



# The Defend Trade Secrets Act

## Comparing the new federal statute with the UTSA.

BY ALEX HARRELL AND MICHAEL YIM

Marking a sea change in federal intellectual property law, on May 11, 2016, President Barack Obama signed into law S 1890, titled the Defend Trade Secrets Act of 2016, which establishes the first federal private right of action for trade secret misappropriation and opens the doors of federal courts to trade secrets litigants.

Unsurprisingly, mounting cybersecurity risks were the driving force that spurred this legislation. Indeed, the Senate specifically observed in its report that “[p]rotecting trade secrets has become increasingly difficult given ever-evolving technological advancements. Thieves are using increasingly sophisticated methods to steal trade secrets and the growing use of technology and cyberspace has made trade secret theft detection particularly difficult.”<sup>1</sup> The DTSA offers victims of misappropriation a new forum to seek redress for the harm caused by such acts of espionage.

Theft of trade secrets has been a federal crime since the passage of the Economic Espionage Act of 1996.<sup>2</sup> Prior to the DTSA, however, civil claims for trade secret misappropriation were the exclusive province of state law, which resulted in state-to-state variation on a number of important issues. Efforts at enhancing uniformity have been met with considerable success in recent years, as 48 states have adopted the Uniform Trade Secrets Act, a model statute aimed at bolstering trade secret protection for businesses operating across state lines. Texas was fairly

late to adopt the UTSA, having only enacted its version of the model statute in 2013.<sup>3</sup> Even with the widespread adoption of the UTSA, however, homogeneity has not been achieved.

The DTSA strengthens trade secret protections by furthering nationwide uniformity in this area of law. It is modeled largely upon the UTSA, and thus practitioners in Texas and other UTSA states should see much in the new law that looks familiar. The DTSA does not preempt state law,<sup>4</sup> though, and there are some notable distinctions between the UTSA and the DTSA that warrant special attention.

**Definition of Trade Secret.** In the DTSA, definitions for most key terms are strikingly similar to those found in the UTSA.<sup>5</sup> Some commentators, however, have suggested that the federal law defines “trade secret” more broadly than the UTSA.<sup>6</sup> Notably, the Texas UTSA provides that information may constitute a trade secret only if it comprises “a formula, pattern, compilation, program, device, method, technique, process, financial data, or list of actual or potential customers or suppliers . . . .”<sup>7</sup> The DTSA, on the other hand, does not limit the types of information that may constitute a trade secret, providing instead that: “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 ...”<sup>8</sup> The DTSA further clarifies that a trade secret may consist of “tangible or intangible” information and that it is irrelevant whether or how the information is “stored, compiled or memorialized.”<sup>9</sup> Thus, the DTSA arguably allows for a finding that information existing only in an employee’s mind constitutes an employer’s trade secret.<sup>10</sup>

**Interstate Commerce.** A DTSA action may be brought only if the trade secret at issue is one that “is related to a product or service used in, or intended for use in, interstate or foreign commerce.”<sup>11</sup> This stretches the statute to the limit of Congress’ commerce clause authority and precludes a DTSA action where the trade secret is not “used or intended for use” outside of the plaintiff’s home state. Of course, in the interconnected marketplace of the 21st century, misappropriation claims that are beyond a federal court’s DTSA jurisdiction will likely be the exception rather than the rule. For example, “[c]ourts have consistently held that the internet is an instrumentality and channel of interstate commerce such that any computer that is connected to the internet is part of a system that is inexorably intertwined with interstate commerce.”<sup>12</sup> Thus, any trade secret information related to a product or service that is sold or offered for sale via the internet is likely to satisfy the DTSA’s “interstate commerce” requirement.<sup>13</sup> Even in those seemingly rare instances where the requirement is not met, the plaintiff will not be without recourse; it will simply be limited to pursuing its claim in state court under state trade secret laws.

