The Myth of The Trade Secret Troll

November 15, 2015 by James Pooley

Why We Need a Federal Civil Claim for Trade Secret Misappropriation

Guest Post by James Pooley, former Deputy Director General of the World Intellectual Property Organization. Pooley makes his full argument in a forthcoming George Mason Law Review article available here.

Trade secret theft has been a federal crime since 1996, covered by the Economic Espionage Act ("EEA"). But civil misappropriation claims remain limited to state court filings under common law or local variants of the Uniform Trade Secrets Act ("UTSA"). Calls for federal jurisdiction have grown with the increasing importance of information as a business asset and with the emergence of technology that makes theft of these assets almost infinitely easier. Recent examples involving international actors have galvanized the business community to request a straightforward solution: amend the EEA to provide a federal option for private claims.

Several bills were introduced in the 113th Congress to accomplish this, and to authorize provisional remedies for seizure of relevant property to prevent secret technology from being transferred out of the jurisdiction. The 2014 legislation was not acted on before Congress adjourned. A revised version is pending now, the Defend Trade Secrets Act of 2015 ("DTSA"), reflected in identical House (H.R.3326) and Senate (S.1890) bills.

The approach of the DTSA is fairly simple: use existing language of the EEA where appropriate, such as the definition of a trade secret, and where other language is required to define the civil aspects, such as misappropriation and damages, use language taken from the UTSA. Indeed, the only meaningful departure from the UTSA is to add a section allowing ex parte seizures of the misappropriated property. But even that portion draws from established provisions of the Lanham Act, tightened up considerably from the 2014 bills in order to discourage abuse.

The DTSA has received virtually unanimous support from industry, and also enjoys unusually bipartisan political sponsorship, with 65 cosponsors in the House (45 Republican and 20 Democrat) and ten in the Senate (six

Republican and four Democrat). The only organized opposition has come from a group of law professors who published an “open letter” in 2014 criticizing the previous draft legislation, and who have recently released another letter describing their concerns. Mainly, they argue that we don’t need federal legislation because state laws are uniform enough; that the seizure provisions are too broad; and that the DTSA would limit labor mobility by approving the so-called “inevitable disclosure doctrine.”

As I will explain below, on each of these points the professors are wrong, misled by incorrect assumptions or unjustified speculation. Indeed, in a recent journal article two of them have predicted that the legislation would unleash a never-seen-before class of commercial predator, the “trade secret troll,” who they claim would “roam free in a confused and unsettled environment, threatening or initiating lawsuits for the sole purpose of exacting settlement payments, just like patent trolls.”

This apocalyptic scenario is not only fanciful; it is absurd. While patents are exclusive rights that operate against the world, trade secrets provide no exclusivity and depend on a confidential relationship. The image of a “trade secret troll” may help draw attention to a political argument, but it is a myth, and deserves no serious consideration.

The reality of this legislation is simple and compelling. Giving trade secret owners the option to sue in federal court would fill a critical gap in effective enforcement of private rights against cross-border misappropriation that in the digital age has become too stealthy and quick to be dealt with predictably in state courts. The bills would accomplish this by effecting only very modest changes, relying heavily on existing laws and rules. The seizure provisions in particular are so narrowly drawn that only the most clearly aggrieved plaintiffs would risk invoking the procedure. Having no pre-emptive effect, the federal law would leave in place all relevant state laws and policies, including those relating to mobility of labor.

U.S. trade secret law emerged in the nineteenth century to accommodate the shift from agrarian and cottage production to larger-scale industry, in which the secrets of production would have to be shared with workers or with business partners. Court decisions sought to enforce the confidence placed in those who were given access to valuable information about machines, recipes and processes. At the core of every case was a

confidential relationship. Protecting this trust, the courts explained, was a simple matter of enforcing morality in the marketplace.

The common law origins of trade secrets – in contrast to the federal patent statute – meant that the majority of cases were heard in state court. Even when a federal court took diversity or supplemental jurisdiction over a trade secret dispute, it applied the law of the state in which it sat. And at first there was little variation, with most states looking to the Restatement of Torts § 757 as a guide. But as industrial development continued through the middle of the twentieth century, legal foundations shifted, and the reporters of the Second Restatement dropped the subject completely.

Meanwhile, a school of thought had developed among commentators that trade secret law should be abolished altogether because it was inconsistent with, and therefore preempted by, federal patent law. This argument was famously rejected by the U.S. Supreme Court in Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470 (1974). Two important public interests, the Court explained, were served by trade secret law: the "maintenance of standards of commercial ethics and the encouragement of invention." Without guaranteed secrecy, businesses would be left to expensive self-help security measures that would disadvantage smaller competitors and discourage dissemination of information through sharing. And as a practical matter, there was no conflict between the two systems because they operate so differently: patent law is strong, providing an exclusive right "against the world;" while trade secret rights are "far weaker," because they do not protect against reverse engineering or independent development.

With the Second Restatement's decision not to treat the issue, some were concerned that trade secret law would become too fractured and inconsistent for companies which had been increasingly doing business across state lines. Therefore, in 1979 the National Conference of Commissioners on Uniform State Laws issued the first of two versions of the UTSA, proposing harmonized rules on establishing and enforcing trade secret rights. Measured by adoption rates, the UTSA has been a great success, with 47 of the 50 states so far embracing it (New York is the leading holdout). However, measured by its objective of uniformity, the law has been a disappointment. Unlike the UCC, the UTSA has frequently been enacted with customized features.

