# How Energy Firms Can Use The Defend Trade Secrets Act

Law360, New York (November 16, 2016, 3:55 PM EST) –

*Benjamin Fernandez*

*Natalie Hanlon Leh*

*Kirsten Donaldson*

Whether it's hydraulic fracturing fluid ingredients, customer lists, geologic and seismic data or employee know-how, energy companies routinely face trade secret issues. With the enactment of the federal Defend Trade Secrets Act in 2016, energy companies have an additional tool to help them safeguard against misappropriation of their proprietary information.

**What Was the Trade Secrets Landscape Like Before the DTSA?**

Before enactment of the DTSA, no federal civil case of action was available to private litigants for trade secret misappropriation. The only federal protection was through a criminal trade secret statute, which required the Federal Bureau of Investigation (FBI) to file suit on behalf of private companies.

Unless private individuals and companies were able to bring a claim under diversity jurisdiction or another federal jurisdictional hook, the only civil remedy available to combat trade secret misappropriation prior to the DTSA was to bring a civil lawsuit under a patchwork of state tort laws based largely on the Uniform Trade Secrets Act (UTSA).

The UTSA is a framework recommended by the Uniform Law Commission that has been enacted in slightly different forms in 48 states.[1] Many saw the UTSA as a step forward to codify and harmonize standards and remedies regarding trade secret theft, despite slight variations from jurisdiction to jurisdiction due to changes states made during adoption of the UTSA and differences in the way state courts interpreted the law.

The notable doctrine of “inevitable disclosure” also arises from the UTSA. This doctrine allows employers to seek injunctive relief against former employees when it is unavoidable or inevitable that the employee will unlawfully make use of the employer's trade secrets.[2]

States have exercised varying degrees of hesitancy in adopting and enforcing this doctrine. The Texas Uniform Trade Secrets Act, however, which entered into effect on Sept. 1, 2013, embraces the inevitable disclosure doctrine wholeheartedly[3] and permits issuance of injunctive relief in connection with threatened trade secret misappropriation.

As state civil laws were not preempted by the federal DTSA, the inevitable disclosure doctrine may provide another tool to prevent trade secret theft, particularly where robustly enacted, as in Texas.

**What Changed With Enactment of the DTSA?**

Enacted on May 11, 2016, the DTSA amended the Economic Espionage Act (EEA) of 19964 to provide owners of trade secrets with a federal cause of action for trade secret misappropriation if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce.[5]

The term "trade secret" is broadly defined,[6] and covers all forms of information for which the owner has taken reasonable measures to keep secret and that have independent economic value as a result of not being generally known.[7] Trade secrets could include confidential formulas, manufacturing techniques, customer lists or any other type of financial, scientific, technical, engineering or vital information which the company takes affirmative steps to keep secret.

Unlike patents and copyrights, trade secrets do not have expiration dates so long as they remain secret. And unlike patents, trade secrets can be protected without any registration, and without need for publication or public disclosure. However, there is one potential downside of trade secrets: once a trade secret is disclosed, all protections cease, unlike other forms of intellectual property.

Pursuant to the DTSA, private individuals and companies now have the ability to bring federal claims for misappropriation of trade secrets under a statute of nationwide applicability. The DTSA attempts to fill in the gaps that were lacking in the patchwork of state civil laws, which many expect to result in greater predictability in trade secret litigation.

Some key provisions of the DTSA include:

1. Statute of Limitations. In alignment with the UTSA, the DTSA provides for a three-year statute of limitations running from "the date on which the misappropriation with respect to which the action would relate is discovered or by the exercise of reasonable diligence should have been discovered."[8]
2. Civil Seizure. The DTSA authorizes federal courts to issue a narrowly-tailored ex parte order for seizure of property necessary in "extraordinary circumstances" to preserve evidence or to prevent the propagation or dissemination of the trade secret.[9] The purpose of this provision is to enable a trade secret owner to proactively contain a theft before it progresses and the trade secret is compromised.[10]
3. Employee Mobility. The DTSA establishes greater mobility for employees by requiring an employer to provide evidence of threatened misappropriation before a court can enjoin a former employee from entering into a new employment relationship.[11]
4. Immunity and the Notice of Immunity Requirement. The DTSA adds provisions to the EEA providing limited immunity for individuals who disclose trade secrets under specific circumstances, and requiring employers to provide notice of these immunity provisions to the employee.[12]

**How Do Energy Companies Encounter Trade Secrets?**

Companies that refine crude oil or process petrochemicals often employ trade secrets in protecting their methods, for example, by shielding their plants from public view and restricting access.

