) days).[22] The seizure order is available in the event a temporary restraining order is justified but the wrongdoer is likely to evade the restraining order, destroy evidence, or otherwise refuse to comply.[23] To obtain an *ex parte* seizure order, a DTSA plaintiff must file an affidavit or complaint showing that (i) the trade secret misappropriation will cause immediate and irreparable injury, which cannot be addressed by injunctive or other relief; (ii) the harm to the applicant outweighs the harm to the DTSA defendant, and substantially outweighs the harm to any third parties; (iii) the applicant is likely to succeed in showing that trade secret misappropriation occurred; (iv) the DTSA defendant has actual possession of the trade secret, and the application describes "with reasonable particularity" where it is located; (v) the DTSA defendant will destroy or hide the trade secret, if given notice; and (vi) the applicant has not publicized the seizure.[24]

The seizure order itself must (1) include findings and conclusions; (2) provide for the narrowest seizure of property necessary; (3) prohibit access by the plaintiff or copying of the information; (4) specify law enforcement's scope of authority; (5) set a hearing within seven days; and (6) require a bond.[25] The bond must be "determined adequate by the court for the payment of the damages that any person may be entitled to recover as a result of a wrongful or excessive seizure or wrongful or excessive attempted seizure."[26] An amendment was added to the DTSA while Congress was considering the bill to ensure that *ex parte* seizures were available only in "extraordinary circumstances" to limit the availability of this relief.[27]

Courts have just begun to consider alleged DTSA violations arising after May 2016. For instance, on December 2, 2016, the United States District Court for the District of Colorado considered whether to issue a preliminary injunction for an alleged DTSA violation in *Engility Corp. v. Daniels*.[28] *Engility* considered claims brought against a former employee of Engility, Daniels, and how he treated Engility data in his possession shortly before and after his final day of employment with Engility. Specifically, several days after he left Engility's employ, Daniels surrendered a flash drive of Engility confidential information to Engility. The "date modified" of the information on the flash drive was the day following

Daniels' last day of Engility employment. There was no dispute that the information contained on the flash drive was properly classified as Engility "trade secrets."

In its motion for a preliminary injunction, Engility sought to enjoin Daniels and his new employer from accepting any business from Engility's customer for whom Daniels had provided work while working for Engility. Daniels had a "Confidentiality Agreement" with Engility, but did not have a covenant not to compete that would otherwise enjoin Daniels from doing business with Engility customers. Therefore, the *Engility* court considered whether under the DTSA (and applicable Colorado law) it could issue an injunction to prevent Daniels and his new employer from doing business with Engility's customers. The *Engility* court held that under the DTSA, it "may only enjoin competition or solicitation if, and to the extent, necessary to protect trade secrets."[29] After analyzing the factual claims, the Court found that an injunction prohibiting competition and solicitation was appropriate under the DTSA because Daniels did not appear credible, and an injunction was necessary to prevent Daniels and his new employer "from taking advantage of trade secrets in their possession."[30] The Court also found that irreparable harm under the DTSA "presumptively exists" if a defendant has misused or is likely to misuse trade secrets.[31] The *Engility* court undertook a thorough analysis of Colorado law since the DTSA expressly forbids issuing an injunction that would conflict with applicable state law. After determining there was no conflict between the DTSA and Colorado law, the *Engility* court issued a preliminary injunction prohibiting Daniels and his new employer from soliciting or accepting business with Engility's customer for a one year period.[32]

While the body of case law applying the DTSA is just now developing, it appears an important tool in enforcing and protecting trade secrets. The DTSA provides significant additional litigation options to safeguard trade secrets and should be considered in any litigation relating to the protection of trade secrets and confidential information.

ABOUT THE AUTHOR

ELISABETH S. GRAY works as a litigator, with Middleton Reutlinger, whose practice focuses on unfair competition, including disclosure of trade secrets and enforcing non-competition and non-solicitation agreements. She has also maintained a high familiarity with eDiscovery and related technology in order to provide defensible eDiscovery solutions for clients, as well as using eDiscovery to the client's advantage in seeking and obtaining eDiscovery from opposing parties. She has successfully obtained numerous court orders requiring the forensic examination of computers, smart phones, and other electronic devices. She received her undergraduate degree from the University of Oregon and her J.D. from Vanderbilt University.

ENDNOTES

1. *See* S. Rep. No. 114-220, at 14 (2016).
2. *See Protecting Trade Secrets: the Impact of Trade Secret Theft on American Competitiveness and Potential Solutions to Remedy This Harm: Hearing on S. 1890 Before the S. Comm. on the Judiciary*, 114th Cong. (2015) (statement of Thomas R. Beall, Vice President and Chief Intellectual Property Counsel, Corning Inc.) ("[T]his particular law is not intended to preempt state law.") (quoted language is from transcript of hearing).
3. The DTSA was passed 87-0 by the Senate and 410-2 by the House. 162 Cong. Rec. S1635-36 (daily ed. Apr. 4, 2016) and 162 Cong. Rec. H2046-47 (daily ed. Apr. 27, 2016).
4. *See, e.g., Syntel Sterling Best Shores Mauritius Ltd. v. Trizetto Grp., Inc.*, No. 15-cv-211, 2016 U.S. Dist. LEXIS 130918 (S.D.N.Y. Sept. 23, 2016) (finding that even where the basis of a DTSA claim began pre-DTSA, because plaintiff alleged the misappropriation was on-going and "continued to occur after the date of the enactment of DTSA," the plaintiff could amend its complaint to add a DTSA claim); *Adams Arms, LLC v. Unified Weapon Sys.*, No. 16-cv-1503, 2016 U.S. Dist. LEXIS 132201 (M.D. Fla. Sept. 27, 2016) (same).
5. 18 U.S.C. § 1836(d).
6. *Id.; see also* 3 Milgrim on Trade Secrets § 13.049[2].
7. *See, e.g.*, Cal. Civil Code § 3426.6 (three-year statute of limitations); Ohio Rev. Code Ann. § 1333.66 (four-year statute of limitations); 765 Ill. Comp. Stat. 1065/7 (five-year statute of limitations).
8. 18 U.S.C. § 1839(3).
9. *Id.*
10. *Id.* § 1839(5).
11. *Id.* § 1839(6).
12. *Id.* § 1839(4).
13. *Id.* § 1836(b)(1).
14. *Id.* § 1836(b)(3)(A)(i).
15. *Id.* § 1836(b)(3)(A)(i)(II).
16. *Id.* § 1833(b)(1).
17. *Id.* § 1833(b)(3).
18. *Id.* § 1833(b)(5).
19. *Id.* § 1836(b)(3)(A)-(B).
20. *Id.* § 1836(b)(3)(C).
21. *Id.* § 1836(b)(3)(D).
22. *Id.* § 1836(b)(2)(B).
23. *Id.* § 1836(b)(2)(A)(ii)(I).
24. *Id.* § 1836(b)(2)(A)(ii).
25. *Id.* § 1836(b)(2)(B).
26. *Id.* § 1836(b)(2)(B)(vi).
27. *Id.* § 1836(b)(2)(A)(i) ("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.") (emphasis added); S. Rep. No. 114-220 at 5 (2016).
28. No. 16-cv-2473, 2016 WL 7034976 (D.C. Colo. Dec. 2, 2016).
29. *Id.* at *11.
30. *Id.*
31. *Id.*
32. *Id.* at *14.