LAW360

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

Top 10 Trade Secrets Developments Of 2014: Part 2

Law360, New York (January 21, 2015, 10:31 AM ET) --

The year 2014 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.

Randy Kahnke

In part 1 of this two-part series, we highlighted five in particular: (1) the growing importance of specifically identifying trade secrets early in litigation; (2) increasing support for passage of a federal civil trade secret law; (3) the developing saga of the Bratz case and importance of perseverance; (4) the need to protect trade secrets during litigation, and the potential consequences of not doing so (i.e., the DuPont reversal); and (5) the continuing trend toward large damages awards and settlements in trade secrets cases.

In part 2, we highlight five more: (6) the further development of trade secret protections abroad; (7) the narrowing of patentable subject matter for software and the alternative of trade secret protection; (8) the risks and rewards of referring trade secret thefts for criminal prosecution; (9) battles over disclosure of fracking trade secrets; and (10) the potential qualification of social media contacts as trade secrets.

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

6. Trade Secret Protection Continues to Take Hold Abroad

Trade secret protection is gaining ground not only at the federal level in the United States (see part 1 of this series) but also abroad. In particular, the European Union is getting closer to enacting a new legal framework that would harmonize trade secret laws across member states. The EU published its first draft proposal for a directive on the protection of trade secrets in November 2013, and in May of 2014, the Council of the European Union agreed on a set of revisions to that directive, which will now be negotiated by the European Parliament and the Council in early 2015.

Unlike European regulations, directives do not apply directly to member states. Instead, they specify objectives that the member states must achieve through legislation or other means within a certain period of time. If adopted, member states will have another two years to implement the protocols, and

that implementation will result in consistent — but not necessarily uniform — protections across the EU. Importantly, however, the directive provides a uniform (and familiar) definition of trade secret: information that (1) is not generally known among or readily accessible to persons who deal with the kind of information in question; (2) has commercial value because of its secrecy; and (iii) has been subject to reasonable steps to keep it secret.

Europe is not alone in seeking to strengthen protections for trade secrets. Japanese lawmakers are debating reforms to strengthen their country's civil and criminal enforcement of trade secrets. On Sept. 30, 2014, Japan's Ministry of Economy, Trade and Industry kicked off a formal initiative to improve trade secret enforcement and to propose new legislation sometime in 2015.

Russia is also strengthening protections with amendments to its trade secret law that took effect in October 2014. Under those amendments, employees who wrongfully disclose their employer's trade secrets must reimburse their employer for any losses that it incurs as a result of the disclosure. This applies both to current and former employees. The Russian law is particularly tough on CEOs, though, who must reimburse their current or former employer not only for actual losses but also lost profits that result from the wrongful disclosure.

Takeaway

Countries around the globe are strengthening protections for trade secrets, which is good news for companies that have significant foreign operations and manufacturing facilities.

7. Software Patentability After Alice and the Trade Secret Alternative

The narrowing of patentable subject matter has changed the landscape for intellectual property protection in the software world. The U.S. Supreme Court's decision in Alice Corp. v. CLS Bank International has made it substantially more difficult to obtain a software patent.[1] The Alice court held that software patent applications must set forth "an inventive concept" beyond computer implementation of an abstract idea. In the wake of Alice, the Federal Circuit and district courts around the country have invalidated numerous software patents because they lacked "an inventive concept."[2] This trend has understandably caused software innovators to reevaluate their approach to protecting intellectual property and to revisit the benefits of trade secrecy.

While the world of patentable subject matter shrinks, the world of trade secret protection may be expanding. In May of 2014, the California Court of Appeal held in Altavion Inc. v. Konica Minolta Sys. Lab. Inc., that general ideas, including combinations of ideas, are protectable as trade secrets.[3] The case involved Altavion's digital stamping technology ("DST"), which enables digital and paper documents to be self-authenticated using bar codes that are encoded with the content of an original document. Konica Minolta Systems Laboratory ("KMSL") was interested in incorporating DST technology into its line of multifunction printers, and the parties signed an nondisclosure agreement during negotiations over a possible licensing agreement. After those negotiations broke down, Altavion discovered that KMSL had applied for patents that included multiple aspects of DST. Altavion sued KMSL in November 2007, for — among other things — trade secret misappropriation.

On appeal, the principal question before the court was whether general ideas and concepts are protectable trade secrets, and KMSL argued that "generalized ideas and inventions are protectable by patents and thus cannot be trade secrets." The California Court of Appeal disagreed. It explained that an overlap exists between trade secret and patent law, and ultimately held that "it is clear that if a

patentable idea is kept secret, the idea itself can constitute information protectable by trade secret law."[4] The court also reiterated the protected status of "compilation" trade secrets, holding that even though certain elements of Altavion's software design concepts were in the public domain, the particular combination of those elements was not public and was a protectable trade secret.

