Bloomberg Law

BNA's
Patent, Trademark & Copyright Journal®

Trade Secrets

The authors run down the significant developments in trade secrets law in 2016.

2016 Trade Secrets Litigation Round-Up



BY JASON C. SCHWARTZ, GRETA B. WILLIAMS, MICHAEL A. JASKIW AND BRITTANY RAIA

The year 2016 marked the enactment of the first federal civil trade secrets statute, what is believed to be the first-ever federal prosecution for trade secret theft in professional sports, and a case holding that the location of bee hives is a trade secret. Building on our 2015 *Trade Secrets Litigation Round-Up*, we survey these and some of the year's other significant legislative, civil and criminal developments, as well as executive actions taken to curtail international economic espionage and trade secret theft.

I. Legislative Developments

The year's most notable trade secret development was the May 11, 2016, passage of the Defend Trade Secrets Act of 2016 (DTSA). The long-awaited statute provides a federal civil cause of action for the misappropriation of trade secrets. Although the new federal law closely follows the text of the Uniform Trade Secrets Act (UTSA), it departs from the UTSA in two notable ways.

First, in ''extraordinary circumstances,'' the DTSA authorizes ex parte seizures of property by federal law enforcement officers to prevent unauthorized dissemination of trade secrets. The ex parte seizure provision is expected to be used when a defendant is seeking to flee the country or planning to disclose the trade secret to a third party immediately.

Second, the DTSA provides certain protections to whistleblowers who disclose trade secrets for the purpose of reporting or investigating wrongdoing. The DTSA requires employers to provide notice of the statute's whistleblower protections in agreements pertaining to trade secrets entered into after the statute's passage; failure to provide this notice precludes the employer from recovering certain damages under the DTSA.

Notably, in December 2016, one federal court rejected the DTSA whistleblower immunity defense on a motion to dismiss, and ordered the defendant to return allegedly stolen trade secrets to his employer. The district court held that a defendant must present evidence to justify the immunity. *See Unum Group v. Loftus*, No. 16-CV-40154-TSH (D. Mass. Dec. 6, 2016).

Since the statute's enactment in May, at least 48 other DTSA actions have been filed in 28 different fed-

Jason C. Schwartz is a litigation partner in the Washington, D.C., office of Gibson, Dunn & Crutcher and a member of the firm's Executive and Management Committees; his practice includes litigating high-stakes trade secrets, non-compete and employment disputes. Greta B. Williams, Michael A. Jaskiw and Brittany Raia are litigation associates in the firm's Washington, D.C., office.

eral district courts and three state courts. These cases generally involve run-of-the-mill trade secret claims, typically with a departing employee alleged to have taken proprietary materials.

In many of the cases filed to date, plaintiffs unsurprisingly cite the DTSA alongside state trade secret laws and in conjunction with claims for breach of confidentiality and non-solicitation agreements. This trend is likely to continue, as there appears to be little downside to pleading both state and federal causes of action. Moreover, federal district courts generally have been friendly to plaintiffs seeking injunctive relief under the DTSA. Out of 13 identified cases in which district courts have considered requests for temporary restraining orders on their merits, courts have granted TROs nine times.

In response to three identified requests for civil seizure orders, however, such an order has issued just once. In that case, a commercial real estate finance company alleged that an employee had copied its master customer contact list to his personal computer. After the employee failed to appear for a TRO hearing or respond to service of process, the court issued an order for the seizure of files on his computer. *See Mission Capital Advisors LLC v. Romaka*, No. 16-CV-5878 (S.D.N.Y. July 29, 2016).

The sample size to date is small, and results are sure to vary based on the facts of each case. Overall, though, district courts have embraced Congress's intent to create a federal civil trade secrets remedy, and seem attuned to trade secret theft as an issue critical to the nation's economy.

II. Civil Case Developments

The past year saw some high-dollar jury verdicts and further development on the law regarding what qualifies for trade secret protection. We highlight these and some other notable civil case developments below.

A. Significant Jury Verdicts

In what is believed to be one of the largest damages awards in a trade secrets case, in April 2016 a Wisconsin jury awarded medical software company Epic Systems Corp. $940 million in damages against Indian technology services provider Tata Consultancy Services Ltd.—$240 million in compensatory damages and $700 million in punitives. The jury concluded that Tata's employees had illegally downloaded documents for Epic's healthcare software, and used trade secrets contained therein to benefit Tata's competing product. *See Epic Sys. Corp. v. Tata Consultancy Svcs. Ltd.*, No. 3:14-cv-00748 (W.D. Wis. Apr. 27, 2016). Tata has asked the judge to vacate the award.

In May 2016, a Massachusetts jury returned a $70 million verdict against Neovasc Inc., concluding it had misappropriated trade secrets related to a valve CardiAQ was developing. *CardiAQ Valve Techs., Inc. v. Neovasc Inc.*, No. 14-CV-12405-ADB, 2016 BL 362886 (D. Mass. Oct. 31, 2016). A few months later, the presiding judge, in light of what he found was Neovasc's ''willful'' misappropriation, awarded CardiAQ an additional $21 million in enhanced damages. Neovasc is appealing the jury award and the judge's enhancement.

