THOMSON REUTERS

Westlaw®

An overview of trade secrets law

By Paul D. Ackerman, Esq., and Aimee N. Soucie, Esq., *Hunton Andrews Kurth

APRIL 8, 2020

Trade secrets are ubiquitous and can be critically important intellectual property assets.

While famous examples include the formula for Coca Cola and spice blend for Kentucky Fried Chicken, trade secret protection extends broadly to nearly any business information that has value because it is not generally known to others in the trade.

By understanding the federal and state laws available to protect trade secrets, businesses can take the steps needed to insure that these valuable assets remain protected.

PART I — STATUTORY & COMMON LAW FRAMEWORK FOR TRADE SECRET PROTECTION

State trade secrets laws

Historically, trade secret law developed unevenly from state to state. In an effort to establish uniformity, in 1979 the Uniform Law Commission first published the Uniform Trade Secrets Act (UTSA), which defines a trade secret as:

information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

(i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and

(ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

The UTSA has been widely adopted by every state except New York. Although there are still variations from state to state, a discussion of the UTSA provides a solid foundation to understand state laws protecting trade secrets.

There is no formal registration requirement for protecting a trade secret. But the trade secret must remain secret and the rights holder must take steps to maintain its secrecy. What this means varies by case, since the standard is one of "reasonable under the circumstances."

Certainly, identifying trade secret information as confidential, limiting access to individuals who "need to know," and having employees enter nondisclosure agreements are starting points.

Although multiple parties may hold rights to the same trade secret, (if they each (i) obtained it properly, such as through independent development, (ii) continue to maintain its secrecy, and (iii) continue to derive value from the information,) a trade secret loses protectable status if it becomes common knowledge within the trade in which it has value.

The UTSA provides a civil cause of action for misappropriation, including both acquisition of a trade secret by improper means and improper disclosure.[1]

Under the UTSA, "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." The UTSA also recognizes "proper means" of obtaining a trade secret, *e.g.*, reverse engineering.

Although multiple parties may hold rights to the same trade secret ... a trade secret loses protectable status if it becomes common knowledge within the trade in which it has value.

The UTSA provides a trade secret owner with remedies including injunctive relief, damages, and attorney's fees.[2] Injunctive relief may include a suitably tailored injunction to enjoin "actual or threatened misappropriation."

The UTSA provides that "in exceptional circumstances, an injunction may condition future use" of the misappropriated trade secret on payment of a reasonable royalty. This compulsory license is intended for cases where "a prohibitive injunction is inequitable."

Monetary damages may include damages for actual loss caused by misappropriation, as well as unjust enrichment. Damages can also be in the form of a reasonable royalty. In the case of "willful and malicious" misappropriation, the UTSA provides for exemplary damages.

The UTSA also authorizes attorney's fees in certain circumstances, including potential liability against a party asserting misappropriation, if the claim is made in bad faith, or against a misappropriator, if it is determined that "willful and malicious misappropriation exists."

Trade secrets in New York state

Instead of the UTSA, New York relies on common law, including Section 757 of the Restatement of Torts.

New York courts have adopted the trade secret definition: any "formula, pattern, device or compilation of information which is used in one's business, and which gives [the employer] an opportunity to obtain an advantage over competitors who do not know or use it."[3]

To determine whether information qualifies as a trade secret, New York courts apply a six-factor inquiry from the Restatement. Unlike the UTSA, there is no baseline requirement to engage in "efforts that are reasonable under the circumstances to maintain its secrecy," though it is one of the six factors.

> A party injured by trade secret misappropriation may seek relief from the ITC even if that party is not using the trade secret in the US.

Also unlike the UTSA, in New York, a trade secret must be for "a process or device for *continuous use* in the operation of the business."[4] Another notable difference is that attorney's fees are far more limited under New York law.

Federal civil trade secrets law

In 2016, the Defend Trade Secrets Act (DTSA) was enacted to provide federal protection for trade secrets. The DTSA is complementary to existing state law and does not preempt it.

Like the UTSA, the DTSA provides both injunctive relief and money damages. With respect to injunctive relief, two provisions of the DTSA that vary from the UTSA are noteworthy.

