Bloomberg Law®

BNA's
Patent, Trademark & Copyright Journal®

2017 Trade Secrets Litigation Round-Up




By Jason C. Schwartz, Greta B. Williams, Mia Donnelly, and Brittany Raia

In 2017, we saw flurry of trade secrets litigation in the self-driving car industry and the Trump administration prosecute an engineer who allegedly sold military trade secrets to an undercover FBI agent whom he believed to be a Russian spy. Building on our 2016 *Trade Secrets Litigation Round-Up*, we survey these and some of the year's other significant civil and criminal developments.

I. Civil Developments

A. The Defend Trade Secrets Act

It has been over a year and a half since the enactment of the Defend Trade Secrets Act (DTSA), which provides a federal civil cause of action for trade secret misappropriation. Since then, more than 360 DTSA complaints have been filed. 2017 also saw the first DTSA jury verdict—a $2.5 million verdict for trade secret misappropriation and trademark infringement, with $500,000 attributed to the DTSA and state trade secret claims. *See Dalmatia Import Group v. Foodmatch, Inc.*, 16-cv-02767 (E.D. Pa. Feb. 24, 2017). Several trends and interesting developments have also emerged, as discussed below.

Jason C. Schwartz is a litigation partner in the Washington, D.C., office of Gibson, Dunn & Crutcher, co-chair of the firm's Labor and Employment Practice Group, and a member of the firm's executive and management committees. His practice includes litigating high-stakes strade secrets, non-compete, and employment disputes. He also serves as the firm's general counsel.

Greta B. Williams is a litigation partner in the firm's Washington office. Her practice covers a wide range of employment matters, including those involving high-stakes trade secrets and non-compete disputes.

Mia Donnelly and Brittany Raia are litigation associates in the firm's Washington office.

1. Ex Parte Seizure

One of the most controversial aspects of the DTSA is the provision that authorizes ex parte seizures of property by federal law enforcement officers to prevent unauthorized dissemination of trade secrets. Most courts that have addressed this provision found ex parte seizure orders unnecessary, instead issuing temporary restraining orders (TRO) or preliminary injunctions under Federal Rule of Civil Procedure 65 to seize property containing alleged trade secrets. *See, e.g., Magnesita Refractories Co. v. Mishra*, No. 2:16-CV-524-PPS-JEM, 2017 BL 21416, at *3 (N.D. Ind. Jan. 25, 2017) (issuing ex parte TRO compelling defendant to turn over his laptop, and noting that ex parte seizure under the DTSA was not necessary because ''Rule 65 did the trick''); *OOO Brunswick Rail Mgmt. v. Sultanov*, No. 5:17-cv-00017-EJD, 2017 BL 4091 (N.D. Cal. Jan. 6, 2017) (issuing TRO prohibiting two former employees from accessing company-issued devices and ordering one employee to deliver his devices to the court).

However, in August 2017, the U.S. District Court for the Western District of Oklahoma granted a land and regulatory services firm's application for ex parte seizure against two former employees. *See Blue Star Land Servs., LLC v. Coleman*, No. Civ. 17-931-R, at 3 (W.D. Okla. Aug. 30, 2017) (Dkt. 10). The court issued a broad order authorizing seizure of ''[a]ny computers, computer hard drives, or memory devices'' in the defen-

dants' possession that may contain trade secrets, as well as the usernames and passwords for those devices and defendants' Dropbox and email accounts. *Id*. It found that given the nature of the trade secrets and the manner in which defendants allegedly took them, combined with their ''alleged duplicity with Plaintiff,'' which ''demonstrate[d] a willingness to evade or ignore the law,'' an order pursuant to Rule 65 would be ineffective. *See id.* at 2-3.