B. Information Eligible for Trade Secret Protection

We also saw several important decisions in 2016 regarding the boundaries of what qualifies for trade secret protection.

For instance, in *Direct Techs., LLC v. Elec. Arts, Inc.*, 836 F.3d 1059, 119 U.S.P.Q.2d 1842 (9th Cir. 2016), Direct Technologies sued Electronic Arts, alleging that EA stole its design for a USB drive related to ''The Sims'' video game and had the drives produced by a competitor. DT brought suit under the California Uniform Trade Secrets Act (CUTSA) and the Copyright Act. In September 2016, the U.S. Court of Appeals for the Ninth Circuit affirmed summary judgment for EA on the trade secret claim, concluding that DT does not derive independent economic value from the secrecy of its design, because DT made no showing that the design had any value outside of this single project for EA. However, the Court reversed summary judgment on DT's copyright claim, concluding that a jury could find the USB's design to be sufficiently original to merit copyright protection.

A Pennsylvania appellate court found that Lyft's trip data was not proprietary or eligible for trade secret protection, and should thus be unsealed. *Lyft, Inc. v. Pa. Pub. Util. Comm'n*, 145 A.3d 1235, 1243 (Pa. Commw. Ct. 2016). Lyft sought a protective order to prevent disclosure of its trip data that the state's Public Utility Commission had ordered it to produce during an administrative proceeding where Lyft was seeking authorization to operate in Pennsylvania. The court denied Lyft's request, finding that the data, which consisted of the total number of trips Lyft had provided during certain periods, was not proprietary and was instead merely ''aggregated information lacking sufficient detail to allow a competitor to cause substantial competitive harm.''

In *McDonald Apiary, LLC v. Starrh Bees, Inc.*, No. 8:14-CV-351, 2016 BL 338908 (D. Neb. Oct. 10, 2016), McDonald Apiary sued Starrh Bees, alleging that Starrh had misappropriated the location of the strategic sites McDonald had chosen for Starrh's beehives. Starrh argued that this location information was not secret, because it could be reverse engineered through simply looking for the beehives' locations on roads, in maps and on the internet. But the court found that the question of trade secret eligibility should survive summary judgment, because there was a difference between information ''that is readily ascertainable and that which is *realistically* ascertainable.''

C. Intersection between the Copyright Act and State Trade Secret Law

In *GlobeRanger Corp. v. Software AG, Inc.*, 836 F.3d 477, 120 U.S.P.Q.2d 1053 (5th Cir. 2016), Software AG appealed a $15 million trial verdict for misappropriation of its radio frequency identification technology, arguing that GlobeRanger's misappropriation claim, brought under the Texas Uniform Trade Secrets Act (TUTSA), was preempted by the federal Copyright Act. The U.S. Court of Appeals for the Fifth Circuit rejected the preemption argument, concluding that the TUTSA provides ''substantially different protection than copyright law,'' because it requires establishing an additional element beyond what is required to make out a copyright violation: that the protected information was taken via improper means or breach of a confidential relationship.

III. Criminal Developments

The Obama Administration continued to aggressively pursue criminal actions to address and deter trade se-

   ISSN 0148-7965

cret theft and economic espionage during 2016. As in prior years, a number of these cases involved Chinese nationals. Below, we highlight some of the most notable criminal cases of 2016.

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 2016, there were six new prosecutions and five new convictions under 18 U.S.C. § 1832, and one new prosecution under 18 U.S.C. § 1831.

For instance, in January 2016, federal prosecutors charged five individuals (including two Chinese nationals) with, inter alia, conspiring to steal biopharmaceutical trade secrets from GlaxoSmithKline in violation of the EEA. The indictment alleges that three of the defendants had formed a company in China to allegedly sell the stolen trade secret information. *See United States v. Yu Xue*, No. 2:16-CR-22-JHS (E.D. Pa. Jan. 20, 2016).

In October 2016, a former executive of a Chinese conglomerate was sentenced to three years in prison for conspiring to steal trade secrets from DuPont Pioneer and Monsanto Co. Mo Hailong pled guilty in January to participating in a long-term conspiracy with several other Chinese nationals to steal valuable corn seeds from the U.S.-based seed manufacturers' production fields and transport those seeds to China, in violation of EEA. *United States v. Mo Hailong*, No. 4:13-CR-147-SMR-CFB (S.D. Iowa Jan. 27, 2016).

B. Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act (CFAA) provides federal civil and criminal causes of action against any person who, in relevant part, ''intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer,'' or who ''intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.'' 18 U.S.C. § § 1030(a)(2)(C), (a)(5)(C), (g).

In 2016, federal prosecutors obtained several significant penalties in CFAA cases involving the theft of trade secrets, and the Ninth Circuit issued some important guidance about the meaning of ''without authorization'' under the CFAA.