First, the statute expressly provides for *ex parte* civil seizure in extraordinary circumstances.

This is "to prevent the propagation or dissemination of the trade secret that is the subject of the action," a powerful tool for rights owners but one tempered with protections for defendants, including requirements for: a prompt hearing following seizure, use of a special master to facilitate return of seized property unrelated to the allegedly misappropriated trade secret, and the rights holder to post security in the event of "wrongful or excessive seizure."[5]

Second, the DTSA expressly limits the scope of injunctions. Specifically, while courts may issue an injunction "to prevent any actual or threatened misappropriation," it may not "prevent a person from entering into an employment relationship," place limits on employment based "merely on the information a person knows," or conflict with state law prohibiting restraints on employment.[6]

The DTSA does not preclude all injunctions limiting an employment relationship, but requires more than a mere inference of potential disclosure based solely on the employee's knowledge.

This is intended to strike a balance between the legitimate competing interests of protection for trade secret owners and an individual's right to work.

Trade secrets in the US International Trade Commission

Another venue to pursue trade secret misappropriation claims is the US International Trade Commission (ITC), which investigates allegations of unfair competition related to intellectual property rights with respect to products that enter the US from abroad.

Section 337 of the Tariff Act of 1930, as amended, governs these unfair acts (and specifically, 19 U.S.C. § 1337(a)(1)(A) governs trade secret misappropriation).

A trade secret owner has a cause of action in the ITC even if misappropriation occurs entirely abroad.[7] This makes it attractive because foreign companies not otherwise subject to US jurisdiction can be subject to jurisdiction in the ITC.

The only remedy in the ITC is injunctive relief in the form of an exclusion order preventing importation into and/or sale in the US of the offending products (and a cease and desist order to prevent sale of existing US inventory).

Exclusion orders in trade secret related investigations can be in force for up to 10-25 years.[8]

The Federal Circuit held in 2011 that the issue of trade secret misappropriation in the ITC "is one of federal law and should be decided under a uniform federal standard, rather than by reference to a particular state's tort law."[9]

Prior to enactment of the DTSA in 2016, the ITC interpreted this to mean that it should apply the UTSA, Restatement (Third) of Unfair Competition, and/or federal common law; although an ITC opinion on trade secret misappropriation has yet to issue post-DTSA, parties have begun including it in their trade secret-based ITC complaints.[10]

A party injured by trade secret misappropriation may seek relief from the ITC even if that party is not using the trade secret in the US, as long as the accused products were imported, use the stolen trade secret, and compete with any products manufactured domestically by the injured party.[11]

Federal criminal trade secret statutes

Several federal statutes impose criminal penalties for trade secret theft. Most notable are the Economic Espionage Act of 1996 (EEA) and Computer Fraud and Abuse Act (CFAA).

The EEA criminalizes two forms of trade secret misappropriation, "economic espionage," which requires a theft "knowing that the offense will benefit any foreign

government, foreign instrumentality, or foreign agent," and "theft of trade secrets," which applies to theft "intending or knowing that the offense will, injure any owner of that trade secret," and in both cases, penalties are severe.[12]

For economic espionage, individuals face up to $5,000,000 in fines and up to 15 years' imprisonment, and organizations face fines up to $10,000,000 or three times the value of the stolen trade secret.

For commercial theft, individuals face fines and up to 10 years' imprisonment and organizations may be fined up to $5,000,000 or three times the value of the stolen trade secret.

Although not specifically directed to trade secret theft, the CFAA has been used in criminal prosecutions where electronically-based trade secrets are taken from a computer system.

> Historically, the DOJ has prioritized prosecutions of cases involving acts of foreign espionage.

The CFAA provides criminal penalties for knowingly accessing a computer without authorization or exceeding authorized access, to obtain "information contained in a financial record of a financial institution," "information from any department or agency of the United States," or "information from any protected computer," which includes any computer "used in or affecting interstate or foreign commerce or communication."[13]

This could be nearly any device used by a business and connected to the internet.

