The New “Defend Trade Secrets Act”:
What It Means And How It Can Be Utilized
To Defend Against Trade Secret Misappropriation
By: William J. McCabe & Gene W. Lee

I. Overview

On May 11, 2016, President Obama signed the Defend Trade Secrets Act (DTSA) into law. Trade secret misappropriation has been estimated to cost the U.S. economy over $300 billion and 2.1 million jobs annually. Employees and business partners are estimated to account for 85% to 90% of trade secret misappropriation. The good news is that companies can usually enter into written agreements with employees and business partners that will help them preserve their trade secrets and position themselves for a strong action under the DTSA. Although the DTSA covers both civil and criminal misappropriation, this article focuses on civil aspects.

II. DTSA Background

Before the DTSA was enacted, trade secret owners had to look to individual state laws for a civil remedy. Although 47 states have adopted a version of the Uniform Trade Secrets Act (UTSA), it has not been adopted in a uniform manner. Such a patchwork of laws made civil remedies for trade secret misappropriation difficult, especially for companies whose business, employees, or trade secrets cover multiple states.

---

1 William J. McCabe and Gene W. Lee are partners at Perkins Coie LLP.
Before the DTSA, a federal civil action based on a state law claim for misappropriation (absent a separate federal question) required “diversity of citizenship” between the trade secret owner and the accused misappropriator. This often served as a barrier to trade secret actions being filed in federal court, where the judiciary and procedures can favor certain litigants, because companies and their employees are often citizens of the same state. With the DTSA, a civil action under the DTSA can include claims based on other federal or state laws, including claims under the UTSA or other appropriate state laws because the DTSA does not “preempt or displace” other federal or state laws for trade secret misappropriation. 4 Despite the DTSA, not all plaintiffs have chosen to assert DTSA claims, and some opt to litigate in state court instead. But the DTSA gives plaintiffs a predictable tool they can choose to use against alleged misappropriators.

III. Elements of a DTSA Case

The DTSA allows a trade secret owner to bring an action “if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce.” 5 The DTSA contains a broad definition of “trade secret”:

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, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing…. 6

---

4 18 U.S.C. §1838 (“Except as provided in section 1833(b), this chapter shall not be construed to preempt or displace any other remedies, whether civil or criminal, provided by United States Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret . . . .”).
For “information” to qualify as a trade secret, the owner must have “taken *reasonable measures* to keep [the] information secret” and the information must have “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.” Taking “reasonable measures” to maintain secrecy is the responsibility of the trade secret owner and typically includes various steps to restrict both access and dissemination of confidential information. Interpreting “reasonable measures” in a pre-DTSA case, one Court stated, “It is not necessary ‘that an ‘impenetrable fortress’ be erected to retain legal protection for a trade secret.’”

Misappropriation under the DTSA requires that the trade secret be acquired by “improper means,” which can include “theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means.” Misappropriation “does not include reverse engineering, independent derivation, or any other lawful means of acquisition.” In other words, if the public can discover a “trade secret” from analysis of the products or services that a company puts in the marketplace, there is likely no relief under the DTSA.

Company employees work with, or even create, trade secrets as part of their jobs. However, an employee who acquires a trade secret by “theft” or “breach … of a duty to maintain

---

7 *Id.*
8 *See, e.g., Syntel Sterling Best Shores Mauritius Ltd. v. Trizetto Grp., Inc.*, No. 15CV211LGSRLE, 2016 WL 5338550, at *6 (S.D.N.Y. Sept. 23, 2016) (“reasonable measures” under the DTSA alleged based on “measures to keep the information secret by making those who use it subject to confidentiality provisions and limitations, and only making it accessible through strictly controlled servers”); *M.C. Dean, Inc. v. City of Miami Beach, Florida*, 199 F. Supp. 3d 1349 (S.D. Fla. 2016) (DTSA “reasonable measures” not met where there is disclosure to others who have no obligation to protect the confidentiality).
11 *Id.*
secrecy” likely has acquired it by “improper means.”\textsuperscript{12} A company should have clear non-disclosure agreements that require employees (and others with access) to maintain the confidentiality of company information and to return all confidential information, even if the employee has saved that confidential information to personal sources (e.g. personal email, cloud accounts, or external devices), immediately at the end of employment (or at the end of a project). Breach of such an agreement may constitute “improper means” and will help lay the foundation for a successful misappropriation claim.