**Civil Seizure.** The civil seizure provision is the most notable aspect of the DTSA that separates it from the UTSA. Under that provision, the plaintiff may obtain an order on an ex parte basis directing a federal marshal to seize from the defendant the allegedly misappropriated trade secret.<sup>14</sup> The civil seizure remedy has long been available to trademark infringement litigants under the Lanham Act,<sup>15</sup> and federal courts applying the DTSA’s comparable provision may therefore look for guidance in Lanham Act jurisprudence.<sup>16</sup>

At first glance, civil seizure seems like a powerful tool. But such orders are subject to a number of limitations and may be employed “only in extraordinary circumstances.”<sup>17</sup> To issue a civil seizure order, a court must find that:

1. other forms of extraordinary relief, such as a temporary restraining order, would be inadequate because the restrained party would evade, avoid, or otherwise not comply;
2. the applicant will suffer “immediate and irreparable injury” without the order;
3. the harm the applicant will suffer “outweighs the harm to the legitimate interests” of the defendant;
4. the applicant will likely succeed at trial on the merits of its misappropriation claim;
5. the person against whom seizure is ordered has actual possession of the trade secret and any property to be seized;
6. if the applicant provided notice before the issuance of the order, the defendant would destroy, move, hide, or otherwise make the alleged trade secret inaccessible;
7. the application describes with reasonable particularity

the matter to be seized and, to the extent reasonable under the circumstances, identifies the location where the matter is to be seized; and

8. the applicant has not publicized the requested seizure.<sup>18</sup>

Consistent with federal court practice regarding temporary restraining orders, the plaintiff must provide security for the payment of damages to the defendant should it later be found that the seizure was wrongful or excessive.<sup>19</sup>

Even where the plaintiff meets its burden, the court may order only “the narrowest seizure of property necessary” to protect the alleged trade secret.<sup>20</sup> Moreover, the seizure must be “conducted in a manner that minimizes any interruption of the business operations of third parties” and, to the extent possible, will not interrupt the legitimate operations of the defendant.<sup>21</sup>

Setting aside its limitations, plaintiffs considering civil seizure as a litigation option should exercise caution. The DTSA requires a hearing not later than seven days after a civil seizure order is issued, at which time the court will determine if the order should be modified or dissolved.<sup>22</sup> If the court concludes the seizure was wrongful or excessive—terms the DTSA does not define<sup>23</sup>—the defendant may recover from the plaintiff its reasonable and necessary attorney’s fees, as well as damages for any lost profits, cost of materials, and loss of good will occasioned by the seizure.<sup>24</sup> The defendant may also recover punitive damages upon a showing that the plaintiff sought the seizure in bad faith.<sup>25</sup>

**Remedies.** Like the UTSA, the DTSA authorizes an injunction to prevent “actual or threatened misappropriation” and allows the plaintiff to recover monetary damages for the actual loss and any unjust enrichment caused or, alternatively, a reasonable royalty for the unauthorized disclosure or use of the trade secret.<sup>26</sup> The DTSA limits the scope of any injunction, however, by ostensibly restricting the application of the “inevitable disclosure doctrine,” a theory applied in a handful of UTSA states under which a court may enjoin “threatened” misappropriation by prohibiting a company’s former employee from competing with the company or accepting employment with one of its competitors if doing so would inevitably compromise any of the company’s trade secrets that the former employee knows.<sup>27</sup>

A DTSA injunction cannot “prevent a person from entering into an employment relationship” and the court may use the injunction to place conditions on a person’s employment only where there is “evidence of threatened misappropriation” and not merely evidence that the person knows the alleged trade secret.<sup>28</sup> Additionally, if the enjoined person resides in a state with laws prohibiting restraints on the practice of a lawful profession, trade or business, a DTSA injunction cannot conflict with those laws.<sup>29</sup>

A plaintiff may further recover under either the DTSA or UTSA its reasonable and necessary attorney’s fees where a trade secret has been “willfully and maliciously misappropriated,” together with exemplary damages of up to twice the amount of actual damages awarded.<sup>30</sup> Both laws also allow for the recovery of attorney’s fees by a defendant, where the court finds a claim of misappropriation was made in bad faith, and by a plaintiff, where the defendant moves to terminate or

opposes in bad faith an injunction.<sup>31</sup>

**Immunity Provisions.** The DTSA provides immunity from criminal or civil liability to any person who discloses a trade secret to a federal, state, or local government official solely for the purpose of reporting or investigating a suspected violation of the law.<sup>32</sup> Also, if an employer retaliates against an employee for reporting a suspected violation of the law by the employer, the DTSA permits the employee to disclose the employer's trade secret to his attorney and use it in any subsequent retaliation lawsuit, provided that the employee must: (1) file any document containing the trade secret under seal and (2) only disclose the trade secret pursuant to a court order.<sup>33</sup> The DTSA's immunity provisions contain no limitation with respect to the type of "suspected violation of the law." An employee is thus entitled to claim the benefit of the immunity provisions whether he discloses a trade secret to a government official or his counsel in the course of reporting a suspected violation by his employer of a criminal statute, an environmental regulation, a labor standard, or any other manner of law.