Our 2014 *Round-Up* discussed the August 2014 indictment of Su Bin, the owner and manager of a Chinese aviation company, for violations of the CFAA. In March 2016, Bin pled guilty to conspiring to export trade secret information about sensitive military programs, after accessing computer systems belonging to U.S. defense contractors. In July, Bin was sentenced to 46 months in prison and ordered to pay a $10,000 fine. *United States v. Bin*, No. 8:14-CR-00131-CAS-1 (C.D. Cal. July 18, 2016).

In July 2016, a former St. Louis Cardinals executive also received a 46-month prison sentence in what is believed to be the first-ever federally-prosecuted case of corporate espionage in North American professional sports. Christopher Correa pled guilty in January to five counts of accessing the Houston Astros' computers in violation of the CFAA. Correa admitted that he illicitly accessed the Astros' private online database, which contained scouting reports and information about possible trades. Correa was also ordered to pay $279,038 in restitution to the Astros. *United States v. Correa*, No. 4:15-CR-679 (S.D. Tex. July 21, 2016).

Finally, the Ninth Circuit issued yet another ruling in the high-profile case of David Nosal, who, as reported in the 2014 and 2015 *Round-Ups*, was charged in 2008 with violating the CFAA and misappropriating trade secrets from his former employer's database. In 2013, Nosal was convicted on charges that that he accessed the database ''without authorization'' under the CFAA.

In July 2016, a divided Ninth Circuit panel affirmed Nosal's conviction. The court found that Nosal had accessed his former employer's network ''without authorization'' because ''once authorization . . . has been affirmatively revoked, the user cannot sidestep the statute by . . . accessing the computer through a third party.'' *United States v. Nosal*, 828 F.3d 865, 868-69, 2016 BL 214844 (9th Cir. July 5, 2016).

Nosal subsequently petitioned the Ninth Circuit for rehearing en banc. He argued that the panel gave no guidance on how to distinguish innocuous password sharing, like borrowing a spouse's password with his permission, from actual criminal conduct. The American Civil Liberties Union filed an amicus brief in support. In December, in a published opinion denying Nosal's petition for rehearing, the Ninth Circuit affirmed Nosal's conviction under the CFAA. The divided panel clarified that Nosal's use of another's password to access his former employer's database and take its data was distinct from innocent password sharing because the employer explicitly revoked his access and his access was made ''knowingly and with intent to defraud.'' *United States v. Nosal*, No. 14-10037, 2016 BL 409354 (9th Cir. Dec. 8, 2016).

IV. Executive Actions

As noted in the 2015 *Round-Up*, on April 1, 2015, President Barack Obama signed an executive order establishing a sanctions program authorizing penalties on foreign actors who engage in cyberattacks or commercial espionage. In March 2016, the president extended this order through April 1, 2017. Obama relied upon this authority in his widely-reported sanctions against Russia as a result of alleged election-related hacking. (Note: Prior to sanctioning Russia, Obama amended the April 1, 2015, order to provide additional authority for responding to cyber activity aimed at interfering with the U.S. election process.).

In last year's *Round-Up*, we also reported on a September 2015 agreement between Obama and President Xi Jinping of China regarding economic espionage, under which neither government would conduct nor knowingly support cyber-enabled theft of intellectual property, including trade secrets, for commercial advantage. In October 2016, U.S. officials and outside experts reported that Chinese hacking thefts of American corporate trade secrets had plummeted in the 13 months after Obama and Xi's agreement, with one cyber-security firm finding a 90 percent drop during that timeframe. One expert called this ''the biggest success we've had in this area in 30 years,'' attributing the success to ''the threat of sanctions and the impact on [the Chinese] economy.'' Ken Dilanian, *Russia May Be Hacking Us More, But China is Hacking Us Much Less, NBCNews* (Oct. 12, 2016, 6:25 AM). Interestingly, a June 2016 report by another cyber-security company shows that the decrease in Chinese hacking thefts be-

gan in mid-2014, a year before President Obama and President Xi Jinping announced their agreement. *See* Michael D. Goldhaber, *In Praise of Cyber Lawfare*, *Am. Law* (Sept. 1, 2016).

Conclusion

Developments in 2016 demonstrate that U.S. companies remain vulnerable to trade secret theft and misappropriation from domestic and foreign actors.

As we look ahead, it remains to be seen how President Trump will approach trade secret theft and cyberespionage involving foreign actors. While Trump has downplayed allegations that Russia interfered with the presidential election, he may take a tougher stance with China. Indeed, he stated in June that ''[i]f China does not stop its illegal activities, including its theft of American trade secrets, I will use every lawful presidential power to remedy trade disputes.''

In 2017, it will also be interesting to monitor developments under the DTSA. Because the statute is not retroactive, it will likely take some time for DTSA cases to gain momentum in federal court, and, even after the look back period expands, many plaintiffs may elect to file trade secret actions in state courts, which are sometimes quicker to act on such matters. Nonetheless, trade secret filings in federal court are likely to increase in the coming year.

  PTCJ ISSN 0148-7965