

New Federal Trade Secrets Law Enacted – Effective Immediately

By Jackson Wyrick and Michael Plumleigh

Unlike patents, copyrights and trademarks, prior to this month, trade secrets have not been protected by federal law in the United States. Instead, trade secrets have been protected by individual state laws, with almost all states (48) enforcing laws modeled after the Uniform Trade Secrets Act (“UTSA”), although not necessarily uniformly.

That dichotomy changes with the adoption of the [Defend Trade Secrets Act](#)¹ (“DTSA”), recently passed in the U.S. Senate and the House of Representatives with overwhelming support. President Obama [signed](#) the DTSA into law on May 11. The DTSA was enacted and went into effect immediately thereafter.

The DTSA does not preempt existing state law on trade secrets (except for the whistleblower protection discussed below). The federalization of trade secrets protection represents the largest expansion of federal intellectual property law since the passage of the Lanham Act, which created federal trademark law in 1946. Companies, as well as employees and contractors with access to trade secrets, should familiarize themselves with the three key components of the new federal DTSA, which are described below.

Creation of a Federal Cause of Action for Misappropriation of Trade Secrets

The cornerstone of the DTSA is the creation of a new, federal civil cause of action that trade secret owners can bring against alleged misappropriators of trade secrets,² provided that they do so within 3 years of the discovery (or the date discovery should reasonably have occurred) of the misappropriation.³ There is substantial overlap between this new federal cause of action and causes of action currently available to trade secret owners under individual state laws; the DTSA largely follows the UTSA.

One important benefit for companies with operations, employees and consultants located in multiple states is that they can adopt a uniform approach for protecting their trade secrets under the DTSA, rather than having to navigate different requirements and approaches imposed by individual state laws on trade secrets and civil procedure. There are a number of important differences, and since trade secret owners have the option of pursuing recourse against a misappropriator in state or in federal court, they should become aware of those differences.

One key difference when alleging trade secret misappropriation is how the DTSA and some state laws require plaintiffs to describe the trade secrets at issue in complaints. Many state laws (including California’s) require the plaintiff to describe the trade secrets at issue with particularity, and this is often a concern.⁴ Complaints become part of the public record, so any trade secrets described with particularity in a complaint may lose their status as trade secrets. In contrast, the DTSA does not require plaintiffs to disclose their trade secrets with particularity in pleadings.⁵ As a result, businesses in states like California or subject to the laws of such states may prefer to bring federal claims under the DTSA.

Another key difference between the DTSA and the trade secrets laws of some states is the availability of injunctive relief to plaintiffs claiming misappropriation based on the “inevitable disclosure doctrine.” That doctrine allows a court to grant injunctive relief barring a former employee

For more information on trade secret protection and other intellectual property matters, please contact Michael Plumleigh at mplumleigh@mh-llp.com or 650-331-7005.

New Federal Trade Secrets Law Enacted – Effective Immediately

Client Alert

May 12, 2016

from taking a job with a new employer based merely on the assumption, rather than a showing of actual evidence, that a former employee would disclose proprietary information belonging to his or her former employer while working for that new employer. The DTSA, like several states including California, does not allow injunctive relief based on the inevitable disclosure doctrine; but some other states do. Trade secret owners in those states may prefer to bring state trade secret actions over DTSA actions, since their burden of proving misappropriation would be lower.

Filing an action under the DTSA also provides the opportunity for supplemental federal jurisdiction over other state law claims that are related to and typically accompany trade secret misappropriation actions, such as employment, unfair competition and breach of contract causes of action.⁶

Practice Tip: Owners of trade secrets considering bringing a cause of action for misappropriation of a trade secret should consult legal counsel regarding the differences between a federal action under the DTSA and an action under state trade secret statutes.

Creation of *Ex Parte* Seizure Procedure

One additional consideration for plaintiffs deciding between a federal or a state cause of action is the DTSA's *ex parte* seizure procedure, which allows courts to order seizures of material or content from a party without providing prior notice to that party.⁷ Neither the USTA nor any state trade secrets laws have an analogous seizure feature. Under the DTSA, the *ex parte* seizure procedure is only available for use in extraordinary circumstances where the court is convinced that the party receiving notice would "destroy, move, hide, or otherwise make such matter inaccessible to the court, if the applicant were to proceed on notice to such person...."⁸

The seizure mechanism in the DTSA provides trade secret owners with an important new protection against destruction of key evidence of misappropriation. However, it does not remove the need for judicial review of the appropriateness of the seizure. Instead, the court sets a hearing within 7 days after the issuance of the seizure order,⁹ and there are consequences (including possible damages) for any misrepresentations to the court that result in unlawful or excessive seizures.¹⁰