**Notice Requirements.** In any contract or agreement that governs the use of a trade secret, the DTSA obligates employers to provide notice to their employees of the federal law's immunity provisions.<sup>34</sup> If an employer fails to comply with this notice provision and later files suit against the employee for misappropriation of trade secrets, the DTSA bars the employer from recovering its attorney's fees or any exemplary damages.<sup>35</sup> This requirement only applies to contracts or agreements entered into or updated after DTSA's enactment in 2016, so companies need not race to renegotiate old agreements with their employees.<sup>36</sup> As to any new agreements or older contracts that are amended, however, companies should be mindful and ensure they have complied with the notice requirement. If they do not, the recourse available to them in any prospective DTSA suit is limited.

**Enhanced Criminal Penalty.** Recognizing the rising value of trade secrets in an ever more competitive and innovative marketplace, Congress also increased the criminal fine for trade secret misappropriation from \$5 million to "the greater of \$5,000,000 or 3 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."<sup>37</sup>

Congress aptly observed that "trade secret theft occurs in the United States and around the world" and "harms the companies that own trade secrets and the employees of the companies."<sup>38</sup> Broadly speaking, the DTSA mitigates the harm of trade secret misappropriation by augmenting existing protections and opening an alternative forum for claims. **TBJ**

## Notes

1. S. Rept. 114-220, § 1.
2. Pub. Law 104-294 (codified at 18 U.S.C. §§ 1831-39, 1030, 4243).
3. Tex. Civ. Prac. & Rem. Code § 134A.001, et seq.; see Joseph F. Cleveland Jr. and J. Heath Coffman, *Protecting Trade Secrets Made Simple*, 76 Tex. Bar J., No. 8, 751-56 (Sept. 2013). Bills adopting UTSA have also been introduced in New York and Massachusetts, the two remaining holdouts. See N.Y. Senate Bill S3770; Mass. House Bill H.4323.
4. 18 U.S.C. § 1838.
5. Compare Tex. Civ. Prac. & Rem. Code § 134A.002 with 18 U.S.C. § 1839.
6. See, e.g., Joseph D. Mornin, *What You Need to Know About the Defend Trade Secrets*

Act, 28 Intell. Prop. & Tech. L.J., No. 9, 20, 21 (Sept. 2016).

