The Defend Trade Secrets Act: Examining the DTSA's Language, Use, and Future

Authors: Michael Renaud, Bret Cohen, and Nicholas Armington, Mintz Levin Cohn Ferris Glovsky and Popeo PC

American corporations face an increasing threat of misappropriation of valuable trade secrets through corporate espionage. Indeed, former Attorney General Eric Holder stated that "[t]here 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." The newly enacted Defend Trade Secrets Act (DTSA) provides a robust new tool to combat trade secret theft in an age of ubiquitous connectivity that allows for easy transfer of digital information. This article explains the salient provisions of the DTSA, examines the implications of early judicial decisions applying the DTSA, and discusses the possible future impact the DTSA will have on trade secret litigation in United States district courts and at the International Trade Commission.

Provisions of the DTSA

The DTSA creates a federal private civil cause of action for trade secret misappropriation that allows an owner of a stolen trade secret to bring a civil action "if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce." Civil remedies for trade secret misappropriation previously were exclusively a matter of state law. With the passage of the DTSA, United States district courts have original jurisdiction over civil actions for trade secret theft for the first time. Importantly, the DTSA does not preempt existing state trade secret laws, but exists in parallel with state trade secret law regimes, giving corporations affected by trade secret misappropriation options with which to address trade secret theft.

The DTSA defines "trade secret" broadly, as follows:

> 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, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—
>
> > (A) the owner thereof has taken reasonable measures to keep such information secret; and
> >
> > (B) 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.

This definition does not differ significantly from the definition for trade secret in the Uniform Trade Secrets Act (UTSA), a model act created by the Uniform Law Commission, and adopted by the vast majority of U.S. states (Massachusetts and New York being the only exceptions).

Misappropriation is also defined specifically as follows:

> (A) 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
>
> (B) disclosure or use of a trade secret of another without express or implied consent by a person who—
>
> > (i) used improper means to acquire knowledge of the trade secret;
> >
> > (ii) at the time of disclosure or use, knew or had reason to know that the knowledge of the trade secret was—
> >
> > > (I) derived from or through a person who had used improper means to acquire the trade secret;
> > >
> > > (II) acquired under circumstances giving rise to a duty to maintain the secrecy of the trade secret or limit the use of the trade secret; or
> > >
> > > (III) derived from or through a person who owed a duty to the person seeking relief to maintain the secrecy of the trade secret or limit the use of the trade secret; or
> >
> > (iii) before a material change of the position of the person, knew or had reason to know that—
> >
> > > (I) the trade secret was a trade secret; and
> > >
> > > (II) knowledge of the trade secret had been acquired by accident or mistake.

Interestingly, the terms of the Economic Espionage Act (EEA), which the DTSA modifies, suggest that the DTSA could be used to remedy misappropriation of trade secrets even where the theft occurs outside of the United States. Specifically, the EEA includes a provision relating to its applicability to conduct outside the United States, indicating that the law applies to conduct occurring outside the United States if the offender (1) is a citizen or permanent resident of the United States, (2) United States corporation, or (3) if "an act in furtherance of the offense was committed in the United States." This provision was not changed by the DTSA's amendment of the EEA, suggesting that the DTSA may be applicable to trade secret misappropriation that takes place overseas. Such overseas application may be especially useful given the increase in economic and corporate espionage originating in China. "Chinese actors are the world's most active and persistent perpetrators of economic espionage." Compounding this threat is the reality that "[s]ignificant structural and institutional impediments undermine effective IPR enforcement in China[, including] a lack of coordination among government agencies, insufficient resources for enforcement, local protectionism, and a lack of judicial independence." Given the difficulties of enforcing IP rights in China, the EEA's applicability to overseas conduct may prove very valuable to victims of trade secret theft.

Civil Seizure Mechanism and Other Remedies

The DTSA provides for a civil seizure mechanism allowing a court to order the seizure of property by United States marshals necessary to prevent the dissemination of stolen trade secrets. Using this tool, an American company may be able to quickly prevent distribution of misappropriated trade secret information before the completion of a formal DTSA case. Civil seizure can occur only in "extraordinary circumstances" and requires a showing that:

- an order pursuant to Fed. R. Civ. P. 65 or other equitable relief would be inadequate;
- an immediate and irreparable injury will occur if seizure is not ordered;
- harm to the applicant from denial of a seizure order (1) outweighs the harm to the person against whom seizure is ordered, and (2) substantially outweighs the harm to any third parties by such seizure;
- applicant is likely to succeed in showing that the person against whom the order is issued misappropriated or conspired to misappropriate a trade secret through improper means;
- the person against whom the order will be issued has possession of the trade secret and any property to be seized;
- the application describes with reasonable particularity the matter to be seized and, to the extent reasonable under the circumstances, the matter's location;
- the person against whom seizure is ordered would destroy, move, hide, or otherwise make such matter inaccessible to the court if on notice; and
- the applicant has not publicized the requested seizure.

Once a court finds that misappropriation has occurred, it may grant an injunction to prevent potential future misappropriation. Notably, any such injunction cannot prevent an individual from entering into an employment relationship, and any conditions placed on employment must be based on actual evidence of threatened misappropriation and not merely on the individual's knowledge. Additionally, a company may be entitled to punitive damages or attorney's fees where an employee is found to have misappropriated trade secrets and where the whistleblower notice provision has been satisfied (discussed further below).

