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

5 Trade Secret Trends That Could Shape 2013

Law360, New York (February 14, 2013, 1:29 PM ET) -- The year 2012 brought significant developments in trade secret law. Litigators should consider trends that promise to shape further developments in the upcoming year. We highlight five in particular: (1) the increasing federal power being brought to bear on trade secret law; (2) a deepening circuit split over the interpretation of the Computer Fraud and Abuse Act; (3) increasing litigation involving social media; (4) the necessity of written confidentiality agreements for sophisticated businesses to protect trade secrets; and (5) case law that increasingly demands that plaintiffs identify trade secrets with "reasonable particularity" before obtaining discovery.

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

Increasing Federal Attention to Trade Secret Misappropriation

In the past year, the federal government has increasingly cracked down on the theft of trade secrets, both judicially and legislatively — and that momentum appears poised to carry into 2013.

The year 2012 saw a raft of federal prosecutions under the Economic Espionage Act.[1] Coming on the heels of a government report identifying China and Russia as chief perpetrators in the theft of American trade secrets, the prosecutions demonstrate increasing federal attention to a problem with fascinating global and diplomatic implications. In United States v. Liew, for example, prosecutors indicted four individuals and five corporations in the attempted theft of titanium dioxide processes from DuPont.[2] Prosecutors alleged that the Chinese government controlled one of the corporations and expressly encouraged the thefts. The indictment escalated the growing tensions between the two countries over commercial espionage, a dispute worth watching as 2013 unfolds.

Congress likewise took action in 2012, in response to the Second Circuit's decision in United States v. Aleynikov.[3] In Aleynikov, the Second Circuit overturned the conviction of an engineer who stole source code from Goldman Sachs, holding that the intangible source code — which the defendant did not plan to sell — had not been "produced for" nor "placed in" commerce, as required by the Economic Espionage Act. Congress reacted swiftly, amending the EEA to cover "a product or service used in or intended for use in" interstate commerce. Around the same time, Congress also passed the Foreign and Economic Espionage Penalty Enhancement Act of 2012, H.R. 6029.

The act raises the maximum penalty for thefts benefiting a foreign government from $500,000 to $5 million for individuals; for organizations, Congress imposed the greater of $10 million or three times the value of the trade secret to the offender. These bills signal a widespread congressional consensus to protect corporate trade secrets and might encourage federal prosecutors to target trade secret theft even more aggressively in 2013.

It is also worth monitoring whether Congress returns to legislation that stalled in 2012. Three senators proposed the Protecting American Trade Secrets and Innovation Act of 2012, S. 3389, which would have offered a federal cause of action for trade secret disputes involving a "substantial need for nationwide service of process or misappropriation of trade secrets from the United States to another country." The bill did not advance. But a renewed congressional effort to provide a federal claim for trade secret misappropriation could substantially reshape trade secret law as we know it.

Takeaway

Congress has increasingly sought to protect American trade secrets, and trade secret owners and litigators should carefully monitor any renewed proposals to offer a federal cause of action for trade secret misappropriation and consider enlisting federal assistance when their trade secrets are threatened — particularly by foreign competitors.

For the CFAA's "Exceeds Authorized Access," a Circuit Split Awaiting Resolution

The CFAA provides criminal and civil penalties for an individual who "exceeds authorized access" to a protected computer and thereby steals a company's trade secrets.[4] In 2012, two federal Circuits ruled that "exceeds authorized access" does not cover employees authorized to access the information but who then use it contrary to employer restrictions. The two cases — one criminal, one civil — deepened an important split in federal law between the Fourth and Ninth Circuits and the Fifth, Seventh and Eleventh Circuits.

In June 2008, the government filed a 20-count indictment against former Korn/Ferry International executive David Nosal, alleging that he violated the CFAA by encouraging Korn/Ferry employees to obtain information from a confidential database that would then be used to start a competing business. Nosal moved to dismiss the indictment, arguing that the employees obtaining the information had not "exceed[ed] authorized access" because the company permitted them to access the information under certain circumstances. The district court agreed and dismissed most of the CFAA counts. A divided Ninth Circuit panel reversed, holding that "an employee accesses a computer in excess of his or her authorization when that access violates the employer's access restrictions."

