What You Need to Know About the Defend Trade Secrets Act

January 31, 2016 by James Pooley

January 31, 2016 Damages, DTSA, Personal Jurisdiction, Trade Secrets, USPTO Director Dennis Crouch

Guest post by James Pooley. Pooley is the former Deputy Director General of WIPO. He recently testified at the Senate Judiciary Committee in favor of the Defend Trade Secrets Act. See his earlier Patently-O guest posts . He wishes to thank Prof. Peter Menell for contributing to this post.

Last Thursday the Senate Judiciary Committee favorably voted out the Defend Trade Secrets Act ("DTSA"), which would amend the Economic Espionage Act ("EEA") to give trade secret plaintiffs the option of filing civil claims for misappropriation directly in federal court. The vote reflected broad bipartisan support (there are now 27 cosponsors in the Senate) and followed a substantive hearing on December 2 at which I had the privilege to testify. Since that time a number of senators engaged in discussions about how to improve the legislation. The result was a series of amendments, all of which have been adopted. Because the bill is likely to proceed quickly at this point, it would be useful to describe what has changed and what those changes could mean for practitioners and companies.

The notable amendments generally fall into four categories: (1) harmonizing with existing standards under the Uniform Trade Secrets Act ("UTSA"); (2) tightening up the process for preventive seizure of secrets; (3) ensuring that injunctions do not unreasonably restrain employee mobility; and (4) providing an exception for whistleblowers who disclose confidential information in order to report a crime to the authorities. The first three of these are laid out in a "Substitute" for S.1890, and the fourth is described in a separate amendment proposed by Senators Patrick Leahy and Chuck Grassley.

Bringing the DTSA in closer alignment with familiar provisions of the UTSA, the amendments have slightly changed the definition of a trade secret. The EEA had previously required that qualifying information not be known or

readily ascertainable to “the public,” while the UTSA had used the phrase “persons who can obtain economic value from its disclosure or use.” While it was never clear whether this difference would actually matter when applied in litigation, the UTSA formulation has now been adopted, so that the two laws are congruent. (Some still point to the different list of examples of protectable information in the UTSA and EEA definitions, but this has never been shown to make any difference in the broad meaning of the common basic term “information.”)

The amendments have also changed the term of the statute of limitations from five years to three. Although a number of states have designated longer periods (from four to six years), this brings the DTSA into line with the UTSA as it was originally proposed. In the same vein, the enhanced damages provision, which had allowed a punitive assessment up to three times the compensatory award, has been adjusted to match the provisions of the UTSA at twice the amount of compensatory damages.

SEIZURE PROVISIONS

The ex parte seizure provisions have been substantially tightened, providing more assurance that this remedy will not be abused. First, the bill now expressly refers to seizure as available only in “extraordinary circumstances.” Second, an ambiguity identified by Senator Whitehouse at the December hearing has been resolved by clarifying that the target of the seizure must be in “actual” possession of the trade secret and property to be seized. Third, access to the seized material is more limited: only federal law enforcement can perform the seizure, with assistance as necessary from state authorities and an independent technical expert, but the applicant is barred. And following the seizure, the court may have the material sorted by a special master who, like the technical expert, must be under confidentiality restrictions. Fourth, in issuing its order the court must direct when the seizure may be carried out, and whether force may be used to access locked areas. Finally, in a new section the bill requires the Federal Judicial Center to develop “best practices” for seizure and handling of electronically stored information.

MOVING ON FROM “INEVITABLE DISCLOSURE”

One of the most interesting and potentially impactful provisions of the amendments concerns the preservation of employee mobility. Recognizing

the critical importance of preventive relief to a right that can be so easily destroyed, the UTSA has always permitted injunctions against "threatened misappropriation," and the same language is used in the DTSA. But because the DTSA would establish a national standard, some expressed fears that the "inevitable disclosure doctrine," which has been expressly rejected in some states, might be used by federal judges to block an employee from taking a new job. The draft bill had tried to address this concern with a proviso that no injunction could "prevent a person from accepting an offer of employment under conditions that avoid actual or threatened misappropriation," but this did not quiet the controversy.

To understand the nature of the dispute we need to wind back the clock to 1995, when the Seventh Circuit issued its decision in Pepsico v. Redmond, 54 F.3d 1262 (7th Cir. 1995), affirming a five-month injunction against a former marketing executive who had lied about his plans to take an identical position with another company that was about to launch a directly competitive product. Although the court had emphasized the executive's bad behavior, it also summarized that "defendant's new employment will inevitably lead him to rely on the plaintiff's trade secrets." Commentators promptly wrenched this phrase from its context and warned that Pepsico could be used to justify enjoining someone from taking a job just because of what he or she knew. This is how the so-called "inevitable disclosure doctrine" was born.