Whistleblower Immunity and Notice Requirement

Employers should be keenly aware of the notice provision within the whistleblower immunity section of the DTSA because compliance with the notice provision may impact whether an employer is entitled to certain relief under the statute. The DTSA's whistleblower immunity protects employees from liability for disclosure of trade secrets to an attorney or government official for the purpose of reporting illegal activity. To take advantage of punitive damages and attorney's fees under the statute, employers must advise their employees of the existence of the whistleblower immunity. Companies can satisfy the notice requirement by providing notice of the immunity in an employment or other agreement that governs the use of trade secret

information or by cross-referencing a policy document that includes a statement about the DTSA's whistleblower immunity. Therefore, employers should consider revamping their confidentiality and other employment agreements to include the DTSA notice.

DTSA Jurisprudence

Thus far, the DTSA has been used to address misappropriation of trade secrets by former employees. Two such cases are discussed below.

Henry Schein, Inc. v. Cook, Case No. 16-cv-03166 (N.D. Cal.)

In the first decision under the DTSA, the U.S. District Court for the Northern District of California granted a temporary restraining order (TRO) and preliminary injunction preventing a sales consultant from using or sharing confidential data that she allegedly stole from her former employer. Plaintiff Henry Schein, Inc. (HSI) alleged that before leaving HSI, the defendant misappropriated trade secrets by (1) forwarding to her personal email numerous proprietary customer related reports, (2) failing to return her work laptop containing sensitive customer related data for a number of weeks, and (3) remotely accessing proprietary ordering and purchasing data following her resignation.

The Court found that HSI was likely to suffer irreparable injury due to loss of customer relationships and economic value of accumulated customer data because the defendant was allegedly using misappropriated customer data in efforts to divert HSI customers to her new employer. The TRO and preliminary injunction prohibited the defendant from accessing or using the trade secret information and granted HSI's request that the defendant be required to preserve the materials she allegedly misappropriated. A further discussion of this case can be found here.

Monsanto Co. v. Chen, Case No. 4:16-cv-876 (E.D. Mo.)

In another recent case under the DTSA, Monsanto Company and The Climate Corporation (collectively, "Monsanto") sought a TRO and preliminary injunction after a former employee, with an offer to join a competing Chinese seed company, allegedly used sophisticated software capable of performing digital reconnaissance and exfiltrating data to download trade secret information from secure servers.

Monsanto argued that there was a substantial likelihood that it would succeed on the merits because the former employee used improper means, including unauthorized access to Monsanto's secure environment, to covertly acquire highly valuable trade secret information that Monsanto had taken reasonable steps to keep confidential. Monsanto also argued that it would suffer irreparable harm if the former employee was not prevented from disclosing trade secrets to the seed company in China because the misappropriated material related to strategy and sensitive products and explained confidential research. The Court granted a TRO and preliminary injunction directing the former employee to (1) return all trade secret information, (2) disclose the persons with whom the trade secret information was shared, and (3) identify all cloud storage locations where trade secret information was kept. A further discussion of this case can be found here.

Future Application

While DTSA jurisprudence is still largely undeveloped, some common themes have emerged. First, the trade secrets misappropriated in early DTSA cases have typically been in digital form, *i.e.*, forwarded emails and data downloaded to thumb drives. Given the ubiquitous connectivity of the modern workplace this trend is likely to continue. Additionally, cases where an employee used external digital storage devices and/or cloud storage services to allegedly store misappropriated trade secrets may be a candidate for use of the civil seizure mechanism, especially if it is clear that the employee may not fully comply with a TRO or preliminary injunction. The civil seizure mechanism has not yet been used. Cases involving trade secret misappropriation using digital means, however, may be the first in which civil seizure is employed, given the increasing threat of industrial espionage using advanced software and computing techniques.

Second, because there is still little case law interpreting the provisions of the DTSA, courts will likely continue to rely on state trade secret law precedent to support decisions under the DTSA. This trend will continue until the volume of DTSA decisions increases.

Third, it is likely that the DTSA will become the trade secret statute of choice at the International Trade Commission, which has seen a recent increase in investigations into misappropriation of trade secrets. The ITC is a Federal agency with broad investigative powers on matters of trade. One type of investigation conducted by the ITC is a Section 337 investigation wherein, if the ITC finds a violation, it can exclude articles from importation into the United States. Until the enactment of the DTSA, the ITC relied on the UTSA as the relevant law pertaining to Section 337 investigations of trade secret misappropriation. The ITC has the potential to provide powerful relief to companies whose trade secrets are misappropriated (domestically or abroad) and then used, for example, in the manufacture of an article being imported into the United States.

Conclusion

The DTSA provides American companies with another potent option to protect against and remedy misappropriation of trade secrets. Although DTSA jurisprudence is still developing, it is likely that the DTSA will become the statute of choice for addressing trade secret misappropriation in United States district courts and at the ITC. For continuing coverage of the DTSA, visit www.globalipmatters.com for updates.