Takeaway

Software innovators may find that maintaining their intellectual property as trade secrets is preferable to seeking a patent in a post-Alice world.

8. The Risks and Rewards of Referring Trade Secret Thefts for Criminal Prosecution

A trend is developing toward referring instances of trade secret theft to the government for criminal prosecution. In U.S. v. Nosal, David Nosal, a former employee of Korn/Ferry International, was convicted of various crimes including violation of the Computer Fraud and Abuse Act and ordered to pay Korn/Ferry $827,983.25 in restitution.[5]
The criminal case against Nosal, a former executive recruiter for Korn/Ferry, concerned the unauthorized downloading of large numbers of "source lists," (i.e., lists of candidates to be used when filling positions at particular client companies) and other proprietary information.[6]

After conducting a forensic audit, Korn/Ferry and its outside counsel referred the case to the federal government for investigation. In April 24, 2013, a federal jury convicted Nosal of three counts of computer fraud in violation of CFAA, two counts of unauthorized downloading, copying, and duplicating of trade secrets without authorization, in violation of the Economic Espionage Act, and one count of conspiracy to violate the EEA. On Jan. 8, 2014, Nosal was sentenced to one year and one day in prison, assessed a $60,000 fine, and ordered to pay restitution to his former employer under the Mandatory Victims Restitution Act.

In a May 20, 2014, order, U.S. District Judge Edward Chen quantified the restitution award at $827,983.25. The restitution award included $27,400 for costs Korn/Ferry incurred responding to Nosal's actions, $204,825 representing the value of Korn/Ferry's employees' time spent participating in and assisting the government's investigation and prosecution, and $595,758.25 in attorneys' fees incurred by Korn/Ferry in aid of the government's investigation and prosecution. The district court rejected Nosal's arguments that a corporation's costs incurred while investigating criminal activity and assisting the government's prosecution were ineligible for restitution, although it reduced the government's request for $946,929.65 to exclude unnecessary work and to account for staffing inefficiencies.

In some cases, victims of trade secret misappropriation may view the traditional response — a civil lawsuit seeking damages and injunctive relief — as inadequate or unduly costly and burdensome. In some cases, referring the case to the criminal authorities provides an alternative, which provides a host of advantages, including the government's ability to obtain otherwise unavailable evidence. Prosecution may also minimize the trade secret theft victim's attorneys' fees and allow for the recovery of those attorneys' fees without needing to prove that the misappropriation was malicious.[7] And the federal government has publicly declared its interest in partnering with private corporations to investigate and prosecute trade secret theft.[8] On the other hand, referring a case for prosecution involves surrendering a tremendous amount of control, and a criminal prosecution involves a higher burden of proof than a civil lawsuit.

Takeaway

Referring trade secret theft for criminal prosecution provides an alternative to civil litigation. But victims of trade secret theft should carefully consider the costs and benefits before taking it.

9. Battles Over Disclosure of Fracking Trade Secrets

A trend is also developing toward increased protections against public disclosure of fracking trade secrets. In 2014, North Carolina joined several other states that have enacted legislative provisions protecting the confidential information that fracking companies are required to submit to the state.[9]

The passage of the Energy Policy Act in 2005 ended most federal regulation of fracking.[10] Since then, several states have stepped into the vacuum and enacted regulations that create disclosure obligations on oil and gas companies that engage in frac sand mining.[11] The disclosure obligations vary from state to state, but some call for the disclosure of proprietary or trade secret information. For instance, the Illinois Hydraulic Fracturing Regulatory Act requires disclosure of detailed information regarding all chemicals used in the fracking process, including "the anticipated concentration in the base fluid, in percent by mass, of each chemical to be intentionally added to the base fluid."[12]

Given the public interest in fracking, it is unsurprising that a number of requests for this type of information have been filed under various states' analog to the federal Freedom of Information Act. In response, several states have enacted statutory protections to prevent the disclosure of proprietary fracking-related information required to be disclosed to the state. Recently, North Carolina joined those states by passing its Energy Modernization Act.[13] North Carolina's statute presumes that fracking information is nonconfidential and discoverable, but allows fracking companies to make an affirmative showing that fracking information qualifies as a trade secret. North Carolina is notable for creating civil and criminal penalties for wrongful disclosure of confidential fracking information.

