IADC COMMITTEE NEWSLETTER

TECHNOLOGY

May 2016

IN THIS ISSUE

The Defend Trade Secrets Act of 2016, signed into law on May 11, 2016, creates federal court jurisdiction and additional remedies for the misappropriation of trade secrets, an area of law that had long been the domain of state courts except in diversity of citizenship cases.

Understanding the Defend Trade Secrets Act of 2016: "We're Not in State Court Anymore"

ABOUT THE AUTHORS

Peter J. Pizzi is a founding partner of Walsh Pizzi O'Reilly Falanga LLP, with offices in Newark New Jersey, New York City and Philadelphia. He is the incoming Chair of the IADC's Technology Committee. He has extensive commercial litigation and technology law experience in disputes before state and federal courts and in arbitration. He is a Certified Information Privacy Professional/United States (CIPP/US) from the International Association of Privacy Professionals (2014) and also a Certified Civil Trial Attorney, a Supreme Court of New Jersey designation. He can be reached at ppizzi@thewalshfirm.com.

Christopher J. Borchert is an associate with Walsh Pizzi O'Reilly Falanga LLP, where his practice focuses on federal and complex commercial litigation with an emphasis on intellectual property and trade secret disputes. In September 2016, he will commence a judicial clerkship with the Hon. Esther Salas, United State District Judge for the District of New Jersey. Mr. Borchert received a J.D. and a certificate in Intellectual Property from the University of Connecticut School of Law and a B.A. in Political Communication from the George Washington University. He can be reached at cborchert@thewalshfirm.com.

ABOUT THE COMMITTEE

The Technology Committee keeps the IADC membership current on the use of technology in litigation, whether in the conduct of discovery or in the use of technology in the courtroom. It educates its members on the impact of technology in their practices – on the ways they communicate with each other, with courts and clients, on the systems they use to record and produce their work, and on technological developments in marketing for law firms. The committee provides information to its members on legal developments in the law governing the use and development of technology, in particular on Internet and computer law and related subjects. Through its members, it acts as a resource to the IADC staff and leadership on technology issues facing the organization. Learn more about the Committee at www.iadclaw.org. To contribute a newsletter article, contact:

John Christian Nemeth
Vice Chair of Publications
McDermott Will & Emery
jcnemeth@mwe.com

On May 11, 2016, President Obama signed into law the Defend Trade Secrets Act of 2016 ("DTSA"), a powerful new statutory regime intended to bolster protections for U.S. trade secret holders. The statute will have an immediate impact on federal court practitioners, as it creates a private cause of action for the misappropriation of trade secrets and expressly confers jurisdiction of such actions to the U.S. federal district courts. The DTSA also contains a civil seizure mechanism through which an owner of a trade secret may apply to a district court for an order compelling the seizure of property necessary to prevent the dissemination of the trade secret. In this way, the DTSA seeks not only to harmonize the substantial and diverse body of state trade secret law, but also to equip trade secret holders with new tools to safeguard their intellectual property.

The statute owes its origins in part to the Justice Department's unsuccessful prosecution in *United States v. Aleynikov*, 676 F.3d 71 (2d Cir. 2012), in which the Second Circuit reversed the conviction of a Sergei Aleynikov, a former Goldman Sachs programmer, for theft of trade secrets, finding that proprietary computer code fell outside the scope of the then-existing federal statutory schemes because it was not "produced . . . for interstate or foreign commerce." Aleynikov had allegedly uploaded Goldman Sachs high-frequency trading code to a server in Germany as he was leaving Goldman's employment for a Chicago hedge fund. In response to *Aleynikov* and related concerns about international and domestic "hacktivism," legislation was proposed to amend the Economic Espionage Act, and it is that amendment which President Obama signed into law earlier this month.

This article provides a brief overview of the DTSA and identifies the key provisions applicable to practitioners, employers, and private parties that work with or rely on trade secrets.

Private Cause of Action (§ 1836)

The DTSA provides for a private cause of action by an owner of a trade secret that is misappropriated, provided the trade secret "is related to a product or service used in, or intended for use in, interstate or foreign commerce." Under the DTSA, federal district courts have original jurisdiction of such actions. The DTSA is also forward-reaching in that it applies only to misappropriation that occurs after its enactment.

Civil Seizure

As noted above, the DTSA contains a civil seizure mechanism. Under this provision, a district court may, based on an affidavit or verified complaint satisfying certain statutory requirements (discussed below), "upon ex parte application but only in extraordinary circumstances, issue an order providing for the seizure of property necessary to prevent the propagation or

dissemination of the trade secret that is the subject of the action."

