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 1

Law360, New York (December 16, 2015, 10:27 AM ET) --

Randall E. Kahnke

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 (part 2 will publish in January), we highlight 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."

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

1. The United States and China Pledge Cooperation in Combating Trade Secret Theft

The United States and China may finally have achieved a breakthrough in combating trade secret theft. Tensions mounted over the issue in the first half of 2015, as the United States threatened sanctions against Chinese entities that participate or benefit from economic espionage. But the second half of 2015 saw increased cooperation between the two countries, raising hopes that Chinese-based theft of U.S. trade secrets may be on the decline.

For years, U.S. businesses have confronted cyberattacks — often involving attempted theft of trade secrets — from Chinese hackers. The issue came to a head in 2015. In July, the FBI highlighted a 53 percent increase in economic espionage cases, the vast majority of which originated in China and appear to have been state sanctioned. The attacks reportedly cost the U.S. economy hundreds of billions of dollars over that time frame.

In response, the United States ratcheted up the pressure on China in the first half of 2015. In April, President Obama issued an executive order declaring the "increasing prevalence and severity" of foreign-based cyberattacks a "national emergency."[1] The order permitted a freeze on U.S.-based assets of those engaging in, supporting, or knowingly reaping the benefits of cyber-based economic espionage. And in August, only weeks before China's President Xi Jinping visited the White House, news leaked that the United States was considering invoking the executive order and imposing substantial economic sanctions against Chinese companies and individuals enjoying the fruits of the theft of U.S. trade secrets.

President Obama's response appears to have paid dividends, as the second half of 2015 has seen an increased commitment between the two countries to combat trade secret theft. After their White House meeting in September, Presidents Xi and Obama agreed both not to conduct or knowingly support cybertheft of trade secrets to support domestic businesses and to increase law enforcement cooperation regarding "malicious cyber activities."[2] And as a result of the countries' Joint Commission on Commerce and Trade in November, China clarified its intent to offer greater judicial protection to companies confronting the theft of trade secrets,[3] including by making preliminary injunctive relief more readily available. These commitments, which a U.S. official termed "a big deal," would enhance the ability of American companies to protect trade secrets in the Chinese court system.

It remains to be seen, of course, whether this diplomatic progress will produce any tangible benefit for U.S. businesses in their efforts to protect trade secrets and confidential information. But 2015 will depart amidst renewed hope that China's targeting of U.S. trade secrets may finally be on the decline.

Takeaway

The United States has made significant diplomatic progress at stanching the flow of U.S. trade secrets to China. The ultimate success of these efforts remains to be seen. In the meantime, companies should continue to beef up protections against foreign-based cyberattacks and theft of trade secrets.

2. Division on the Scope of the Computer Fraud and Abuse Act Persists

A recent decision out of the Northern District of California highlights the continued circuit split on the extent to which the Computer Fraud and Abuse Act reaches the misappropriation of trade secrets. The CFAA imposes civil and criminal liability for obtaining information from a protected computer by either "access[ing a] ... computer without authorization" or "exceed[ing] authorized access."[4] The Ninth and Fourth Circuits have read the CFAA narrowly, applying it only to unauthorized access of information. In contrast, the Fifth, Seventh and Eleventh Circuits have viewed the CFAA more broadly, applying it to improper use of information, as well.

In Koninklijke Philips NV v. Elec-Tech International Co., a federal California district court waded further into this split. The court rejected an agency-based theory of CFAA liability, which would have held parties liable for accessing information through another party that had authorization to access the information.[5] Philips Lumileds, a developer of LED technology, sued 11 defendants, including a Chinese-based competitor, Elec-Tech, along with various Elec-Tech subsidiaries and corporate directors, and a former Lumileds engineer and current Elec-Tech employee, Gangyi Chen. Lumileds alleged that Chen, while still employed, downloaded thousands of files containing trade secrets and confidential information, went to work for Elec-Tech, and shared the data with four of the other defendants. Six months later, Elec-Tech announced new LED products. Lumileds asserted nine state law claims and one CFAA claim, arguing that although Chen had access to the information, those with whom he shared the information did not have legitimate access, and their use of the information violated the CFAA. Defendants moved to dismiss for failure to state a CFAA claim.

Following the Ninth Circuit's interpretation of the CFAA, the district court nixed Lumiled's "indirect access theory" of CFAA liability. The court reiterated the view that "the CFAA was designed to target hacking, not misappropriation."[6] Based on that distinction between access and use, the court concluded that because the four Defendants did not download the information themselves, they did not "engage in the hacking" but "merely benefited from its results." Indeed, the court warned that if it had

allowed “the mere pleading of an agency relationship” to “render [an] outsider subject to liability,” “it would effectively federalize all trade secret misappropriation cases where parties use a computer to download sensitive or confidential trade secret information — which would be nearly every trade secret case nowadays.”[7] The court dismissed the CFAA claim and declined to exercise supplemental jurisdiction over the remaining state law claims.

