CLIENT ALERT

The Latest Attempt to Federalize Trade Secret Law

Aug.13.2012

On July 17, the Protecting American Trade Secrets and Innovation Act of 2012 was introduced in the Senate. If passed, the law would revolutionize the legal regime governing trade secrets by conferring federal jurisdiction under a new federal law over cases in which plaintiff certifies either misappropriation from the United States to another country or that there is a substantial need for nationwide service of process to prosecute the claim. Nearly every major trade secret case, the sponsors say, should meet one or both of these requirements. The act also contains a series of important features that attempt to make it easier for trade secret holders to shut down misappropriations in the early stages and to recover damages.

The act is not the first effort to federalize trade secret law, but there seems to be growing support for the enterprise, and some commentators have suggested that it is only a matter of time. To be sure, there is an increasingly broad consensus that trade secret holders need additional protections beyond the existing legal regime to secure their investments against rogue employees, cyber hackers and over zealous competitors abroad.

Indeed, the act's sponsors — Sens. Herb Kohl, D-Wis., Chris Coons, D-Del., and Sheldon Whitehouse, D-R.I., — have specifically pointed to the internationalization of trade secret theft, which is said to have cost American companies billions and billions of dollars annually, as a principal motivation for the bill.

Trade secret holders and their lawyers need to understand the act, be heard, and be ready to proceed under its provisions.

The Current Regime Governing Trade Secret Protection, And Its Alleged Shortcomings

Unlike the other pillars of intellectual property — patents, copyright and trademarks — trade secret protection is principally a matter of state law. Trade secret protection was a hodgepodge of state common law decisions until the Uniform Trade Secrets Act (UTSA), which was drafted in 1979.

Over the last three decades, the UTSA has been adopted in most states, but not all versions are identical. For example, different state versions of the UTSA have different limitations periods and only some states accept the often important official comments. Moreover, important commercial hubs like New York and Texas never adopted the UTSA and instead retained common law doctrines or enacted other statutes, which are quite different.

Further complicating matters, even where the provisions are identical, the courts of different states have decided common questions differently. For example, some state courts have accepted the inevitable disclosure doctrine, which prohibits employees from moving to a company in a related industry where disclosure of employer secrets may be inevitable, while others have rejected it — while still others have not ruled on the issue. Although it is a uniform law, a UTSA decisions in one state is not binding on courts in another state. All of which has prompted some critics to charge that the UTSA has failed in its fundamental charge of uniformity — to harmonize the law across state lines.

Trade secret cases are often in federal court as well, either based on diversity of citizenship or under the Computer Fraud and Abuse Act (CFAA). Originally passed in 1986, the CFAA as amended creates a federal cause of action stemming from unauthorized access to a computer, including a network or server. Because most business, and therefore trade secret theft, today involves computers, the CFAA is an avenue into federal court for many plaintiffs. But it is not without limits.

For example, the circuits are split on if the CFAA confers federal jurisdiction in the not uncommon situation where otherwise authorized users (e.g., employees) are alleged to have exceeded their authorization by copying and sending electronic files in violation of employment policies. In any event, federal jurisdiction has proven no solution of lack of uniformity. Federal courts are faced with the same challenges of analyzing the patchwork of state laws, and must defer to the state courts of that jurisdiction for binding decisions. Indeed, federal court trade secret decision are not binding on other federal courts, or even on a state court in that jurisdiction.

Lack of uniformity and lack of consistency in application in trade secret law is the primary criticism of the current regime, but it is hardly the only one. Supporters of the act also charge that the current regime has proven ill-suited for the Internet revolution and internationalization of the modern business world.

Back in 1979, when the UTSA was drafted, computer use by individual employees was just beginning, and servers, the Internet, email, network computing, and portable devices were unheard of. Today, no business could operate without them. Thus, a common fact scenario in trade secret cases now involves a user in one jurisdiction, accessing servers in a second jurisdiction, to take data owned by an entity in a third jurisdiction, for the benefit of an entity in a fourth jurisdiction.

The current regime, critics charge, has no clear guidance on which substantive law to apply. Many trade secret cases, therefore, now begin with a high level of uncertainly about which state statutory and decisional law controls. And, often, that question is never fully answered, with a court in one forum conducting parallel analyses under its own and one or more other state laws.

Prosecuting a trade secret case on such facts in state court can also have serious practical challenges. Obtaining subpoenas across states lines for the requisite third-party discovery is expensive and takes time, although successful protection often depends on obtaining immediate relief in the form of an injunction. Otherwise, the thief may be further undermining the secrecy of or commercially exploiting the idea.