7. Tex. Civ. Prac. & Rem. Code § 134A.002(6).
8. 18 U.S.C. § 1839(3).
9. *Id.*
10. Mornin, 28 Intell. Prop. & Tech. L.J., No. 9 at 21.
11. 18 U.S.C. at § 1836(b)(1).
12. *Freedom Banc Morg. Servs., Inc. v. O'Harra*, No. 2:11-cv-01073, 2012 WL 3862209, \*6 (S.D. Ohio 2012) (quotation marks and citations omitted).
13. *RFA Brands, LLC v. Beauvais*, No. 13-14615, 2014 WL 7780975, \*10 (E.D. Mich. 2014) (noting that "plaintiffs presented evidence that defendant disseminated these statements through its internet advertising, and therefore demonstrated that the statements entered interstate commerce ..."); *PQ Labs, Inc. v. Yang Qi*, No. 12-0450 CW, 2014 WL 4954161, \*4 (N.D. Cal. 2014) ("By placing the advertisements on the internet, [the defendant] put them into interstate commerce.").
14. 18 U.S.C. at § 1836(b)(2).
15. 15 U.S.C. § 1116(d).
16. Peter J. Toren, *The Defend Trade Secrets Act*, 28 Intell. Prop. & Tech. L.J., No. 7, 3, 6 (July 2016) (noting that "[t]he only existing seizure remedy in intellectual property law is found at 15 U.S.C. § 116(d) of the Lanham Act" and postulating that courts may look for "guidance to this section in addressing [civil seizure] applications under the DTSA").
17. 18 U.S.C. at § 1836(b)(2)(A)(i).
18. *Id.* at § 1836(b)(2)(A)(ii)(I)-(VIII).
19. *Id.* at § 1836(b)(2)(B)(vi).
20. *Id.* at § 1836(b)(2)(B)(ii).
21. *Id.* If the material seized is electronically stored information, any party claiming an interest in the information may make a motion at any time—which may likewise be heard on an ex parte basis—for an order to encrypt the storage medium on which the information resides. *Id.* at § 1836(b)(2)(H).
22. *Id.* at §§ 1836(b)(2)(B)(v), (b)(2)(F).
23. Since courts applying the DTSA's civil seizure provision may look for guidance to Lanham Act jurisprudence, it should be noted that the Lanham Act similarly provides an aggrieved defendant with remedies in the event of a "wrongful" seizure, though the act does not explicitly address "excessive" seizures. 15 U.S.C. § 1116(d). Courts interpreting the Lanham Act's civil seizure provision have noted that "Congress intentionally left the definition of 'wrongful seizure' to 'case-by-case interpretation.'" *Waco Int'l, Inc. v. KHK Scaffolding Houston, Inc.*, 278 F.3d 523, 530 (5th Cir. 2002) (citing Joint Statement on Trademark Counterfeiting Legislation, 130 Cong. Rec. H12076, at 12083 (Oct. 10, 1984)). Generally speaking, to establish a claim for wrongful seizure under the Lanham Act, "the claimant must show: (1) that the seizure was brought in bad faith; or (2) that the items seized were predominately legitimate." *Ford Motor Co. v. O.E. Wheel Distributors, LLC*, 868 F.Supp.2d 1350, 1371 (M.D. Fla. 2012) (citing *Martin's Herend Imports v. Diamond & Gem Trading*, 193 F.3d 765, 773 (5th Cir. 1999))."
24. *Id.* at § 1836(b)(2)(G). (providing that "[a] person who suffers damage by reason of a wrongful or excessive seizure . . . has a cause of action against the applicant for the order under which such seizure was made, and shall be entitled to the same relief as is provided under section 34(d)(11) of the Trademark Act of 1946 (15 U.S.C. § 1116(d)(11))").
25. *Id.*
26. *Id.* at § 1836(b)(3); Tex. Civ. Prac. & Rem. Code §§ 134A.003(a), 134A.004(a).
27. See, e.g., *Moore v. Comm. Aircraft Interiors, LLC*, 278 P.3d 197, 202 (Wash. Ct. App. 2012) (noting that the inevitable disclosure doctrine is applicable without regard to whether there is any evidence of affirmative misconduct by the former employee); 849 A.2d 451, 468 (Md. 2004) (observing that the inevitable disclosure doctrine is "based on the original employer's claim that a former employee who is permitted to work for a competitor will—even if acting in the utmost good faith—inevitably be required to use or disclose the former employer's trade secrets in order to perform the new job").
28. 18 U.S.C. § 1836(b)(3)(A)(i)(I).
29. *Id.* at § 1836(b)(3)(A)(i)(II).
30. *Id.* at § 1836(b)(3)(C), (D); Tex. Civ. Prac. & Rem. Code §§ 134A.003(a), 134A.004(b), 134A.005.
31. 18 U.S.C. § 1836(b)(3)(D); Tex. Civ. Prac. & Rem. Code § 134A.005.
32. 18 U.S.C. § 1833(b)(1).
33. *Id.* at § 1833(b)(2).
34. *Id.* at § 1833(b)(3)(A).
35. *Id.* at § 1833(b)(3)(C).
36. *Id.* at § 1833(b)(3)(D).
37. *Id.* at § 1832(b).
38. Pub. Law 114-153, § 5.



### ALEX HARRELL

is an associate in the Dallas office of Drinker Biddle & Reath. He has extensive experience handling trade secrets cases and serves on the Trade Secrets Committee of the Intellectual Property Section of the State Bar of Texas, which monitors federal and state statutes and judicial decisions relating to the protection and misappropriation of trade secrets.



### MICHAEL YIM

is a partner in Sedgwick's New York office. He is a member of the firm's labor and employment team and litigates noncompete and trade secret matters nationwide.