Although developments over the last year have increased the chances that the U.S. Supreme Court will resolve the circuit split over the CFAA’s reach, that split persists today. And Congress has not amended the CFAA or created the long-debated federal claim for trade-secret misappropriation, which could shed light on the CFAA’s scope.

Takeaway

The Lumileds decision reinforces the need for counsel bringing or defending CFAA claims based on the misappropriation of information to pay attention to the respective jurisdictional views on the matter—at least until Congress or the Supreme Court clarifies the extent of CFAA liability for misappropriation.

3. The Importance of Careful Presuit Investigation

A trend is developing toward holding plaintiffs and their lawyers liable for unsupported trade secret lawsuits. The continuing fallout from the FLIR Systems Inc. v. William Parrish lawsuit is a prime example of this trend.[8]

In 2004, FLIR, a manufacturer of infrared cameras and thermal imaging systems, purchased Indigo Systems Corporation, a manufacturer of certain components of FLIR’s products called microbolomoters. For the next two years, FLIR employed two former officers of Indigo. In 2006, those two former Indigo officers left FLIR to form their own business, which would also manufacture microbolomoters. The former Indigo officers attempted to avoid a dispute by promising not to misappropriate FLIR’s trade secrets, but FLIR sued them in California state court seeking damages and injunctive relief.

The trial court denied the officers’ summary judgment motion, finding that there were triable issues of fact and emphasizing that the technology involved was “highly technical.”[9] In denying the officers’ motion, the trial court relied on FLIR’s expert declarations that the officers’ new venture could not succeed without using FLIR’s trade secrets. After trial, however, the court rejected all of FLIR’s claims and found that FLIR had brought the litigation in bad faith. Specifically, the trial court found that FLIR’s suit was based on an inevitable disclosure theory (i.e., that a former employee’s responsibilities at a new company will inevitably require the disclosure of the former employer’s trade secrets) that California has rejected because it impedes employee mobility.[10] The court sanctioned FLIR and awarded the former Indigo officers $1.6 million in attorneys’ fees and costs. The California Court of Appeals affirmed the award against FLIR.[11]

In 2012, the former officers brought a malicious prosecution lawsuit against Latham & Watkins LLP and the individual Latham attorneys who had represented FLIR, alleging that they should have known that the original suit was impermissibly based on the inevitable disclosure theory and brought with an anti-competitive purpose.[12] The trial court granted Latham’s anti-SLAPP motion, finding that the lawsuit had been brought outside the statute of limitations. The California Court of Appeals held that the suit was timely filed but affirmed the SLAPP dismissal on the grounds that the “interim adverse judgment rule” established that Latham had a basis to bring the suit.[13] In other words, the appellate court held that Latham had a legitimate basis to bring the suit because it had survived summary judgment in the

underlying action. The court of appeals rejected the officers' arguments that the interim adverse judgment rule did not apply because the summary judgment ruling was procedural and not substantive and because the summary judgment ruling was nullified by the court's post trial finding of bad faith.[14]

The California Supreme Court has granted the former officers' petition for review.[15] The California Supreme Court's decision may provide much needed guidance to trade secret litigators regarding the boundary between zealous advocacy and anti-competitive behavior.

Takeaway

Trade secret owners are justifiably concerned when employees who had access to trade secrets form new, competing ventures. But trade secret owners (and their attorneys) should balance their desire to move expeditiously against the need to ensure that they have a sufficient legal and factual basis for filing (and maintaining) suit.

4. The Trans Pacific Partnership Promises to Enhance Trade Secret Protection ... or Maybe Not

Support for an international agreement on trade secret protection is growing, but the terms of such an agreement are still uncertain. The years-long secret negotiation of the Trans-Pacific Partnership, a wide-ranging trade agreement between 12 participating member nations, concluded on Oct. 4, 2015. Although not yet approved by Congress, the TPP has the potential to alter the protection of trade secrets across Australia, Brunei Darussalam, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, the United States and Vietnam. The TPP does not, however, apply to Russia, China or North Korea.

In October 2015, the Office of the United States Trade Representative released a report summarizing the then-undisclosed terms of the TPP.[16] According to the USTR, the TPP's intellectual property chapter would "cover[] patents, trademarks, copyrights, industrial designs, geographical indications, trade secrets, other forms of intellectual property, and enforcement of intellectual property rights." According to the report, TPP member nations would be required to "provide strong enforcement systems, including, for example, civil procedures, provisional measures, border measures, and criminal procedures and penalties for commercial-scale trademark counterfeiting and copyright or related rights piracy." Specifically, the USTR report claimed that TPP members would be required to "provide the legal means to prevent the misappropriation of trade secrets, and establish criminal procedures and penalties for trade secret theft, including by means of cyber-theft."