Fines and penalties under the CFAA vary but, in cases "where the offense was committed for purposes of commercial advantage or private financial gain," an individual may be fined and face up to five years' imprisonment.[14]

There is also an opportunity for "restitution" under the EEA and CFAA under 18 U.S.C. § 3663, the Mandatory Victims Restitution Act.

Restitution can include payment for "expenses related to participation in the investigation or prosecution of the offense or attendance at proceedings related to the offense."

PART II — RECENT TRADE SECRETS CASES AND ENFORCEMENT TRENDS

Recent civil trade secrets cases

According to Lex Machina, over 1,100 trade secrets cases were filed in 2017, a more than 30% increase over 2016.[15]

One of the higher-profile cases over the last few years is *Waymo v. Uber*,[16] filed in the Northern District of California in February 2017, alleging trade secret theft (under the DTSA and California's UTSA) by Anthony Levandowski, a prominent engineer on Waymo's self-driving car project.

The complaint alleged Levandowski downloaded thousands of files before leaving Waymo to start his own self-driving technology company, Ottomotto (Otto). Within months of formation, Otto was acquired by Uber.

Waymo allegedly learned of the theft secrets when it was inadvertently copied on an email from a component supplier attaching drawings of an Uber circuit board that was strikingly similar to Waymo's design.

The case settled five days into trial with Uber issuing a written apology and paying Waymo with equity reportedly valued over $200 million.

A case recently decided under Florida's UTSA, *Yellowfin Yachts v. Barker Boatworks*, provides guidance on what constitutes efforts "reasonable under the circumstances" to maintain the secrecy of a trade secret.

Yellowfin alleged that certain "customer information" was a trade secret taken by its former vice president of sales, Kevin Barker, who founded a competing company.

Yellowfin further alleged that it took reasonable steps to protect secrecy by limiting employee access to customer information and maintaining the information on a password-protected computer system.

But Yellowfin had provided a copy of the information to Barker, who had not signed a confidentiality agreement, and encouraged him to maintain the information on his personal laptop.

The court held that "Yellowfin effectively abandoned all oversight in the security of the Customer Information…[and] no reasonable jury could find that Yellowstone employed reasonable efforts to secure the information."[17]

Thus, it is not enough to have reasonable systems in place to protect the secrecy of a trade secret; those systems must be consistently followed.

Bladeroom Group v. Emerson Electric, a recent decision from the Northern District of California, provides guidance on awards of exemplary damages and attorney's fees under California's UTSA.

The court found that "after Facebook expressed to Emerson the desire for a data center consistent with Bladeroom's technology, employees from Emerson (and Facebook) lured Bladeroom into revealing its trade secrets under the guise of a potential data center contract or corporate acquisition, and then used the information it obtained to surreptitiously design and build Facebook's data center at Lulea 2," noting "from a

commercial ethics perspective, the misconduct certainly falls within the category of reprehensible," and ordering Emerson to pay $30 million in exemplary damages and Bladeroom's attorney's fees because "Emerson's misappropriation of trade secrets was willful and malicious."[18]

Recent criminal trade secrets enforcement

Historically, the DOJ has prioritized prosecutions of cases involving acts of foreign espionage. Recently, the focus on economic espionage with ties to China has increased.

On November 1, 2018, then US Attorney General Jeff Sessions announced the "China Initiative" to "identify priority Chinese trade theft cases, ensure that we have enough resources dedicated to them, and make sure that we bring them to an appropriate conclusion quickly and effectively."[19]

On the same day, the DOJ unsealed an indictment against United Microelectronics, a Taiwan-based semiconductor foundry; Fujian Jinhua Integrated Circuit Co.; and three Taiwan nationals, alleging trade secret theft from US company Micron Technology.

In addition to the criminal indictment, the DOJ filed a civil action to prevent the defendants from exporting the allegedly stolen technology to the US to compete with US firms.

Throughout 2019, indictments involving alleged theft by Chinese actors continued to be unsealed. For example, in January 2019, the DOJ unsealed a 10-count indictment in the Western District of Washington against Huawei "alleging theft of trade secrets conspiracy, attempted theft of trade secrets, seven counts of wire fraud, and one count of obstruction of justice."