2. Whistleblower Immunity and Notice

The DTSA authorizes whistleblowers to disclose trade secrets to government officials or an attorney in confidence for the sole purpose of reporting or investigating wrongdoing, and in court filings under seal, and requires employers to provide notice of the statute's whistleblower provisions in agreements pertaining to trade secrets entered into after the statute's passage. Failure to provide this notice results in loss of the employer's ability to recover exemplary damages or attorneys' fees in an action against an employee to whom notice was not provided. This provision has been largely untested since the DTSA's enactment.

Notably for employers, however, in the one 2017 court opinion addressing the DTSA's whistleblower provisions, the court found that because the employer did not provide the requisite notice in its employment agreement (or elsewhere), it could not recover attorneys' fees or exemplary damages under the DTSA. *Xoran Holdings LLC v. Luick*, No. 16-13703, 2017 BL 321228 (E.D. Mich. Sept. 13, 2017).

3. Inevitable Disclosure Doctrine

Many commentators viewed the DTSA as a rejection of the inevitable disclosure doctrine given its requirement that any conditions placed on an employee moving to a competitor ''be based on evidence of threatened misappropriation and not merely on the information the person knows.'' 18 U.S.C § 1836(b)(3)(A)(i)(I).

However, a few recent decisions suggest that the doctrine still has legs. In *Molon Motor & Coil Corp. v. Nidec Motor Corp*., No. 16-cv-03545, 2017 BL 158814, at *7 (N.D. Ill. May 11, 2017), although custom gearmotor manufacturer Molon did not allege any specific facts about its former employee passing on information to his new employer, the court found that Molon's allegations stated a plausible trade secret misappropriation claim because they were sufficient to ''trigger the circumstantial inference that the trade secrets inevitably would be disclosed.'' *See id.* at *7; *see also Fres-Co Sys. USA, Inc. v. Hawkins,* 690 Fed. App'x 72, 76 (3d Cir. 2017) (affirming preliminary injunction under the DTSA and finding that packaging material manufacturer Fres-Co Systems demonstrated that its former sales representative would likely use its confidential information in his new position with a direct competitor, given the ''substantial overlap'' between his work for the two companies).

B. Other Civil Developments

In 2017, we also saw courts review significant jury verdicts and address trade secrets in the self-driving car industry.

1. Judicial Review of Significant Jury Verdicts

In our 2016 *Round-Up*, we highlighted what was believed to be one of the largest damages awards in a trade secrets case: $940 million to medical software company Epic Systems against India's top software services provider, Tata Consultancy Services Ltd. In September 2017, the court slashed the award by more than half to $420 million. *See Epic Sys. Corp. v. Tata Consultancy Servs. Ltd*., No. 3:14-cv00748 (W.D. Wis. Sept. 29, 2017) (Dkt. 326). The court found that $100 million of the initial $240 million compensatory damages award, which was based on Tata Consultancy's ''unspecified use of 'other information,' '' was excessive and without sufficient support in the record. *See id.* at 11-12. The court also reduced the $700 million punitive damages award to $280 million pursuant to Wisconsin's punitive damages cap. *See id.* at 17.

Other courts, however, showed deference to some of the high-dollar jury verdicts we have previously highlighted in this *Round-Up*. In April, an Illinois federal judge affirmed a $74 million verdict against construction and mining equipment manufacturer Caterpillar Inc. for theft of trade secrets from rival Miller UK Ltd. *See Miller UK Ltd. v. Caterpillar Inc*., No. 1:10-cv-03770 (N.D. Ill. March 31, 2017). And in September, the U.S. Court of Appeals for the Federal Circuit affirmed a $112 million award ($70 million jury award, plus subsequent enhanced damages and interest) to CardiAQ Valve Technologies Inc. against a company it collaborated with on a heart valve implant. *See CardiAQ Valve Techs. Inc. v. Neovasc Inc.*, Nos. 17-1302 (Fed. Cir. Sept. 1, 2017).

2. Trade Secret Disputes in the Self-Driving Car Industry

2017 also saw several trade secret lawsuits filed in the self-driving car space.

