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

Recent Trade Secret Reform — And What Else Needs To Change

Law360, New York (September 23, 2013, 11:24 AM ET) -- Earlier this year, U.S. Attorney General Eric Holder warned of the "devastating harm" that trade secret theft poses to American innovation. "There are only two categories of companies affected by trade secret theft," he said. "Those that know they've been compromised — and those that don't know it yet."

President Obama sounded a similar alarm in his 2013 State of the Union address. "We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy," the president said.

The administration is not alone in its newfound focus on trade secret theft. Congress is passing trade secret laws and considering bills with unseen intensity. And more state legislatures have passed comprehensive trade secret statutes.

Despite these efforts, two shortcomings in the nation's trade secret strategy continue to stand out. First, Congress has not enacted a federal civil trade secret statute, deferring instead to a state-by-state patchwork of civil remedies. Second, two states, New York and Massachusetts, have yet to adopt the Uniform Trade Secrets Act.

This article examines the recent changes to trade secret law and describes the work still to be done.

Recent Federal Trade Secret Legislation

Twice in the past year Congress has amended the Economic Espionage Act, the 1996 statute that made theft of trade secrets a federal crime.

The first amendment, the Theft of Trade Secrets Clarification Act of 2012, was enacted last December. It was a response to United States v. Aleynikov, 676 F.3d 71 (2d Cir. 2012), which involved a Goldman Sachs programmer, Sergey Aleynikov, who, before being wooed away by a competitor, took half a million lines of source code.

Prosecutors argued that the code was proprietary, a complex computer algorithm that could adversely affect Goldman's market share if misused. A district court jury agreed, and Aleynikov was sentenced to eight years in prison. But the Second Circuit reversed, holding that the stolen code was "purely intangible property" and not, as then required by the EEA, a trade secret "that is related to or included in a product that is produced for or placed in interstate or foreign commerce."

Ten months after Aleynikov's acquittal, Congress changed that text. Specifically, Congress softened the requirement that the product must be "produced for or placed in" interstate

or foreign commerce. Now the statute requires only that the product be "used in or intended for use in" interstate or foreign commerce. Congress further expanded the EEA to include both products and "services."

The second amendment, the Foreign and Economic Espionage Penalty Enhancement Act of 2012, came in January 2013. For violations of certain parts of the EEA, Congress raised the penalties for individuals tenfold, from $500,000 to $5 million. And for organizations, Congress increased the penalties from $10 million to the greater of $10 million or "3 times the value" of the stolen trade secret. The "3 times the value" language could result in massive payouts: Under the revised statute, "value" encompasses "expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided."

Congress has not stopped there. Lawmakers in recent months have proposed additional legislation aimed at further strengthening the EEA.

In July 2013, Sens. Sheldon Whitehouse, D-R.I., and Lindsey Graham, R-S.C., proposed a draft bill that would expand the EEA to expressly cover trade secret theft sponsored by foreign governments as well as trade secrets taken at a foreign government's behest. The bill would also clarify that the EEA applies to a hacker whose code passes through domestic computers but who is never physically present in the United States. And the bill would add trade secret theft as a predicate act for a Racketeering Influenced Corrupt Organizations Act claim. A hearing is expected this fall.

In June 2013, Rep. Mike Rogers, R-Mich., and others proposed the Cyber Economic Espionage Accountability Act. It calls for the U.S. Department of Justice to bring more economic espionage cases against foreign actors. It would also permit government officials to revoke the visas and freeze the financial assets of foreign agents who participate in cyber crimes. The bill remains in committees in the House and Senate.

And in May 2013, Sen. Carl Levin, D-Mich., and others introduced the Deter Cyber Theft Act. It would create, among other things, a watch list of countries that engage in economic espionage against U.S. companies or individuals. It remains in the Senate Committee on Finance.

In addition to bolstering the criminal rules, Congress has ventured into the important realm of trade secret civil actions.

In July 2012, Sens. Whitehouse, Chris Coons, D-Del., and Herb Kohl (the now-retired Democrat from Wisconsin) introduced a bill that would have grafted a federal right of civil action for trade secret theft onto the EEA. Sadly, the bill, known as PATSIA (Protecting American Trade Secrets and Innovation Act of 2012), died in the Senate Committee on the Judiciary.

