Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

10 Key Trade Secret Developments Of 2015: Part 2

Law360, New York (January 15, 2016, 10:46 AM ET) --

Kerry L. Bundy

2015 brought significant developments in trade secret law, both in the U.S. and abroad. In-house counsel and private practitioners should consider trends that promise to shape further developments in the years ahead.

In part 1 of this two-part series, we highlighted five trends in particular: (1) increased cooperation between the United States and China on cyberattacks; (2) the continued circuit split regarding the scope of the Computer Fraud and Abuse Act; (3) heightened scrutiny applied to unsupported trade secret suits; (4) the Trans-Pacific Partnership's potential effect on the protection of trade secrets around the world; and (5) the increasing prevalence of threats to confidential information in every field and industry, even America's "national pastime."

In part 2, we highlight five more: (6) yet another attempt at providing a uniform federal regime and a federal cause of action for trade secret misappropriation; (7) the interplay between state trade secret law and preemption under the federal Copyright Act, as analyzed by the Fifth Circuit; (8) federal prosecutors' increasing focus on prosecuting those who steal the financial industry's trade secrets; (9) the EU's significant progress toward the passage of the Trade Secret Directive; and (10) the end of the long-running battle between DuPont and Kolon and the challenges a trade secret owner must overcome to resist misappropriation by a foreign company.

A "takeaway" summarizing key issues and guidance appears at the end of each topic.

6. Another Year, Another Attempt at Offering Federal Trade Secret Protection

The Defend Trade Secrets Act is back. On July 29, 2015, only months after watching the 2014 version fizzle, a bipartisan group of U.S. senators and representatives introduced the Defend Trade Secrets Act of 2015. As the bill gained momentum toward the end of 2015, observers are wondering whether a federal cause of action for trade secret misappropriation may finally become a reality.

If the DTSA sounds familiar, that is because introducing it has become something of a yearly congressional routine. Last year in a Law360 piece, we **profiled** the gathering momentum behind the Defend Trade Secrets Act of 2014. Introduced by Sens. Christopher Coons, D-Del., and Orrin Hatch, R-Utah, the bill was intended to enhance trade secret protection by strengthening remedies for trade secret theft. But it was criticized for, among other things, its relatively broad provisions enabling the seizure of computers and other property that were used in the alleged misappropriation. The signs of

momentum proved temporary, and like its 2013 predecessor bills, the Defend Trade Secrets Act of 2014 failed to be enacted.

Undeterred, the DTSA's supporters renewed their efforts in 2015 and sought to ameliorate some of the concerns with the 2014 bill. In particular, the 2015 DTSA curtails a court's power to order the seizure of property allegedly used in the misappropriation. Where previous versions permitted seizure even if simply to preserve evidence, the 2015 bill limits that power to situations where seizure is "necessary to prevent the propagation or dissemination of the trade secret that is the subject of the action." The bill also requires a finding that

- a temporary restraining order is insufficient to protect the trade secret;
- an immediate and irreparable injury will occur absent seizure;
- the harm to the plaintiff absent seizure outweighs the harm to the legitimate interests of the defendant; and
- the plaintiff is likely to succeed in showing
    - the existence of a trade secret;
    - misappropriation of the trade secret by the defendant; and
    - possession of the trade secret by the party against whom seizure would be ordered.

Support for the bill among members of Congress continues to swell: According to a recent report, the DTSA has 15 co-sponsors in the Senate and over 90 co-sponsors in the House.[1] Whether this bipartisan support will translate to final passage or, as with previous versions, fizzle before reaching a final vote remains to be seen. Signs of progress have emerged from the Senate Judiciary Committee, where the bill remains as of this writing. And the DTSA's sponsors appear motivated to push the bill through to the floor. The upcoming weeks will tell us whether the Defend Trade Secrets Act will finally become reality, or whether supporters will have to wait for the 2016 version.

Takeaway

The Defend Trade Secrets Act is back, and momentum is again building toward a federal cause of action for trade secret misappropriation. Stay tuned — will this finally be the year?

7. The Fifth Circuit Does Copyright Preemption

While observers wait to see whether a federal cause of action for trade secret misappropriation will finally materialize, trade secret litigators continue to practice in the federal courts where the requirements of diversity or federal question jurisdiction are satisfied. In 2015, two cases from the Fifth Circuit — one decided, one pending — relate to another potential method for reaching federal court: removal based on complete copyright preemption of trade secret claims.