In February 2017, Google's self-driving car unit Waymo LLC sued Uber, alleging that it misappropriated Waymo's self-driving car technology. *See Waymo LLC v. Uber Techs., Inc.*, No. 3:17-cv-00939 (N.D. Cal). Specifically, Waymo alleges that ex-Waymo engineer Anthony Levandowski downloaded 14,000 confidential files related to Waymo's self-driving car technology before he left and started his own company, which Uber later acquired. Waymo further alleges that Uber used Levandowski's files and Waymo's trade secrets to develop its own self-driving car technology. Uber denies using Waymo's trade secrets and argues that it built its self-driving car technology independently. Trial was set to begin in December, but was postponed in late November. A new trial date has not been set.

Another similar case involving Tesla settled in April 2017, less than three months after it was filed. In January 2017, Tesla sued former employee Sterling Anderson after Anderson quit to start a self-driving car company called Aurora. *See Tesla Motors Inc. v. Anderson,* No. 17CV305646 (Cal. Super. Jan. 26, 2017). Tesla, which sued Aurora and Anderson's co-founder in the same suit, alleged that Anderson stole ''hundreds of gigabytes'' of confidential and proprietary information before leaving. Under the settlement, Aurora agreed to undergo future audits to ensure Anderson is not keeping or using any of Tesla's confidential information. The settlement also established a process to allow Tesla to recover all of the allegedly proprietary information that Anderson purportedly stole.

   ISSN 0148-7965

II. Criminal

The Trump administration, like the Obama administration before it, has continued to aggressively pursue criminal actions to address and deter trade secret theft and economic espionage in 2017. Below, we highlight some of the most notable criminal prosecutions of 2017, along with recent developments in some long-running criminal appeals and the Computer Fraud and Abuse Act (CFAA).

A. Economic Espionage Act

The Economic Espionage Act (EEA) criminalizes the theft of trade secrets (18 U.S.C. § 1832) and economic espionage (18 U.S.C. § 1831). In fiscal year 2017, there were 13 new prosecutions (up from six in 2016) and five new convictions under 18 U.S.C. § 1832, and seven new prosecutions (up from one in 2016) and one conviction under 18 U.S.C. § 1831.

For instance, on May 22, 2017, Gregory Allen Justice pled guilty to attempting to commit economic espionage by stealing trade secrets from his former employer (a U.S. defense contractor) related to sensitive satellite information and selling them to a person he believed to be a Russian agent. That agent was actually an undercover FBI agent. In September, Justice was sentenced to five years in prison.

As in prior years, many of 2017's criminal cases involved foreign nationals allegedly acting on behalf of foreign entities and attempting to steal trade secrets from U.S. companies. For instance, on May 24, prosecutors charged seven individuals—including two Chinese nationals—with the theft of trade secrets from a Swedish engineering firm (with a subsidiary in Houston) for the benefit of a Chinese company. *See United States v. Shan Shi,* No. 1:17-cr-110 (D.D.C. June 8, 2017). The trade secrets at issue relate to ''syntactic foam,'' which the Chinese company allegedly intended to sell to military and civilian state-owned enterprises in China. *Id.*

In May, Xu Jiaqiang pled guilty to economic espionage and trade secret theft in connection with the theft of source code from his U.S. employer (reportedly IBM) for the benefit of the National Health and Family Planning Commission of the People's Republic of China. *See United States v. Jiaqiang Xu*, No. 7:16-cr-10 (S.D.N.Y. Jan. 5, 2016).

B. Criminal Appeals

The year 2017 saw significant developments in the appeals of several high-profile trade secret convictions that we have covered in this *Round-Up* in prior years.

People v. Aleynikov

Former Goldman Sachs computer engineer Sergey Aleynikov was convicted in May 2015 under New York state law in connection with the theft of high frequency trading source code from Goldman Sachs after his federal convictions for violations of the EEA and the National Stolen Property Act were overturned by the U.S. Court of Appeals for the Second Circuit.