Practice Tip: Trade secret owners considering whether to bring a federal or state cause of action for misappropriation of a trade secret should consider whether the DTSA's *ex parte* seizure procedure would help them preserve key evidence of misappropriation. The DTSA's seizure mechanism should only be pursued if the trade secret owner believes that it can convince the court that seizure is necessary to preserve evidence (*i.e.*, because the alleged misappropriator is likely to destroy evidence of misappropriation upon receiving notice). Companies that are recipients of trade secrets or other proprietary information should consider developing a plan for responding to seizure orders, which could require them to hand over important and valuable information if they or their employees are suspected of misappropriation by a former employer or other party. The DTSA does provide recipients of a seizure notice with certain protections. For example, a recipient of a seizure notice can request that the information being seized be encrypted.¹¹ Recipients of a seizure notice who have not developed a response plan should consult counsel on how to respond and what protections are available.

Whistleblower Protection

The DTSA provides civil and criminal immunity from liability and prosecution under both federal and state laws to an employee or contractor¹² who discloses a trade secret in confidence to "a Federal, State, or local government official, either directly or indirectly,¹³ or to an attorney . . . and solely for the purpose of reporting or investigating a suspected violation of law," or in a court filing.¹⁴

In addition to providing such employees and contractors with immunity, the DTSA also requires that employers provide notice of that protection "in any contract or agreement with an employee [or contractor] that governs the use of a trade secret or other confidential information" entered into or amended after the passage of the DTSA.¹⁵ Employers can meet this requirement by including in any NDAs, PIIAAs and other agreements governing employee's or contractors' use or treatment of trade secrets a cross-reference to a policy document provided to employees or contractors describing the employer's reporting policy for suspected violations of law.¹⁶ Employers who fail to comply with the above notice requirements cannot recover exemplary damages or

Client Alert

May 12, 2016

attorney fees in misappropriation actions against employees or contractors under the DTSA.

Practice Tip: Employers, including those who hire contractors, should be sure to provide notice of the DTSA's protections to their employees and contractors in any new NDAs, PIIAAs and any other similar agreements or employment policies that govern the employee's or contractor's use or treatment of trade secrets and in amendments to any of the foregoing. Congress' intent in drafting the immunity provision so narrowly was not only to shield qualifying disclosures by employees and contractors from suit, but also to give employers recourse against rogue employees and contractors who disclose trade secrets under circumstances other than those set forth in the DTSA.

Conclusion

The DTSA represents a significant expansion of federal intellectual property law that should be beneficial to trade secret owners. It provides them with a federal cause of action for misappropriation of trade secrets that may be superior to the causes of action available under state law. Additionally, a DTSA action provides trade secret owners with a new *ex parte* seizure tool that is designed to prevent the destruction of key evidence of misappropriation of trade secrets. However, the DTSA also requires employers to notify employees and contractors that they have immunity if they disclose trade secrets confidentially to a government official or a lawyer. This immunity is designed to prevent disclosures by employees and contractors that harm the owner of the trade secret, but also to encourage responsible whistleblowing.

- ¹ The version cited here is Senate Bill 1890.
- ² DTSA § 2(b)(1).
- ³ DTSA § 2(d).
- ⁴ California Code of Civil Procedure § 2019.210.
- ⁵ DTSA § 3(b)
- ⁶ 28 U.S.C. § 1367(a).
- ⁷ DTSA § 2(b)(2).
- ⁸ DTSA § 2(b)(2)(A)(ii)(VII).
- ⁹ DTSA § 2(b)(2)(B)(v).
- ¹⁰ DTSA § 2(b)(2)(G).
- ¹¹ DTSA § 2(b)(2)(H). Further details on the nature of the encryption are unclear.
- ¹² DTSA § 7(b)(4).
- ¹³ It is unclear what constitutes an "indirect" communication of disclosure.
- ¹⁴ DTSA § 7(b)(1)(A).
- ¹⁵ DTSA § 7(b)(3)(A), 7(b)(3)(D).
- ¹⁶ DTSA § 7(b)(3)(B).

This bulletin is intended as an information source for clients and friends of Montgomery & Hansen, LLP. The content should not be construed as legal advice, and readers should not act upon information in this publication without professional counsel. This material may be considered advertising under certain rules of professional conduct. Permission is granted to make and redistribute, without charge, copies of this entire document provided that such copies are complete and unaltered and identify Montgomery & Hansen LLP as the author. All other rights reserved.