The DTSA has a three-year statute of limitations running from the date on which misappropriation was discovered or “by the exercise of reasonable diligence should have been discovered.”\textsuperscript{13}

\textbf{IV. Remedies under the DTSA}

Although the DTSA allows a Court to issue an injunction “to prevent any actual or threatened misappropriation,”\textsuperscript{14} the Court may not “prevent a person from entering into an employment relationship” and any “conditions placed on such employment shall be based on evidence of threatened misappropriation and not merely on the information the person knows.”\textsuperscript{15} In other words, the DTSA cannot be used to prevent an employee from joining a competitor unless there is evidence of threatened improper disclosure.

Damages under the DTSA can include “actual loss,” “unjust enrichment,” or a “reasonable royalty” caused by the misappropriation.\textsuperscript{16} If the misappropriation was willful and

\begin{footnotesize}
\begin{enumerate}
\item Id.
\item 18 U.S.C. §1836(d).
\end{enumerate}
\end{footnotesize}
malicious, the court may “award exemplary damages in an amount not more than 2 times the amount” of actual damages. In such circumstances the court may also award reasonable attorney’s fees to the prevailing party. It is too early to tell how damages awards under the DTSA will compare to damages awards under state laws, but the damages provisions under the DTSA and the UTSA are largely similar. If recent non-DTSA cases are any guide, the risks involved in trade secret litigation remain significant. For instance, last year a Western District of Wisconsin jury in *Epic Systems Corp. v. Tata Consultancy Services, Ltd.* returned a $940 million verdict ($240 million in compensatory damages and $700 million in punitive damages) and entered an injunction in a case arising out of alleged theft of trade secrets relating to healthcare software. Meanwhile, a Texas jury earlier this year entered a $500 million verdict in *Zenimax Media Inc. v. Oculus VR LLC* despite finding in the defendant’s favor on the trade secrets claim, nonetheless awarding $500 million on related copyright infringement and trademark false designation claims.

In extraordinary cases, the DTSA allows *ex parte* “seizure of property necessary to prevent the propagation or dissemination of the trade secret.” An *ex parte* order should not be requested lightly. The moving party must meet a high standard to obtain a seizure order---including likelihood of success on the merits and a showing that other preliminary relief would be insufficient. And a party who obtains a seizure order, which is later determined to have been

---

18 Case No. 14-cv-00748 (W.D. Wis.).
19 Wisconsin law caps punitive damages at twice compensatory damages, so the final award may be reduced.
20 Case No. 14-cv-1849-K (N.D. Tex.).
improper, may need to pay a party “who suffers damage by reason of a wrongful or excessive
seizure”\textsuperscript{22} damages and attorney’s fees if the claim of misappropriation was made in bad faith.\textsuperscript{23}

V. Conclusion

Trade secret owners can protect themselves by having carefully drafted, thoughtful, written policies coupled with signed agreements that specify the types of information that are confidential and how such information should be handled. Written policies should include provisions for marking confidential information “confidential” and limiting access to persons authorized to receive it. Agreements should include obligations to maintain confidentiality and to return any and all company information – including confidential information – from any of the employee’s business or personal files or accounts. Agreements should be signed at the beginning of employment (or the start of a business relationship) and be acknowledged – preferably in writing – at the end of employment (or end of the business relationship).

During litigation, accused misappropriators often try to show that trade secret owners failed to take “reasonable measures” to keep maintain secrecy or allowed the trade secret to leak out. Trade secrets and other confidential information should be treated as valuable and be kept in a secure environment and accessed only by those with permission.

Finally, it is important that companies provide their employees with the tools they need to keep their proprietary information confidential. Those tools should include clear policies, training, secure electronic devices, and appropriate means to securely interface with the company as are demanded by modern business.

\textsuperscript{22} 18 U.S.C. §1836(b)(2)(G).
\textsuperscript{23} 18 U.S.C. §1836(b)(3)(D).
WILLIAM (BILL) J. MCCABE | PARTNER

NEW YORK, NY
30 Rockefeller Plaza
22nd Floor
New York, NY USA
+1.212.262.6900
WMcCabe@perkinscoie.com

GENE W. LEE | PARTNER

NEW YORK, NY
30 Rockefeller Plaza
22nd Floor
New York, NY USA
+1.212.262.6900
GLee@perkinscoie.com