CHICAGOLAWBULLETIN.COM

Serving Chicago's legal community for 157 years

FRIDAY, APRIL 27, 2012

Chicago Daily Law Bulletin

Volume 158, No. 83

Trade secret protection finally moves center stage

Cyberspace has proven surprisingly vulnerable to attack. Even the Chinese government, al-Qaida and Citigroup have seen their websites taken down in recent weeks. As the battle for cyberspace heats up, the vulnerability of cyber information has moved to the center of national intellectual property strategies. In the just-released 2011 Report on Intellectual Property Enforcement by the U.S. intellectual property enforcement coordinator (colloquially called "the IP czar"), enhanced trade secret protection was listed among the U.S. government's priorities. Yet both domestic and international enforcement remain woefully outdated.

Trade secrets may be among the longest-lived forms of intellectual property internationally. Even Filippo Brunelleschi, when he was supervising the construction of the Duomo in Florence, Italy, in the 15th century, relied on trade secrets to protect his new engineering system for building a dome without centering the scaffolding. Like the formula for Coca-Cola, another famous trade secret, Brunelleschi's genius on this one point has remained largely undiscovered. Yet despite its long existence and practical utility, confidential commercial information was not protected internationally until the late 20th century. Despite early treaties such as the Paris Convention for the Protection of Industrial Property which in 1925 prohibited acts "contrary to honest commercial practices," international standards for trade secret protection only came into their own with the enactment of the Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS) in 1994.

Under Article 39(2) of TRIPS, "undisclosed information" whose secrecy the holder has protected using "reasonable steps under the circumstances," and which "has commercial value because it is secret," is required to be protected against "being disclosed, acquired by or used by others without ... consent in a manner contrary to honest commercial practices." While every government protects secret governmental information, protection of secret commercial information has been a relatively hard sell internationally. TRIPS is largely perceived as promoting patent protection for innovation because it rewards disclosure. Trade secrets, by valuing secrecy, are a direct contradiction of this policy.

TRIPS requires all signatories to provide civil enforcement for trade secrets, including ex parte injunctive relief. It even requires the issuance of protective orders to maintain confidentiality under Article 42 "unless this would be contrary to existing constitutional requirements." In countries that lack a long history of trade secret protection, however, protective orders are either nonexistent or generally unenforceable. Most countries do not provide judges with contempt power, merely the ability to impose (often minimal) civil fines. In countries like China, preliminary injunctive relief is usually unavailable since trade secrets are considered an issue of unfair competition requiring detailed examinations to determine likely success.

The creation of "innovation strategies" by many rapidly developing countries, including China and India, has further undermined trade secret protection internationally. As countries focus on the encouragement of "indigenous innovation" and "technology transfer" to develop local industry, trade secret protection becomes even more problematic. Trade secret misappropriation is one of the most underreported IP violations because companies do not want to admit that they have lost control of their valuable know-how. Yet even with such underreporting, according to the IP czar, "[T]he pace of foreign economic collection of information and industrial espionage activities against major U.S. companies is accelerating." Of the seven cases brought under the U.S. Economic Espionage Act (EEA) in 2010 by the Department of Justice, six involved theft of information that was passed, or attempted to be passed, to Chinese companies. These efforts were not focused on a particular industry but involved trade secrets in increasingly diverse areas, including the automotive, hazardous waste management, mobile telecommunications and pesticides industries.

GLOBAL IP

DORIS ESTELLE LONG

Doris Estelle Long is a law professor and chairwoman of the intellectual property, information technology and privacy group at The John Marshall Law School. She has served as a consultant on IPR issues for diverse U.S. and foreign government agencies, including as attorney adviser in the Office of Legislative and International Affairs of the USPTO. She can be reached at 7long@jmls.edu.

While most firms focus on enhanced security measures to prevent unauthorized disclosures, cyberspace teaches that all technology provides only relative security. As companies move more research and development activities offshore, security breaches may become even more difficult to prevent. Fortunately, increased need may finally be giving rise to better protection. Although the much-maligned Stop Online Piracy Act (SOPA) has been put on hold, it is likely that the provisions providing for enhanced criminal penalties for trade secret theft under the EEA will be treated separately. These provisions increase prison terms to 20 years and monetary fines to $5 million. They also provide for sentencing enhancement for any effort to transmit a stolen trade secret outside of the United States.

> ***"Trade secret misappropriation is one of the most underreported IP violations because companies do not want to admit that they have lost control of their valuable know-how."***

Recent enforcement activities before the International Trade Commission (ITC) also give trade secret owners greater tools to remove the value of trade secret misappropriation from foreign actors.

Even companies that only use or license their trade secrets in the United States may well find their information stolen and transferred to foreign competitors. With international protection so difficult, the EEA needs to be strengthened now. In addition to enhanced penalties for attempted foreign transfers of U.S. trade secrets, the definition of protected trade secrets should be expanded to plainly cover the theft of proprietary source code, prototypes and other business assets regardless of whether they have been placed in the marketplace. Such an extension would avoid the recent anomalous result in *U.S. v. Aleynikov*, where the 2nd U.S. Circuit Court of Appeals found that the unauthorized electronic transfer to Germany of the proprietary source code used in Goldman Sach's high-frequency trading system did not qualify for criminal prosecution because the source code itself was not placed into interstate commerce by its owner. Enhanced trade secret protection should be part of future trade negotiations, including the proposed TransPacific Partnership. Finally, trade secret owners need to start aggressively prosecuting thefts. With the current focus on cybersecurity, they will surely find a more willing audience for their complaints.