The federal Copyright Act offers copyright owners certain exclusive rights over works that fall within the scope of the Act, including (among others) the rights to "reproduce," "distribute" and "perform" those works.[2] In order to defend the exclusivity of these protections, the act preempts all state law claims if those claims are brought against works falling within the subject matter of copyright and if they assert a right equivalent to any of the owner's exclusive copyright rights.[3]

The defense of complete copyright preemption under Section 301 packs a punch not just substantively

but jurisdictionally. Courts — including the Fifth Circuit — have held that copyright preemption of even one state law claim can support a defendant's removal to federal court.[4] But exactly which state law claims are amenable to preemption (and which are not) remains an issue that has divided federal courts.

The Fifth Circuit addressed that very issue in 2015. In Spear Marketing Inc. v. Bancorpsouth Bank,[5] a plaintiff filed a bevy of Texas state law claims — including for trade secret misappropriation and for violation of the Texas Theft Liability Act — related to the alleged theft of trade secrets in plaintiff's software program. After the defendants removed the case to federal court on the basis of copyright preemption, the district court denied plaintiff's motion to remand, holding that the TTLA claim was preempted. It also granted summary judgment against plaintiff's trade secret misappropriation claim.

The Fifth Circuit affirmed both rulings. Addressing preemption, the court held that plaintiff's TTLA claim satisfied the first prong of copyright preemption because it was "based on ideas fixed in tangible media," namely, computer software. It also held that the second prong of copyright preemption was satisfied because the wrongful acts claimed by plaintiff — copying, communicating and transmitting — were "equivalent acts to reproducing and distributing." As a result, the Fifth Circuit held, plaintiff's TTLA claim fell within the preemptive scope of the Copyright Act and the district court correctly denied remand of that claim.[6]

While Spear Marketing involved copyright preemption of a TTLA claim, the Fifth Circuit is now poised to analyze the scope of copyright preemption related to a state trade secret misappropriation claim. In GlobeRanger Corp. v. Software AG USA Inc.,[7] a Northern District of Texas court denied defendants' motion for judgment as a matter of law on the basis of copyright preemption, after a jury awarded $15 million to plaintiff on its trade secret claim. Notably, the court and parties recognized that the Fifth Circuit has never analyzed how the second prong of copyright preemption — whether the state law claim protects "equivalent" rights to those protected by federal copyright — applies to Texas trade secret misappropriation claims. On appeal, the Fifth Circuit will have the opportunity to address that issue, with oral argument scheduled for February 2016.[8]

Takeaway

The door to federal court opens when the federal Copyright Act completely preempts one of plaintiff's state law claims. The Fifth Circuit appears poised to address the scope of that preemptive power as it relates to state trade secret claims. Stay tuned.

8. Federal Prosecutors Focus On Source-Code Thieves, but the Flash Boy Makes a Getaway — Again

Sophisticated financial institutions continue to seek any competitive advantage in the lucrative high-frequency trading industry. At the same time, misappropriation of the valuable source code used to engage in high-frequency trading by former employees is on the rise. Source code comprises the original program instructions for computer software. Source code — the only kind of code human beings can read — reveals how a computer program works and can unlock a firm's trade secrets underlying its high-frequency trading program.

Recognizing that the confidentiality of source code is central to the vitality of the country's financial markets, federal prosecutors have shown an increased willingness in recent years to go after those accused of misappropriating source code from investment firms. In a recent case out of the Northern District of Illinois, two former employees of Citadel LLC, a Chicago-based hedge fund operating in the high-frequency trading space, pleaded guilty to participating in a scheme to steal Citadel source code to

devise their own personal trading platform.[9] This case is part of a broader trend initiated by the U.S. Department of Justice to bolster its enforcement efforts related to trade secret theft in the financial services industry.[10]

These increased enforcement efforts, however, have faced setbacks. A prime example is the saga of Sergey Aleynikov, dubbed by some as a "Flash Boy."[11] Aleynikov, a former programmer at Goldman Sachs Group Inc., has been twice accused of stealing the bank's high-frequency trading source code. New York federal prosecutors initially obtained convictions under the National Stolen Property Act and the Economic Espionage Act, but the Second Circuit overturned those convictions.[12] Undeterred, state prosecutors in Manhattan then pursued charges under New York state law: unlawful use of secret scientific material and unlawful duplication of computer related material. A jury convicted Aleynikov of the first charge but the trial judge later reversed that conviction, concluding that the state had failed to present evidence that Aleynikov downloaded the source code to a "tangible reproduction" or with intent to misappropriate.[13]

Takeaway

The Citadel and Aleynikov cases foreshadow potential future developments in the pursuit of source-code theft convictions. Federal prosecutors will likely intensify efforts to bring to justice employees who steal their former employers' proprietary source code — both in the financial services sector and beyond. And state legislatures will likely re-examine their laws to determine whether they adequately cover this more modern and ever growing form of trade secret misappropriation. Regardless, in-house counsel should consider reporting electronic thefts to law enforcement agencies.