After granting en banc review, the Ninth Circuit affirmed the district court's dismissal.[5] Although recognizing the competing interpretations offered by the Fifth, Seventh and Eleventh Circuits, the court held that "exceeds authorized access" "is limited to violations of restrictions on access to information, and not restrictions on its use." The court determined that this narrower interpretation best matched the statutory language and a legislative history that evidenced an anti-hacking objective. The broader interpretation posed by other circuits, it reasoned, could criminalize "whole categories of otherwise innocuous behavior" — such as at-work Internet surfing or fibbing in an online-dating profile — that technically violates an employer's or provider's access restrictions.

Less than four months later, the Fourth Circuit likewise endorsed a narrow interpretation of "exceeds authorized access," in WEC Carolina Energy Solutions LLC v. Miller.[6] A civil suit, Miller involved an employee who, before resigning, allegedly downloaded confidential information and used it to lure customers away from his former employer. The Fourth Circuit upheld the district court's dismissal of the suit, agreeing with the Ninth Circuit that "the CFAA fails to provide a remedy for misappropriation of trade secrets or violation of a use policy where authorization has not been rescinded." Although recognizing that its conclusion would likely "disappoint employers hoping for a means to rein in rogue employees," the court pointed aggrieved companies to potential state-law remedies.

Trade secret litigators must now wait for the U.S. Supreme Court to resolve this now-entrenched circuit split. Unfortunately, the upcoming year may not produce that resolution: the United States elected not to seek certiorari in Nosal, and the Supreme Court dismissed the Miller cert petition at the parties' request.

Takeaway

Until the circuit split is resolved, whether an aggrieved company can enforce computer use restrictions under the CFAA's "exceeds authorized access" language likely will depend on the suit's venue and thus the relevant circuit's law.

For Employers, Social Media Accounts Require Written Policies

The ascent of social media has been meteoric. The past year showed signs of trade secret law beginning to catch up to the trend.

One significant case — Christou v. Beatport LLC — involved the popular MySpace platform.[7] A nightclub owner sued a competing company led by a former employee, alleging that the employee had misappropriated trade secrets — such as lists of friends and contact information — contained in a MySpace account. The defendant moved to dismiss. Noting that the issue was one of first impression, the court held that the information could constitute a trade secret under a Tenth Circuit eight-factor test. The court seemed especially swayed by the nonpublic compilation of potential-customer contact information, the effort put forth by plaintiffs to compile the information, and the difficulty necessary to replicate it. Of course, had the Christou plaintiff implemented a careful written policy outlining who owned and controlled the account, such analysis might have been unnecessary.

Two other examples reinforce this point. First, one case involved an employee who created a Twitter account that promoted company services and eventually reached approximately 17,000 followers.[8] After being fired, the employee continued to use the account after changing the Twitter handle, over the company's protests. The parties eventually settled, although — with no governing agreement — the employee was able to keep the disputed account.

Second, 2012 likewise saw a contentious and protracted lawsuit over a former employee's LinkedIn account.[9] The employee sued after the company locked her out of her LinkedIn account and changed the contact information to that of her replacement. The parties have locked horns for well over a year; at the time of publication, trial had occurred but no resolution has been reported. Had a written agreement unambiguously clarified the ownership of the employee's work-related social media accounts, lengthy and expensive litigation might have been precluded in each case.

Takeaway

Companies using social media accounts for marketing purposes should take note: A failure to draft written policies unambiguously defining the ownership and control of the accounts can be costly.

For Sophisticated Companies, "Reasonable" Means "Written"

Two cases in 2012 highlighted the danger sophisticated companies face when they neglect written agreements to protect confidential information.

In March, the Seventh Circuit affirmed summary judgment on a trade secret misappropriation claim in Fail-Safe LLC v. A.O. Smith Corp.[10] While negotiating a joint development product, plaintiff Fail-Safe disclosed to the defendant alleged trade secrets involving technology designed to prevent pool suction entrapment. During the negotiations, Fail-Safe signed the defendant's confidentiality agreement but never obtained a return promise from the defendant or otherwise designated its disclosures as confidential.