A few examples will help illustrate the scope of the problem. California dropped the language requiring that a trade secret be not “readily ascertainable,” with the result that the defendant is required to specially plead that circumstance as an affirmative defense. Illinois also eliminated the “readily ascertainable” language, and it prohibits royalty injunction orders, sets a different limitations period and allows permanent injunctions. Idaho requires that computer programs carry a “copyright or other proprietary or confidential marking” to qualify for protection. Georgia limits protection of customer lists to physical embodiments, in effect allowing employees to appropriate such information in (human) memory. South Carolina’s version of the UTSA requires a court hearing an injunction request to consider “average rate of business growth” in determining a head start period, and prescribes very particular rules for discovery of trade secret information, even for local discovery in aid of an action pending in another jurisdiction.

When Congress considered the EEA in 1996, there was some discussion of adding a civil right of action, but this was deemed impractical in view of the need for swift legislative action. In the years since its enactment, the EEA has had a mixed record of success. As reported by one veteran prosecutor, the average of about eight prosecutions per year is a “languid pace” that probably has done little to create a deterrent effect. In part this may be due to a reluctance of victims to bring cases to the prosecutor, either because of a loss of control or Fifth Amendment effects on civil claims, or it may be due to a lack of resources or interest within the various offices of the U.S. Attorneys, who have discretion whether to accept qualifying cases.

Calls for a federal trade secret law with a private right of action had already begun before the EEA was passed. After it became law, a number of scholars noted the anomaly and suggested that, because the national economy had become primarily knowledge-based, and because even with the UTSA state law was far from uniform, a federal civil law should be enacted. More recent commentary, while continuing to emphasize the drawbacks of variations in state law, also has pointed out the economic advantages of federalization, particularly for small businesses, which rely more heavily on secrecy than on patenting, as well as the procedural advantages for trade secret owners, including national service of process.

The highly-publicized cyberattacks of recent years have exposed not only the precarious security of personal financial and health information, but also the vulnerability of American corporate secrets. Thirty years ago information security consisted mainly of guarding the photocopier and watching who went in and out the front door. Now, with the Internet connected to millions of smartphones, and with electronic storage devices the size of a coin, information assets (which account for over 80% of the value of U.S. public companies) can be moved quickly and silently across state and international borders. In that context, existing procedures at the state level seem impossibly quaint. If a case in Illinois requires testimony of a witness in California, the plaintiff has to petition its home court to authorize a deposition, and then file an action in California based on the Illinois order, to secure the required subpoena. During the weeks or months of this process, the witness could easily have left the country, with the secrets in her pocket.

In other words, the time-critical nature of interstate and international misappropriation of valuable digitized data requires an immediate and sophisticated response mechanism, and neither state law nor the EEA criminal framework provides a satisfactory solution. Federal courts, however, can provide the necessary resource. First, they will be operating under a single, national standard for trade secret misappropriation and a transparent set of procedural rules, offering predictability and ease of use. Second, they will provide nationwide service of process and a unified approach to discovery, enabling quick action by trade secret owners even when confronted with actors in multiple jurisdictions. Third, as a result of their extensive experience with complex cross-border litigation involving intellectual property, they will be able to resolve ex parte matters fairly and jurisdictional issues quickly and efficiently. Fourth, their generally more predictable discovery procedures will serve the legitimate needs of trade secret plaintiffs, who typically must develop most of the facts to prove their case through defendants and third parties.

In this context, the objections raised by the law professors are not convincing. First, it is not fair to describe existing state law as “coherent,” “robust and uniform,” so that U.S. businesses already enjoy “a high level of predictability.” The rhetoric does not obscure the reality of a patchwork of differing standards and rules – in some ways more divergent than before enactment of the UTSA – that necessarily creates friction and inefficiency for companies with interstate operations.

Second, while admitting that the current language on ex parte seizure is "more limited in scope" than the 2014 legislation (for example, only property "necessary to prevent the propagation or dissemination of the trade secret" can be seized), the professors think this tightening is not enough and that the provision "may still result in significant harm." No evidence is provided, but only speculation that mere invocation of the procedure might cause small businesses to "capitulate," and that the "chilling effect on innovation and job growth . . . could be profound." Again, the reality could hardly be more different. The DTSA is loaded with limitations making seizure very difficult to achieve, and with liabilities making it prohibitively expensive to be wrong in asking for it. In the unusual case where the plaintiff has no substantial basis for the claim, the defendant will simply file an opposition, the seizure will be dissolved, and the plaintiff will pay for the harm. Surely the benefits of the DTSA are worth that occasional risk.

Third, the professors assert that new language, added to the DTSA to ensure that mobility of labor is respected, embraces the so-called "inevitable disclosure doctrine," which they view as the equivalent of a judge-made noncompetition agreement. In fact, that "doctrine" is nothing more than a method of analysis under the common-sense UTSA provision allowing injunctions against "threatened misappropriation." This method has been applied thoughtfully in a majority of jurisdictions, resulting in a wide range of conditional remedies, and has only rarely been applied in a way that stops anyone from taking a new job.

The DTSA is sorely needed to fill a gap in remedies available to U.S. businesses that now operate in an information-based, globalized economy. This is one of those instances where federal structures are required to address a critical set of interstate and international problems. The DTSA has been carefully constructed to deter and punish abuse. Using well-established definitions and norms, it provides a choice to file a familiar claim in an effective forum. And there is absolutely no danger that enacting this statute will generate some new form of "troll" behavior to this point unknown in trade secret law