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

Trade Secrets: Potential New Laws — And New Risks

Law360, New York (February 25, 2014, 12:38 PM ET) -- Trade secret theft has become a high-profile issue for the U.S. government, and the last year has seen a flurry of trade secret-related legislation being proposed by Congress. Some of these bills focus on modifying causes of action. For example, the Private Right of Action Against Theft of Trade Secrets Act of 2013 would allow anyone who suffers injury as a result of a violation of the Economic Espionage Act to seek damages, adding a civil cause of action to the existing criminal law. That would give companies a new arrow in the quiver in the fight against trade secret theft.

Another proposed bill — Aaron's Law Act of 2013 — attempts to resolve a split in the circuit courts over the interpretation of the Computer Fraud and Abuse Act's prohibition of unauthorized access to computers. Several courts have interpreted unauthorized access broadly to mean a violation of company policies, while others have taken a narrower view that says it means circumventing a physical or electronic barrier. Aaron's Law would write that view into the statutes.

Other proposed bills target cybertheft by foreign entities. The Cyber Economic Espionage Accountability Act would create immigration and financial penalties for foreign individuals who engage in cyberespionage. It would require the president to draw up a list of foreign officials and agents who are engaged in cyberespionage, making them ineligible for a U.S. visa and putting them at risk of having their U.S. assets frozen.

The Deter Cyber Theft Act would take a similar approach at a higher level, requiring the director of National Intelligence to compile a list of countries engaged in cyberespionage and the U.S. intellectual property being misappropriated or targeted by foreign entities. The worst offenders would be designated "priority foreign countries." The bill creates a two-tiered system of import restrictions: prohibiting foreign articles containing technology and proprietary information misappropriated from the U.S. from entering the country, and banning articles "purchased or exported" by an entity owned or controlled by a "priority foreign country" if the articles are the same or similar to articles produced using technologies or IP targeted in the U.S. by cyberespionage. It would not be necessary to show that stolen trade secrets are involved, just that the IP has been targeted by cyberespionage.

Finally, the U.S. Attorney's office is increasingly willing to work with U.S. companies to pursue foreign trade thieves, and Congress has weighed in with a proposed bill called "Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology" or SECURE IT. Among other things, this bill facilitates sharing cyberthreat information and ratchets up penalties for violations of existing trade secret law under CFAA. The purpose of the bill fits with the idea that government and business should be more collaborative in protecting against trade secret theft by foreign governments or entities.

Technology Makes It Complicated

While the legislative wheels turn, evolving technology makes the protection of trade secrets more complex. The proliferation of portable data-storing devices makes it easy to steal information and difficult for companies to prevent that theft. This will likely create a focus on what constitutes reasonable measures to protect secrets.

The rise of social media is changing the trade secret landscape, and the law is trying to catch up — often, in court. There is a trend of costly litigation involving the use of social media accounts for marketing purposes and contesting who owns the account and the information it contains.

Social media is widely used in business, and employees often mix their personal and business activities. This behavior raises a range of issues. For example, are lists of friends and contact information contained on a MySpace account a trade secret of the MySpace user's company? At least one district court has held these lists can be trade secrets of the employer, because the effort and expense in connecting with potential customers made that information a protectable trade secret.

But not all courts agree. In Eagle v. Morgan, the CEO of a company called Edcomm Inc. had opened a LinkedIn account and used it to promote the company and build social and professional relationships. After the CEO left, the company cut off her access to the LinkedIn page, but she regained access a few weeks later. In the ensuing litigation, the company said that the CEO had taken its trade secrets — the names and contacts on the LinkedIn page. The court determined, however, that this wasn't a trade secret because it was readily ascertainable by the business community and publicly known.

With these types of gray-area issues in play, companies need to pay closer attention to upfront prevention through nondisclosure and assignment of rights agreements that take social media into account and when possible, keep employee and personal social media accounts separate.

Trade Secret Preemption: Gaining Steam

The Uniform Trade Secrets Act provides a cause of action for trade secret theft. But it also creates an often-used way to try to avoid tort claims related to the UTSA claim, because many courts say the UTSA provides a statutory remedy in such cases, and that it preempts any tort claims.

Now, however, there is a question about whether tort claims involving the theft of confidential information — that is, important information that falls short of being a trade secret — would be subject to UTSA preemption. In California and many other states, the answer to that question is "yes," although a minority of courts have disagreed, saying that you should be able to proceed with tort litigation in such cases. But many federal courts have yet to consider the issue, and for those that have, the rulings are not uniform. Over time, it is expected that most courts will follow California's lead in finding that the UTSA preempts tort claims based on misappropriation of confidential information.

Trade secrets theft often involves insiders with access to key data, a threat that is particularly difficult to counter due to mobile technologies that make it easy to capture company information.

Key Cases to Consider

Christou v. Beatport (D. Colo.)

The court in this case ruled that MySpace friend lists were trade secrets. Although the names could be found in public directories, the court said that the contact information connected to those names had been properly password-protected, involved a cost to develop, and included information that was not publicly available.

Phonedog v. Kravitz

A website sued a former employee, saying that he had taken trade secrets when he left the company with a Twitter account that he had maintained for the company while employed there. The Northern District of California court refused to dismiss the case, saying that Twitter accounts and passwords could

be trade secrets.

—By Mark A. Romeo, Crowell & Moring LLP

Mark Romeo is a partner and trial lawyer in Crowell & Moring's labor and employment and litigation groups in Orange County, Calif., and is a member of the firm's trade secrets working group.

This article was adapted from the firm's "Litigation Forecast 2014."