Requirements for a Seizure Order

A district court may not issue a seizure order unless it makes certain statutory-based findings. Specifically, the court must find that (1) an order pursuant to FRCP 65, or another form of equitable relief, would be inadequate to prevent the dissemination of the trade secret because the target of the order would evade, avoid, or otherwise not comply with such an order; (2) an immediate and irreparable injury will occur if the seizure is not ordered; (3) the harm to the applicant of denying the application outweighs the harm to the legitimate interests of the target of the seizure and substantially outweighs the harm to any third parties who may be harmed by such seizure; (4) the applicant is likely to succeed in showing that (i) the information is a trade secret, and (ii) the target of the seizure (a) misappropriated the trade secret of the applicant by improper means; or (b) conspired to use improper means to misappropriate the trade secret of the applicant; (5) the target of the seizure has actual possession of (i) the trade secret, and (ii) any property to be seized; (6) the application describes with reasonable particularity the matter to be seized and, to the extent reasonable under the circumstances, identifies the location where the matter is to be seized; (7) the target of the seizure, or persons acting in concert with the target, would destroy, move, hide, or otherwise make such matter inaccessible to the court, if the applicant were to proceed on notice to such person; and (8) the applicant has not publicized the requested seizure.

Elements of a Seizure Order

The DTSA further provides that any civil seizure order shall provide for the "narrowest seizure of property necessary" and "direct that the seizure be conducted in a manner that minimizes any interruption of the business operations of third parties and, to the extent possible, does not interrupt the legitimate business operations of the person accused of misappropriating the trade secret." Additionally, the seizure order shall be accompanied by an order protecting the seized property from disclosure by (i) prohibiting access by the applicant or the target of the seizure order and (ii) prohibiting any copies, in whole or in part, of the seized property. The seizure order shall also set a date for a seizure hearing (discussed below) and require the applicant to provide adequate security to cover damages that result from a wrongful or excessive seizure or attempted seizure.

Seizure Hearing

Under § 1836(b)(2)(F), a court that issues a seizure order must hold a hearing at the earliest possible time, and not later than 7 days after the order has issued, wherein the applicant must prove factual and legal bases supporting the order. If the applicant fails to meet that burden, the seizure order shall be dissolved or modified appropriately. In addition, a party against whom the order has

been issued, or any person harmed by the order, may move the court at any time to dissolve or modify the order after giving notice to the party who obtained the order.

Remedies

The DTSA provides for both injunctive relief and damages. Under § 1836(b)(3)(A), a court may grant an injunction so long as the injunction does not prevent a person from entering into an employment relationship or otherwise conflict with an applicable State law prohibiting restraints on the practice of a lawful profession, trade, or business. In addition, a court may grant an injunction requiring affirmative actions to be taken to protect the trade secret. Further, in exceptional circumstances where an injunction would be inequitable, the court may condition future use of the trade secret upon payment of a reasonable royalty for a period of time no longer than the period for which such use could have been prohibited by injunctive relief.

Under § 1836(b)(3)(B), a court may award damages for actual loss caused by the misappropriation of the trade secret, as well as damages for any unjust enrichment that are not connected to actual loss; ***or*** in lieu of actual damages, a reasonable royalty for the unauthorized wrongdoer's disclosure or use of the trade secret. Furthermore, if the misappropriation is found to be willful or malicious, a court may award reasonably attorney's fees and exemplary damages not more than two times the amount of the actual damages or reasonable royalties. A court may also award reasonable attorney's fees if a misappropriation claim or a motion to terminate an injunction is made or opposed in bad faith.

Statute of Limitations

Finally, the statute of limitations for a private cause of action for misappropriation of trade secrets is three years 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." For purposes of the statute of limitations, a continuing misappropriation constitutes a single claim of misappropriation.

Whistleblower Exception - § 1833(b)

Immunity

The DTSA carves out a liability exception for individuals who disclose a trade secret to the government under certain circumstances. Specifically, § 1833(b)(1) provides that an individual is exempt from criminal and civil liability for disclosure of a trade secret that is made (1) in confidence to the government or an attorney and (2) solely for the purpose of reporting or investigating a suspected violation of law. The DTSA's immunity provision also covers the disclosure of a trade secret that is made in a complaint or other document filed in a lawsuit or other proceeding, if the filing is made under seal.