After negotiations stalled and the defendant began marketing two anti-entrapment devices, Fail-Safe sued. The district court granted summary judgment, and the Seventh Circuit affirmed, holding that Fail-Safe's efforts to protect its confidential information were not "reasonable" under the circumstances. Distinguishing a previous Seventh Circuit opinion, the court reasoned that although small companies have been held "to a looser standard [of reasonableness]," Fail-Safe was "a sophisticated party familiar with [confidentiality] agreements." Further, even if the parties' relationship had "hinted at confidentiality," Fail-Safe acted unreasonably in failing "to take any steps to maintain [] secrecy."

This point was reinforced in Formfactor Inc. v. Micro-Probe Inc.,[11] a case involving a familiar scenario — a lawsuit over an employee who leaves a company to work for its competitor. A Northern District of California court granted summary judgment on the company's trade secret misappropriation claim, holding that, among other grounds, the company had failed to take "reasonable efforts to protect the secrecy of any particular trade secret." Specifically, the company (1) entered no written confidentiality agreement with the employee; (2) authorized the employee to access alleged trade secrets from home using personal email and external hard drives; and (3) did not require the employee to return confidential data upon resigning. In light of these actions, the company could not plausibly claim that its information constituted trade "secrets."

Takeaway

Sophisticated companies that do not obtain written confidentiality agreements from companies or employees receiving confidential information should not expect that a court will protect them from the consequences.

No Reasonable Particularity, No Discovery

The California Code of Civil Procedure requires trade secret plaintiffs to identify their alleged trade secrets with "reasonable particularity" before obtaining discovery.[12] No other state demands "reasonable particularity" as a matter of statute. But in the past year, courts outside California have reiterated that, for plaintiffs, no "reasonable particularity" means "no discovery."

In Switch Communications Group v. Ballard,[13] a magistrate judge in the District of Nevada held that the plaintiff had identified its alleged trade secrets too generally, thus failing to trigger the defendant's duty to respond to discovery. Notably, the court carefully laid out the policy reasons for demanding early "reasonable particularity": without it, (1) plaintiffs could file lawsuits as "fishing expeditions" aimed at discovering defendants' trade secrets; (2) courts could not discern whether the information sought is relevant; (3) a defendant would be hard-pressed to mount a defense; (4) plaintiffs could simply shape their case around the information they receive.

Indeed, a New York state court touched on each of those factors in MSCI Inc. v. Jacob,[14] precluding further discovery and holding that plaintiff could not satisfy the "reasonable particularity" standard simply "by identifying those components not claimed to be trade secrets." Finally, in AAR Manufacturing Inc. v. Matrix Composites Inc.,[15] the Florida District Court of Appeal reiterated that Florida law likewise demands "reasonable particularity" before discovery, although it held that the plaintiff had met that standard.

Takeaway

Even outside California, courts increasingly hold that identifying trade secrets with "reasonable particularity" is a prerequisite to further discovery. Trade secret plaintiffs — and defendants — should take note.

--By Randall E. Kahnke, Kerry L. Bundy and Peter C. Magnuson, Faegre Baker Daniels LLP

Randall Kahnke and Kerry Bundy are partners and Peter Magnuson is an associate in Faegre Baker Daniels' Minneapolis office.

[1] 18 U.S.C. § 1832.

[2] No. 3:11-cr-00573 (N.D. Cal.).

[3] 636 F.3d 71 (2nd Cir. 2012).

[4] 18 U.S.C. § 1030(a)(4).

[5] United States v. Nosal, 676 F.3d 854 (9th Cir. 2012).

[6] 687 F.3d 199 (4th Cir. 2012).

[7] 849 F. Supp. 2d 1055 (D. Colo. 2012).

[8] PhoneDog v. Kravitz, No. C 11-03474 MEJ (N.D. Cal.).

[9] Eagle v. Morgan, No. 2:11-cv-4303 (E.D. Pa.).

[10] 674 F.3d 889 (7th Cir. 2012).

[11] No. C 10-3095 PJH, (N.D. Cal., June 7, 2012).

[12] Cal. Code Civ. Pro. 2019.210.

[13] No. 2:11-CV-00285-KJD, (D. Nev. June 19, 2012).

[14] 945 N.Y.S.2d 863, 866 (Sup. Ct. 2012).

[15] 98 So. 3d 186, 188 (Fla. Dist. Ct. App. 2012).