In July 2015, a New York trial court overturned his state conviction, finding insufficient evidence that Aleynikov made a tangible reproduction of the source code as required by the statute because he transmitted the code electronically.

In January 2017, however, a New York appellate court reversed, concluding that ''[i]t would be incongruous to allow defendant to escape criminal liability merely because he made a digital copy of the misappropriated source code instead of printing it onto a piece of paper.'' *People v. Aleynikov*, 148 A.D.3d 77, 85-86 (N.Y. App. Div. 2017). Aleynikov appealed to New York's highest court, and oral argument is set for March 2018.

United States v. Liew

In 2014, Walter Liew was convicted under the EEA for (among other things) the theft of trade secrets related to DuPont's titanium dioxide products, which are used to produce specialized coatings and plastics. On appeal, Liew argued that DuPont had not taken reasonable efforts to protect its trade secrets because, in 1967, DuPont had built a chloride plant for Sherwin-Williams, which agreed to keep its proprietary information confidential for 15 years, but then sold the plant.

The Ninth Circuit rejected that argument, and upheld Liew's trade secrets conviction. ''[U]nder the EEA's then-current definition of trade secrets, it was not 'clear' or 'obvious' that disclosure to a single competitor made information 'generally known to' or 'readily ascertainable' by 'the public.' '' *United States v. Liew*, 856 F.3d 585, 598-99 (9th Cir. 2017). The court did not address how the outcome might differ under the EEA's current definition of trade secrets (as amended by the DTSA), which requires that the information derive value from not being known to or readily ascertainable by others ''who can obtain economic value from the disclosure or use of the information.'' 18 U.S.C. § 1839(3) (2016).

C. Computer Fraud and Abuse Act

The CFAA, which is often invoked in theft of trade secrets cases, provides for both criminal and civil causes of actions against those who ''intentionally access[] a computer without authorization or exceed[] authorized access, and thereby obtain[] . . . information from any protected computer,'' or who ''intentionally access[] a protected computer without authorization, and as a result of such conduct, cause[] damage and loss.'' 18 U.S.C. § § 1030(a)(2)(C), (a)(5)(C), (g). As we have previously reported, the U.S. Courts of Appeal have struggled with and split over how to define ''without authorization'' and ''exceeds authorized access.''

This year, the Supreme Court denied certiorari in two cases involving the ''without authorization'' provision that would have helped define the scope of CFAA liability. The high court declined to review *United States v. Nosal*, 828 F.3d 865 (9th Cir. 2016), in which the Ninth Circuit held that Nosal accessed a computer ''without authorization'' when he used another person's login credentials (with that person's permission) to access his former employer's computer after the employer had revoked Nosal's right to access the computer. The court's denial also ended Nosal's nearly decade-long fight to have his CFAA conviction overturned.

The Supreme Court also declined to take up the case of *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058 (9th Cir. 2016), where the Ninth Circuit ruled that social media aggregator Power Ventures violated the CFAA by accessing Facebook user data. The court rejected Power Ventures' claim that permission from Facebook users was sufficient to avoid the CFAA after Facebook had explicitly revoked any permission via a cease-and-desist letter. The denial of certiorari in these cases leaves intact the Ninth Circuit's broad view of what it means to access a computer ''without authorization.''

III. Conclusion

Developments in 2017 demonstrate that U.S. companies remain vulnerable to trade secret theft and misappropriation from domestic and foreign actors.

While the Trump administration initiated over twice as many prosecutions under the EEA in fiscal year 2017 than the Obama administration did the year before, it remains to be seen what additional executive actions President Trump may take to deter and prevent trade secret theft and cyberespionage involving foreign actors.

In 2018, we will also be watching how courts grapple with the various provisions of the DTSA, which is still in its relative infancy, as well as the lingering questions about the scope of liability under the CFAA.

PTCJ ISSN 0148-7965