On Nov. 5, 2015, the Obama administration released the full text of the TPP, Chapter 18 of which addresses intellectual property issues.[17] The intellectual property chapter is more than 70 pages long, but the portion addressing trade secret issues is only one page long. The TPP does contain a high-level requirement that each member country "ensure that persons have the legal means to prevent trade secrets lawfully in their control from being disclosed to, acquired by, or used by others (including state-owned enterprises) without their consent in a manner contrary to honest commercial practices."[18] But the agreement is murky on what specific steps the member countries are required to take to achieve that goal.

Notably, the TPP does not require member nations to provide a private civil remedy for trade secret misappropriation, as many commentators had hoped. The TPP does require that member countries "provide criminal procedures and penalties" for trade secret misappropriation.[19] But the TPP also

significantly limits the criminal procedures that member nations must provide. The TPP allows member countries to limit the availability of criminal procedures or penalties to situations in which:

- the acts are for the purposes of commercial advantage or financial gain;
- the acts are related to a product or service in national or international commerce;
- the acts are intended to injure the owner of such trade secret;
- the acts are directed by or for the benefit of or in association with a foreign economic entity; or
- the acts are detrimental to a Party's economic interests, international relations, or national [defense] or national security.[20]

If these provisions are applied literally, the TPP may not — even if it is eventually approved and implemented — actually require its member nations to provide much by way of trade secret protection.

Takeaway

Countries around the world are working toward international agreement on trade secret protections. But until a more definitive agreement is reached, trade secret owners should continue to consider each country's trade secret laws and to take appropriate country-specific steps to protect their intellectual property.

5. Cyberespionage Reaches the Major Leagues

Given the proliferation of malicious online activity in recent years, it was perhaps inevitable that cyberespionage would one day reach the major leagues — Major League Baseball, that is. In June 2015, news leaked that the FBI and the U.S. Department of Justice were investigating St. Louis Cardinals executives reportedly for accessing and reviewing proprietary information contained in an online database owned by the Houston Astros. The investigation made headlines given the high profile of the MLB franchises at issue. But it also should intrigue trade secret litigators for at least two other reasons.

First, the information was unique and at least arguably trade secret. It appears to have been valuable: The Astros and other franchises have invested significant resources into developing and utilizing unique and proprietary statistical models to forecast player performance. And each franchise closely guards its own statistical models, hoping that they give it a competitive advantage over its competitors. These, of course, are prerequisites to trade secret protection under the Uniform Trade Secrets Act.

Second, the means of access was entirely common, albeit with a unique twist. As is often the case, the access involved a former employee — Jeff Luhnow, who left the Cardinals to become the Astros' general manager in 2011. But here, the former employee did not hack into the company's database; rather, the company accessed the database of the former employee's new company. It was rumored that a Cardinals executive may have used Luhnow's — or another former employee's — password from his time with the Cardinals to access the Astros' database. If true, the breach would have been entirely preventable had the Astros used basic password-security measures.

As of yet, no charges have been filed. (The Cardinals have fired an employee who reportedly admitted to accessing the database.) But the news is yet another reminder that, where proprietary and confidential information is involved, no industry is immune from the dangers of cyberespionage.

Takeaway

Companies in every industry must be vigilant against the unauthorized access and use of confidential information and trade secrets. One simple step is to create and enforce effective password protection, particularly for new employees joining the company.

—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.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m

[2] http://www.justice.gov/opa/pr/joint-statement-attorney-general-loretta-e-lynch-and-secretary-homeland-security-jeh-johnson

[3] https://www.commerce.gov/news/press-releases/2015/11/us-and-chinese-delegations-conclude-26th-session-us-china-joint

[4] 18 U.S.C. § 1030.

[5] No. 14-cv-2737 (BLF), 2015 WL 1289984, at *2 (Mar. 20, 2015).

[6] Id. at 4 (emphasis added).

[7] Id. at 6.

[8] 174 Cal.App.4th 1270 (2009).

[9] Id. at 1282-83.

[10] Id. at 1277.

[11] Id. at 1275, 1286.

[12] Parrish v. Latham & Watkins, 238 Cal.App.4th 81 (2015).

[13] Id. at 102.

[14] Id. at 98-102.

[15] 357 P.3d 769 (Cal. 2015).

[16] https://ustr.gov/about-us/policy-offices/press-office/press-releases/2015/october/summary-trans-pacific-partnership

[17] https://ustr.gov/trade-agreements/free-trade-agreements/trans-pacific-partnership/tpp-full-text

[18] Trans Pacific Partnership Agreement, Art. 18.78.1.

[19] Trans Pacific Partnership Agreement, Art. 18.78.2.

[20] Trans Pacific Partnership Agreement, Art. 18.78.3.

All Content © 2003-2015, Portfolio Media, Inc.