9. Europe's Trade Secret Directive Nears Passage, Despite Some Opposition

Trade secret protection is gaining ground not only at the federal level in the Unites States (see Trend 6, above) but also in the European Union. During 2015, the EU made significant progress toward passage of a new legal framework (known as a trade secrets "directive") that would significantly reshape and harmonize — although not standardize — the various trade secret laws in the EU's member nations. Unlike regulations, directives do not regulate member states directly. Rather, directives identify certain objectives that EU member states must achieve, through a variety of means, including legislation, within a defined period of time.

The EU published its first draft proposal for a directive on the protection of trade secrets in November 2013. In May of 2014, the Council of the European Union agreed on a set of revisions to that directive. In December of 2014, the European Public Health Alliance, a group of health care nongovernmental organizations, patients' rights groups and health care practitioners announced its opposition to the directive, claiming that the directive was a "threat to health, environment, free speech, and worker mobility."[14] For instance, the alliance claimed that the trade secrets directive contained "[a]n unreasonably broad definition of 'trade secrets' that enables almost anything within a company to be deemed as such," and "could endanger freedom of expression and information, corporate accountability, information sharing — possibly even innovation — in the EU."[15]

On June 6, 2015, the European Parliament's legal affairs committee approved the directive's text. Constance Le Grip, who is guiding the legislation through parliament, explained that "giving companies the means to protect their know-how and professional information against any unlawful acquisition throughout Europe provides better protection for innovation, competitiveness and employment in Europe."[16] But Le Grip also explained that the committee had "substantially amended and improved

the initial text since it is all the more crucial to protect fundamental freedoms and guarantee the full exercise of freedom of expression and information, starting with media freedom and pluralism, but also to guarantee workers professional mobility."[17] The committee approved a mandate to start informal talks with the EU Council in the hopes of reaching a first-reading agreement.

On Dec. 15, 2015, the EU Commission, the EU Council and the European Parliament (the primary political EU political bodies) reached political agreement — quite unexpectedly — on the draft trade secrets directive.[18] A few days later, the EU Council published the agreed-upon text of the directive, which was largely unchanged from prior versions.[19] The EU Parliament is tentatively scheduled to vote on the directive in March 2016. If the directive is approved by the EU Parliament and the council, it will go into force 20 days later, at which point EU member states will have two years to implement the directive in their national laws.

Notably, the final draft of the directive contains the following definition of trade secrets:

"trade secret" means information which meets all of the following requirements: (a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (b) has commercial value because it is secret; (c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.[20]

This definition is substantially similar to the definition in the Uniform Trade Secrets Act, which has been adopted by many U.S. jurisdictions. If passed, the trade secrets directive could bring much-needed consistency to the regulation of trade secrets.

Takeaway

The EU is very close to enacting a legal framework that would significantly strengthen and standardize the protection of trade secrets in EU member nations. This is good news for companies that operate in Europe, specifically, and for trade secret owners' hopes for increased uniformity in trade secret regulation around the world.

10. The End of the Long-Running Battle between DuPont and Kolon Highlights the Threat of International Trade Secret Misappropriation and the Importance of Persistence

In April 2015, Kolon Industries Inc. finally settled the trade secret claims brought against it by E.I. DuPont de Nemours & Co. and an Economic Espionage Act criminal indictment.[21] Under the terms of the plea agreement, Kolon will pay $275 million to DuPont and $85 million in fines to the government. This settlement puts an end to one of the highest-profile and most significant trade secret cases of the past decade.

The civil dispute between DuPont and Kolon was long-standing and contentious. The battle began in 2009, when DuPont sued Kolon, a South Korean company, for trade secret misappropriation in Virginia federal court. DuPont claimed that Kolon hired former DuPont employees in order to acquire trade secrets related to DuPont's proprietary Kevlar product. In 2011, a jury awarded nearly $1 billion in damages to DuPont. Three years later, in 2014, the U.S. Court of Appeals for the Fourth Circuit reversed the judgment because the trial court had barred Kolon from presenting evidence that DuPont may have disclosed the trade secrets at issue during the course of a 1980s intellectual property dispute between

DuPont and a competitor. The Fourth Circuit remanded the case (to a different trial court judge) for further proceedings. The retrial was scheduled for August 2015. The authors of this article **identified** the Fourth Circuit's decision as one of the 10 most significant trade secret developments of 2014.[22]

While the civil case was unfolding, the United States was also waging a yearslong battle to force Kolon to appear in U.S. district court for arraignment on criminal charges under the Economic Espionage Act. In August 2012, the DOJ obtained an indictment against Kolon.[23] In October 2012, the DOJ served summons on a variety of entities related to Kolon, including its attorney in the civil dispute with DuPont, Kolon's U.S. subsidiary, and the government of South Korea.[24] Kolon moved to quash the indictment on the basis that it had not been properly served under Federal Rules of Criminal Procedure.