And in April 2019, an indictment was unsealed in the Northern District of New York charging a Chinese businessman and former General Electric (GE) engineer with "economic espionage and conspiring to steal GE's trade secrets surrounding turbine technologies...."[20]

CONCLUSION

Trade secrets can be a critically important asset to nearly any business. And the US provides multiple venues to pursue both civil and criminal penalties for misappropriation.

However, to fully enjoy the protection available for their "crown jewels," businesses must take affirmative steps — to both recognize and protect their trade secrets.

Notes

1 UTSA § 1(2).

2 UTSA §§ 2-4 (with 1985 Amendments).

3 *Ashland Mgt. v. Janien*, 82 N.Y.2d 395, 407 (1993).

4 *Softel, Inc. v. Dragon Med. & Scientific Commc'ns, Inc.*, 118 F.3d 955, 968 (2d Cir. 1997) (emphasis added).

5 18 U.S.C. §§ 1836(b)(2)(A)(i), (B), (C), and (D).

6 18 U.S.C. § 1836(b)(3)(A)(i).

7 *Tianrui v. U.S. Int'l Trade Comm'n*, 661 F.3d 1322, 1332 (Fed. Cir. 2011)

8 *See, e.g., Organik Kimya v. U.S. Int'l Trade Comm'n*, 848 F.3d 994, 1004-06 (Fed. Cir. 2017) (affirming 25-year exclusion order); *Crawler Cranes and Components Thereof,* Inv. No. 337-TA-887, Comm'n Op. at p. 70-72 (May 6, 2015) (issuing 10-year exclusion order).

9 *Tianrui*, 661 F.3d at 1327.

10 *See, e.g. Crawler Cranes*, Inv. No. 337-TA-887, Comm'n Op. at p. 34 (pre-DTSA) and *Foodservice Equipment and Components Thereof*, Dkt. No. 3390, Complaint at ¶ 58 (filed May 30, 2019) (post-DTSA).

11 *See, e.g., Crawler Cranes*, Inv. No. 337-TA-887, Comm'n Op. at pp. 34, 51-52; *Rubber Resins and Processes for Manufacturing Same,* Inv. No. 337-TA-849, Comm'n Op. at pp. 60-64 (Feb. 26, 2014).

12 18 U.S.C. §§ 1831-1832.

13 18 U.S.C. §§ 1030(a)(2) and (e)(2).

14 18 U.S.C. § 1030(c)(2).

15 *See* https://bit.ly/2x8PrVz.

16 *Waymo LLC v. Uber Techs., Inc.*, 3:17-cv-00939, N.D. Cal.

17 *Yellowfin Yachts, Inc. v. Barker Boatworks, LLC*, 898 F.3d 1279, 1301 (11th Cir. 2018).

18 *Bladeroom Group v. Emerson Electric,* 5:15-cv-01370-EJD (N.D. Cal.), Docket Entry 956, Order at p. 4 (Mar. 11, 2019).

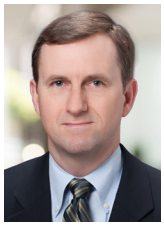
19 China Initiative Fact Sheet (Nov. 1, 2018), https://bit.ly/39pDfOy.

20 *See* https://bit.ly/2IwSbyJ.

This article first appeared in the April 8, 2020, edition of Westlaw Journal Intellectual property.

* © 2020 Paul D. Ackerman, Esq., and Aimee N. Soucie, Esq., Hunton Andrews Kurth

ABOUT THE AUTHORS



Paul D. Ackerman (L) is a partner at **Hunton Andrews Kurth** in New York whose practice involves all aspects of intellectual property law, with an emphasis on technology-related litigation. He can be reached at paulackerman@huntonak.com. **Aimee N. Soucie** (R) is a special counsel in the firm's Washington office whose practice focuses on patent and trade secret litigation at the U.S. International Trade Commission. She can be reached at asoucie@huntonak.com. A version of this article was previously published in the International Law Practicum, October 2019, Vol. 32, No. 1, a publication of the International Law Section of the New York State Bar Association, 1 Elk Street, Albany, NY 12207. Reprinted with permission.