Rep. Zoe Lofgren, the Silicon Valley–based Democrat, tried a different approach in July 2013 with another acronym, PRATSA (Private Right of Action Against Theft of Trade Secrets Act of 2013).

Like PATSIA before it, PRATSA would provide a civil claim for trade secret theft under the EEA. But unlike its predecessor, PRATSA applies to a narrower part of the EEA. It remains in the House Committee on the Judiciary's Subcommittee on Crime, Terrorism, Homeland Security and Investigations.

Recent State Trade Secret Legislation

Each of the 50 states has its own autonomous trade secret law. Nearly all have adopted

some version of the Uniform Trade Secrets Act ("UTSA"), a model statute that gained wide acceptance in the 1980s and 1990s. Only two stragglers remain now that New Jersey and Texas recently codified their trade secret law.

In 2012, New Jersey Gov. Chris Christie signed the New Jersey Trade Secrets Act, NJTSA, replacing the state's common law with a statutory regime.

Like many states late to enact the UTSA, New Jersey tweaked several provisions of the model statute. For example, the NJTSA does not include the UTSA's provision that directs courts to take into account trade secret rulings from other states when deciding cases. The NJTSA also contains weaker language than the UTSA regarding what common law claims are preempted. The NJTSA instead allows certain confidential information that does not qualify for trade secret protection to remain protected.

In May 2013, Texas Gov. Rick Perry followed suit, signing the Texas Uniform Trade Secrets Act, TUTSA. It went into effect in September 2013 and replaced Texas's previous common law regime.

The TUTSA changes Texas law in key ways. It provides a basis for the recovery of attorneys' fees and permits injunctive relief for threatened trade secret theft. It also extends protections to noncontinuous trade secrets. Before the TUTSA, a trade secret plaintiff in Texas had to prove that its trade secrets were used continually. Under the TUTSA, Texas now protects both continuous and noncontinuous trade secrets, such as confidential details about one-time product announcements or so-called "negative trade secrets" about past experiments that failed.

The TUTSA also tweaked the model UTSA. Texas' version adds customer lists and financial data to the definition of a trade secret. And Texas' version specifically provides that information that is readily ascertainable by reverse engineering will generally not qualify for trade secret protection. Most states reach this same result through judicial interpretation, but Texas does so by statute.

With New Jersey and Texas now onboard, 48 states, plus the District of Columbia, Puerto Rico and the U.S. Virgin Islands, have adopted some version of the UTSA.

Remaining Gaps in Trade Secret Legislation

Despite the emergence of trade secret protection on the White House agenda and the flurry of recent legislative activity, conspicuous gaps persist.

Two states, New York and Massachusetts, have yet to enact a version of the Uniform Trade Secrets Act. But that might change soon. Earlier this year, a Massachusetts legislator introduced a bill to enact a version of the UTSA. It remains in committee.

The more problematic gap is at the national level, where the absence of a federal civil trade secret statute has allowed for the inconsistent application of protections crucial to American business. The UTSA is at best a partial fix. As Texas' and New Jersey's recent experiences demonstrate, state legislatures often modify the UTSA. And even if every state had the same UTSA, there would still be a patchwork approach because state courts often issue different interpretations of the same UTSA provisions.

State-by-state differences in trade secret law cost companies and employees, who face uncertainty about which law will apply. And these differences cost courts and litigants, who wage needless battles over forum shopping and choice of law.

Hope thus rests on a federal civil trade secret statute. Preeminent commentators and

respected organizations support a federal approach. The American Bar Association IP Section, for example, endorsed a federal civil cause of action for trade secret theft in April 2013. And in May 2013, the Commission on the Theft of American Intellectual Property, an independent and bipartisan group, recommended that Congress amend the EEA to provide a federal private right of action for trade secret theft.

The need to protect American business from trade secret theft has never been greater. As the attorney general recently warned, "A hacker in China can acquire source code from a software company in Virginia without leaving his or her desk." It is time to fill the gap in recent legislative efforts and enact a federal civil cause of action for trade secret theft.

--By David S. Almeling, O'Melveny & Myers LLP

David Almeling is counsel in O'Melveny's San Francisco office.

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.