Specifically, Kolon argued that the government had not satisfied Rule 4's "mailing requirement," which requires that a summons be mailed to an organization's last known address in the district or to its principal place of business in the United States. Kolon argued that this requirement cannot be satisfied for a foreign company because it has not last known address in the district or principal place of business in the United States. The courts are split on this issue. Some courts have agreed with Kolon's position, while others have held that the "mailing requirement" is no requirement at all. In this case, the district court held that the mailing provision was not a requirement of service.[25] But the district court quashed the summons (although it refused to dismiss the indictment) because the government had not satisfied Rule 4's requirement that it be served on an officer or managing, appointed, or general agent of the organization.[26]

The DOJ was eventually able to effect service of the summons with the help of the South Korean government under the terms of the mutual legal assistance treaty. In December 2014, the district court denied a second motion to quash by Kolon, finding that service through the treaty was sufficient.[27] Four months later — and before Kolon appeared for its arraignment — the DOJ announced that it had entered into a global settlement with Kolon resolving both the criminal charges and DuPont's civil claims.[28]

Takeaway

The DuPont case teaches several lessons. First, the threat of international trade secret misappropriation is significant. Second, the obstacles to resisting this type of misappropriation can be significant. Third, a parallel criminal indictment can provide a powerful tool to force a negotiated resolution. And finally, persistence is a key virtue for in-house counsel and trade secret litigators.

—By Randall E. Kahnke, Kerry L. Bundy, Tyler A. Young and Peter C. Magnuson, Faegre Baker Daniels LLP

Randy Kahnke and Kerry Bundy are partners and Tyler Young and Peter Magnuson are associates in the Minneapolis office of Faegre Baker Daniels.

[1] http://www.tradesecretslaw.com/2015/12/articles/trade-secrets/update-on-the-senate-judiciary-committees-hearing-on-the-protection-of-trade-secrets/

[2] 17 U.S.C. § 106.

[3] 17 U.S.C. § 301.

[4] GlobeRanger Corp. v. Software AG, 691 F.3d 702, 706 (5th Cir. 2012).

[5] 791 F.3d 586 (5th Cir. 2015).

[6] Id. at 598.

[7] No. 3:11-cv-0403, 2015 WL 3648577 (N.D. Tex. June 11, 2015).

[8] See GlobeRanger Corp. v. Software AG, No. 15-10121 (5th Cir.).

[9] U.S. v. Pu, 1:11-cr-00699 (N.D. Ill.) and U.S. v. Uppal, 1:11-cr-00699-2 (N.D. Ill.).

[10] See, e.g., Administration's Strategy on Mitigating the Theft of U.S. Trade Secrets (2003), https://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf.

[11] Michael Lewis, Flash Boys: A Wall Street Revolt (W.W. Norton & Company 2014).

[12] United States v. Aleynikov, 676 F.3d 71 (2d Cir. 2012).

[13] People v. Aleynikov, 15 N.Y.S.3d 587 (N.Y. Sup. Ct. 2015).

[14] http://www.epha.org/6264

[15] Id.

[16] http://www.europarl.europa.eu/news/en/news-room/20150615IPR66493/Trade-secrets-freedom-of-expression-must-be-protected-say-legal-affairs-MEPs

[17] Id.

[18] http://www.europarl.europa.eu/pdfs/news/expert/infopress/20151215IPR07674/20151215IPR07674_en.pdf

[19] http://data.consilium.europa.eu/doc/document/ST-15382-2015-REV-1/en/pdf

[20] Id. at Art. 2, Section (1).

[21] http://www.justice.gov/opa/pr/kolon-industries-inc-pleads-guilty-conspiring-steal-dupont-trade-secrets-involving-kevlar

[22] See http://www.law360.com/articles/603592/top-10-trade-secrets-developments-of-2014-part-1

[23] United States v. Kolon Indus, Inc., 926 F. Supp. 2d 794, at 797 (E.D. Va. 2013)

[24] Id. at 803-04.

[25] Id. at 802.

[26] Id. at 808-21.

[27] United States v. Kolon, Case 3:12-cr-00137 (AJT), Filing No. 173 (December 23, 2014).

[28] United States v. Kolon, Case 3:12-cr-00137 (AJT), Filing No. 190 (April 30, 2015).