2014 also saw the issue of the public's right to discover technical information about the fracking process reach one state's highest court. In Powder River Basin Resource Council v. Wyoming Oil and Gas Conservation Com'n, the Wyoming Supreme Court considered the decision by the Supervisor of the state's Oil and Gas Conservation Commission denying a request for public records documenting the identities of chemicals used in fracking operations in the state.[14] The Wyoming Supreme Court adopted the definition of trade secret articulated by federal courts interpreting the federal Freedom of Information Act, but ultimately determined that it could not conclude on the record before it whether the individual ingredients of a hydraulic fracturing formula could constitute a trade secret.

Takeaway

In the absence of uniform federal regulation, the states will likely continue to develop varied and inconsistent regulatory regimes for fracking. Freedom-of-information requests for fracking information may spur courts to develop or revisit the law regarding the public's right to discover proprietary or trade secret information.

10. LinkedIn Contacts As Trade Secrets

Litigation surrounding the intersection of social media and trade secrets continues. A recent case from the Central District of California suggests that LinkedIn contacts may qualify as protectable trade secrets. Cellular Accessories for Less Inc. v. Trinitas LLC involved a former sales manager of Cellular Accessories,

David Oakes, who decided to start a competing business.[15] While employed by Cellular Accessories, Oakes signed an employment agreement providing that proprietary information — including the company's "customer base" — would remain the property of the company and could not be taken off premises. Oakes also signed a confidentiality agreement prohibiting him from knowingly disclosing or using Cellular Accessories' proprietary information.

When Oakes resigned to start a competing business, he emailed himself a large number of personal and business contacts, as well as supplier, billing, and pricing information. Cellular Accessories sued. Among its allegations, Cellular Accessories claimed that Oakes misappropriated its trade secrets by maintaining his LinkedIn contacts after termination.

On summary judgment, defendants argued that LinkedIn connections cannot qualify as trade secrets under the California Uniform Trade Secrets Act because they were readily observable by all of Oakes' other connections on LinkedIn. In addition, defendants argued that the list could easily be recreated using online business directories. Finally, defendants argued that Cellular Accessories allowed its employees to disclose the identities of other clients in an effort to attract new business and never instructed employees that their LinkedIn contacts were in any way proprietary or confidential information. In response, Cellular Accessories noted that LinkedIn contacts are viewable only to the extent that the user chooses to make them public. Further, even if a customer appeared on a salesperson's contact list, Cellular Accessories argued, the observer would not know whether the contact was actually a customer or some other contact of the salesperson.

The court refused to take judicial notice of LinkedIn's functionality and stated that the parties "did not make sufficiently clear whether and to what degree Oakes' contacts were indeed made public (and whether this was done with [Cellular's] explicit or implicit permission)."[16] As such, the court found genuine issues of material fact as to trade secret misappropriation in relation to Oakes' LinkedIn contacts, leaving a jury to decide the issue absent a negotiated resolution.

Takeaway

If companies hope to maintain ownership and control over their employees' social media accounts, they need to consider developing guidelines for social media use and consider stating that such information qualifies as the company's confidential or proprietary information.

—By Randall E. Kahnke, Kerry L. Bundy, Tyler A. Young and Ryan J. Long, Faegre Baker Daniels LLP

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

[1] 134 S. Ct. 2347 (2014).

[2] See e.g., Buysafe Inc. v. Google, No. 2012-1575 (Fed. Cir. Sept. 3, 2014); Loyalty Conversion Sys. V. American Airlines, Inc., No. 13-CV-655 (E.D. Tex. Sept. 2, 2014).

[3] No. A134343, 2014 (Cal. Ct. App., May 8, 2014).

[4] Id.

[5] No. CR-08-0237 EMC, (N.D. Cal. May 20, 2014).

[6] No. CR-08-0237 EMC, (N.D. Cal. Jan. 13, 2014).

[7] See, e.g., Unif. Trade Secrets Act § 4, 14 U.L.A. 619 (1985).

[8] http://www.fbi.gov/news/testimony/combating-economic-espionage-and-trade-secret-theft.

[9] 2014-4 N.C. Sess. Laws 9.

[10] 42 U.S.C. §300h(d)(1)(B)(ii).

[11] See Matthew McFeeley, Falling through the Cracks: Public Information and the Patchwork of Hydraulic Fracturing Disclosure Laws, 38 Vt. L. Rev. 849 (2014).

[12] 225 Ill. Comp. Stat. Ann.732/§§1-35(b)(8) (2014).

[13] See note v, supra.

[14] 320 P.3d 222 (Wyo. 2014).

[15] CV 12-06736, (C.D. Cal. Sept. 16, 2014).

[16] Id.