Notice Provision for Employers

Relatedly, the DTSA contains a notice provision applicable to employers that use contracts or agreements to govern an employee's use of a trade secret or other confidential information. Under § 1833(b)(3), an employer that does not provide notice of the immunity set forth in the DTSA cannot be awarded exemplary damages or attorney's fees in any civil action brought under the DTSA against an employee to whom notice was not provided. That said, under this subsection, an employer complies with the notice requirement if the employer provides a cross-reference to a policy document provided to the employee that sets forth the employer's reporting policy for a suspected violation of law. Significantly, this subsection defines "employer" as "any individual performing work as a contractor or consultant for an employer."

Preserving Confidentiality of Trade Secrets in District Courts – § 1835(b)

The DTSA also includes a provision designed to safeguard the confidentiality of trade secrets in district court proceedings. Under § 1835(b), district courts are prohibited from authorizing or directing the disclosure of any information a trade secret owner asserts to be a trade secret unless the court allows the owner to file a submission under seal describing the owner's interest in keeping the information confidential. This provision specifies that a trade secret owner's disclosure of trade secret information, made under seal, shall not constitute a waiver of trade secret protection.

Criminal Penalties for Organizations - § 1832(b)

Prior to the DTSA's enactment, the penalties for an organization found guilty of theft of trade secrets was capped at $5 million. Under the DTSA, those penalties have increased to "the greater of $5 million or 3 times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided."

New Definitions - § 1839

"Trade Secret"

The DTSA slightly narrows the definition of "trade secret." Previously, a trade secret was defined as, among other criteria, deriving independent economic value from not being generally known to, and not being readily ascertainable through proper means by, "*the public*." Under the DTSA, a trade secret retains the same definition with the exception that it derives independent economic value from not being generally known to, and not readily ascertainable through proper means by, "another person who can obtain economic value from the disclosure or use of the information."

"Misappropriation"

The DTSA provides a new definition of "misappropriation": (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."

"Improper Means"

The DTSA also provides a new definition of "improper means": (A) includes theft, bribery, misappropriation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means; and (B) does not include reverse engineering, independent derivation, or any other lawful means of acquisition.

Conclusion

To be sure, the DTSA's benefits do not come without burdens. The DTSA will likely spark an uptick in trade secret litigation in the federal court system and, as federal court practitioners are well aware, most district courts are already overburdened and understaffed. How courts will manage an even greater caseload due to new federal causes of action does not appear to have been part of the equation lawmakers considered in enacting the DTSA. Moreover, the civil seizure provisions introduce an additional procedural mechanism that will require immediate (and highly substantive) responses from the courts. Without doubt, however, the DTSA is a powerful tool for protecting this country's intellectual property.

Meanwhile, the *Aleynikov* saga – which highlighted the shortcomings of federal criminal and civil remedies for the misappropriation of trade secrets – continues as of this writing. Mr. Aleynikov's conviction of analogous New York state charges having been dismissed post-trial in 2015, Aleynikov is pursuing the recovery of millions in legal fees from Goldman Sachs under by-law provisions which indemnify corporate officers (Aleynikov was a "Vice President") who successfully defend against work-related civil or criminal charges. *See Aleynikov v. The Goldman Sachs Group*, Delaware Court of Chancery, Case No. 10636.

Past Committee Newsletters

Visit the Committee's newsletter archive online at www.iadclaw.org to read other articles published by the Committee. Prior articles include:

DECEMBER 2015
Cyber Armageddon: Survival or Annihilation?
Theodore M. Schaer and Elizabeth S. Fitch

JULY 2015
Fitbit Data Brings Another Dimension to Evidence
John G. Browning

DECEMBER 2014
The Ethics of Technology in E-Discovery – An Introduction
Peter J. Pizzi and Julia L. Brickell

SEPTEMBER 2013
Emerging Technology and Its Impact on Automotive Litigation
John G. Browning

JUNE 2012
iPad Apps: Brave New Frontier
Adam Bloomberg and J. Calhoun Watson

AUGUST 2011
TrialDirector: Electronic Trial Presentation – A Primer, Best Practice Tips
Thomas G. Oakes

MAY 2010
Know When to Hold 'Em: The Effective Use of Litigation Holds
Mike Taylor

JULY 2009
New Insights for Jury Profiling and Online Socialization
Merrie Jo Pitera and Stephanie S. Cox

APRIL 2008
Irish Supreme Court "Creates" E-Discovery: The Disappearing Line between Digital Data and Paper Documents
Robert C. Manlowe, Gregory D. Shelton, and Manish Borde

FEBRUARY 2008
Qualcomm v. Broadcom: Lessons for Counsel and a Road Map to e-Discovery Preparedness
Gregory D. Shelton

JANUARY 2008
Simonetta v. Viad Corp: A Disturbing Expansion of the Duty to Warn in Products Liability Cases
Gregory D. Shelton