Extraction and harvesting companies often possess nonpublic seismic and other geological or mineralogical testing data that confers a competitive or business advantage, and often guard the formulations for certain mixtures or compositions used in extracting, storing or early processing of the resource, for example, the chemical composition of hydraulic fracturing fluid. And most companies deal in basic forms of proprietary information — for example, customer lists and contact information — which those companies would not like to send along with a departing employee.

As seen in the case of Southwestern Energy Production Company v. Berry-Helfand, 491 S.W.3d 699 (Tex. 2016), trade secret misappropriation claims can be founded on allegations of misappropriating geological research and analysis performed under a nondisclosure agreement.[13]

On the renewable side of the industry, as observed in the case in which Chinese wind turbine company Sinovel was charged with stealing proprietary information from US company AMSC (formerly American Superconductor Corporation), trade secrets can include design of software for controlling flow of electricity in wind turbines.[14]

**Why Do Trade Secrets Matter in the Energy Sector?**

As employees (sometimes even key employees) in the energy industry move from company to company due to economic downturns or M&A activity, prevention of trade secret misappropriation takes center stage.

Increased government regulation of certain energy industries also intensifies the spotlight on trade secrets, particularly in cases where the government seeks disclosure of proprietary information on the basis of public safety or compliance.[15]

Private sector competitors are not the only ones hunting for trade secrets — the FBI continues to warn against industrial espionage threats against energy and infrastructure companies from foreign governments.[16]

**What Should Energy Companies Do Now?**

Should an employee or contractor walk out the door with a valuable trade secret, before granting relief on a claim under the DTSA, courts will expect the owner of the trade secret to identify the trade secret and explain which measures were taken to reasonably protect its secrecy.

Energy companies wanting to establish robust trade secret protection should begin by identifying and documenting what they consider to be their trade secrets. Next, those companies should review their policies and procedures to ensure that the level of protection for the information is commensurate with its value to the company.

This process can include:

• designing and conducting confidentiality training for new hires;
• regularly documenting employee acknowledgment of confidentiality and information technology policies;
• limiting access to trade secret information to those who need to know the information;
• keeping visitor logs and visitor escort policies;
• augmenting IT measures for both controlling and monitoring access to sensitive information;
• conducting exit interviews for departing employees to inform about and ensure compliance; and
• auditing form employee and consultant agreements relating to confidentiality.

Most importantly, when a genuine problem arises, the trade secret owner should not hesitate to take action by seeking injunctive relief or a cease-and-desist order.

*Benjamin S. Fernandez is a partner at WilmerHale, with experience in patent portfolio management, freedom to operate/competitive landscape and IP diligence. Natalie Hanlon Leh is also a partner at the firm, and serves as lead counsel in patent, copyright, trademark and trade secrets matters. Kirsten Donaldson is of counsel to WilmerHale, working with clients in areas including intellectual property, technology policy, corporate law and administrative practice and procedure.*



[1] The only states that have not adopted the UTSA are New York and Massachusetts.

[2] See Uniform Trade Secrets Act § 2(a) (1985).

[3] See Texas Uniform Trade Secrets Act § 134A.003.

[4] 18 U.S.C. § 1831-1836.

[5] Id. § 1836 (b)(1).

[6] The DTSA definition closely tracks the definition in the Uniform Trade Secrets Act.

[7] 18 U.S.C. § 1839(3).

[8] 18 U.S.C. § 1833(d).

[9] Id. § 1833(b)(2).

[10] S. Rep. No. 114-220, at 3 (2016).

[11] 18 U.S.C. § 1833(b)(3)(A).

[12] Id. § 1833(b).

[13] 491 S.W.3d 699, 713 (Tex. 2016).

[14] www.nytimes.com/2013/06/28/business/energy-environment/chinese-firm-is-charged-in-theft-of-turbine-software.html.

[15] See, for example, government efforts and industry response to regulations requiring disclosure of hydraulic fracturing fluid compositions. www.eenews.net/stories/1059998371.

[16] See, for example, www.houstonchronicle.com/news/houston-texas/houston/article/Concerns-for-energy-espionage-climb-as-oil-7951534.php.