All of these challenges are exacerbated when the boundaries are not state lines but international borders. Discovery, even in Hague Convention jurisdictions, is expensive and may take months. The problem is particularly acute when the thieves themselves lack sufficient contacts to confer jurisdiction in the United States and/or lack domestic assets to attach to satisfy a final judgment. Securing a prison term and million-dollar (uncollectable) fine against rogue former employees is little consolation if their sponsors are free to directly compete with the trade secret holder, unburdened by research and development costs.

The Protecting American Trade Secrets and Innovation Act of 2012

The act seeks to amend the Economic Espionage Act (EEA) to create a federal civil remedy for trade secret misappropriation. In 1996, Congress passed the EEA criminalizing trade secret misappropriation (1) with knowledge that doing so will benefit a foreign government or (2) to place a product using that trade secret into interstate commerce with knowledge that doing so will cause injury to the secret holder. EEA prosecutions were rare until a recent spate of high-profile cases were brought against

employees that attempted to transfer high value secrets to foreign companies. Those prosecutions have been perceived as successful in punishing the employees.

Indeed, months ahead of the act, Sen. Kohl introduced legislation to increase the criminal penalties under the EEA that is now under consideration. But it is not at all clear that the EEA has any impact on the sponsors or ultimate beneficiaries of the misappropriation. To the contrary, there is strong evidence that cyber espionage, now an institutional practice on a massive scale in certain parts of the world, has been undeterred. By providing a civil remedy, the act would give trade secret holders an avenue to obtain compensation for their lost sales, as well as other relief.

Some commentators favored a more comprehensive approach to federalization, such as by enacting some federal version of the UTSA and thereby displacing state law. The act does not do this. Rather, the act contains three important limitations on its scope: First, the act only covers trade secrets that are "related to or included in a product," whereas all ideas may be covered under the UTSA and other state law. Second, the act imposes the requirement of intent, which is not an element under the UTSA. Third, the act confers federal jurisdiction only if plaintiff certifies either (1) misappropriation of trade secrets from the United States to another country or (2) a "substantial need" for nationwide service of process.

These limits, sponsors say, will distinguish "major trade secret cases" from more common and local disputes that should continue to be addressed under state law. Thus, the act does not displace any state law (and, indeed, leaves open the possibly that every violation of the act is still also a violation of state law).

How Will The Act, If Passed, Change Trade Secret Litigation?

The act would revolutionize the way covered trade secret cases are litigated in four major ways:

First, and most obviously, those trade secret cases would be brought in federal court under a new law. The act would essentially create a blank slate for disputes to matriculate up through the courts. But, ultimately, with all federal courts interpreting the same law, greater uniformity should be expected in the long term. In the short term, some very high-profile matters on the meaning of the act's key terms that would have broad ramifications should be expected.

Second, the act confers nationwide service of process. This should make third-party information more readily available at less expense, and force many discovery disputes to the court handling the lawsuit. Theoretically, this means a more efficient process.

Third, the act authorizes ex parte seizures for (1) property that is being misappropriated under the act or (2) to preserve evidence on a showing that doing so is necessary to prevent irreparable injury by clear and convincing evidence. The act substantially lowers the high burden usually needed for ex parte orders.

The act further authorizes entry of a protective order to prevent the disclosure of information seized. Trade secret misappropriation in the Internet age has long presented the problem of how to "unring the bell" — i.e., once the information is out, it cannot be put back in. This provision of the act, sponsors say, should allow the trade secret holder to shut down a misappropriation in real time, before the trade secrets becomes publicly available. In order to prevent misuse of this powerful tool, the act requires a hearing, typically, within three days and permits a party injured by an ex parte order obtained in bad faith to recover damages and attorneys' fees.

Fourth, and perhaps most significantly, the act would take a step toward providing civil remedies for international misappropriation. At present, international trade secret cases have a special set of challenges that, critics argue, do not sufficiently protect trade secret holders. Excepting the U.S. International Trade Commission's decision, affirmed by the Federal Circuit, in the *Tian Rui* case allowing *in rem* jurisdiction based on foreign misappropriation, trade secret holders have had little good news against the tide of rogue employee thefts and institutional cyber attacks cost them billions. The act seeks to make pursing those claims easier.

Remedies available under the act include injunctive relief, protective orders, reasonable royalties, damages for actual harm, damages for unjust enrichment, and exemplary damages in malicious cases of up to the amount of single damages. Also, the act empowers federal courts to award fees and costs in such instances and for bad faith tactics. The three-year limitations period runs from time of discovery or when the misappropriation should have been discovery through the exercise of reasonable diligence.

The act has been referred the Senate Committee on the Judiciary. Trade secret holders and practitioners concerned about national and international trade secret misappropriation must follow these developments.

This information was also published as an expert analysis column in Law360.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Mark A. Klapow
Partner – Washington, D.C.
Phone: +1 202.624.2975
Email: mklapow@crowell.com