Having (mis)construed Pepsico this way, it was easy for some to make it a target, raising the alarm that "inevitable disclosure" was the equivalent of a post-hoc judicially-imposed non-compete agreement. Perhaps unsurprisingly, the backlash was particularly strong in California, where employees are protected by a robust public policy against restrictive covenants. In Whyte v. Schlage Lock, 101 Cal. App. 4th (2002), an intermediate appellate court issued a blistering condemnation of the doctrine and flatly declared it unacceptable under California law. It did this in response to the plaintiff's argument that the doctrine should be available as an "alternative" to proving "threatened misappropriation." Just what kind of evidence might be enough to establish a threat under the UTSA was not addressed. However, that question was answered several years later in another appellate decision, Central Valley General Hospital v. Smith, 162 Cal. App. 4th 501 (2008). The court said that evidence of bad behavior, like a prior misappropriation, an intention to misappropriate, or a refusal to return confidential material, would be enough to supply the inference.

In the meantime, however, the ideological battle lines had been drawn, and the forces mustering against inevitable disclosure, reinforced by many academic and popular articles, were determined to stamp it out if possible, or at least to protect their own jurisdiction from infection. The fervor of the debate apparently distracted everyone from critically examining what "inevitable disclosure" meant, or how it was actually being applied in places that didn't have a reflexive opposition to it. It turns out that the doctrine was almost never used as the opponents assumed, that is where the only threat indicator was how much the employee knew. In fact, in those cases judges typically explained their denials by reminding the plaintiff that if all this information had been so critically important they could have demanded that the employee sign a non-compete agreement.

Following last December's hearing, and in the wake of continuing concerns over the relevant DTSA language, I reached out to my friend Mark Lemley, professor at Stanford Law School. Mark and I had worked together before on issues relating to California's "high velocity" labor market, and after some discussion about what appeared to be this false conflict over the inevitable disclosure doctrine, we suggested to Senate staff that the issue could better be reframed around the kind and quality of evidence that should be required – under the UTSA or the DTSA – to prove "threatened misappropriation," and that the inquiry should focus on the employee's behavior, not merely on how much they knew.

Ultimately, Senator Dianne Feinstein proposed the relevant portion of the DTSA amendments, which now allows an order against threatened misappropriation, provided that it not "prevent a person from entering into an employment relationship, and that conditions placed on such employment shall be based on evidence of threatened misappropriation and not merely on the information the person knows." (In a belt-and-suspenders approach, the DTSA also includes a directly related amendment proposed by Senator John Cornyn that the order may not "otherwise conflict with an applicable State law prohibiting restraints on the practice of a lawful profession, trade, or business.")

The new language on threatened misappropriation has at least two very positive effects. First, it makes express the apparent consensus from the courts that "threatened" misappropriation may not be established merely by the importance of the information that someone knows. This makes sense

not only as a matter of public policy but also of evidence law. Second, it relieves us from the energy-draining debate over “inevitable disclosure,” which was pretty much a straw man that people loved to punch. Courts will not have to consider whether a jurisdiction accepts or rejects this abstract “doctrine,” but instead will ask: what is the actual evidence from which we should conclude that this person (or their new employer) can’t be trusted to honor the integrity of the plaintiff’s trade secrets? Outcomes in particular cases should not be substantially different.

WHISTLEBLOWER PROTECTION

A second major amendment was offered separately by Senators Leahy and Grassley, addressing a new, and in my opinion long neglected, question: how do we assure that employees and contractors who come upon evidence of illegal activity, but who are constrained by nondisclosure agreements from communicating those facts, can safely speak to their lawyers and to law enforcement officials? One might think that this question would already have been reliably answered by now, but it hasn’t been. In a wide-ranging and thoughtful on the subject, Tailoring a Public Policy Exception to Trade Secret Protection, Professor Peter Menell of the UC Berkeley School of Law explores not only the sparse, murky, and sometimes contradictory legal authority, but also the psychology of whistleblowing and the importance of a clear “safe harbor” for those who are thinking of reporting wrongdoing. As he notes, “[t]he same routine non-disclosure agreements that are essential to safeguarding trade secrets can be and are used to chill those in the best position to reveal illegal activity.” As a practical matter, employees and contractors face a stark dilemma, where the upside is a clear conscience (and possibly a reward for uncovering fraud) but the downside can involve painful and relentless retaliation as well as personal, financial, legal, and professional risk. Insulating the whistleblower from costly trade secret exposure serves larger societal interests in law enforcement, tax compliance, and surfacing and deterring securities fraud and fraud against the government..

Yet because of the difficulty of enforcing trade secrets once they leak, companies risk potentially significant losses if employees or contractors mistakenly disclose legitimate trade secrets—i.e., those that do not reveal illegal conduct. Peter’s article provided a balanced and effective solution to this dilemma that protects whistleblowers without jeopardizing disclosure of legitimate trade secrets. The proposed safe harbor insulates whistleblowers

and their counsel from trade secret liability for disclosing trade secret information in confidence to government officials or as part of a lawsuit alleging retaliation by an employer provided that the information is filed under seal. (The federal Trade Secrets Act, 18 U.S.C. § 1905, generally prohibits governmental employees from disclosing trade secrets.) The proposed statutory exception to trade secret liability provides clear assurance to potential whistleblowers that they do not violate their NDAs merely by consulting legal counsel regarding reporting allegedly illegal conduct to a responsible government official through a confidential channel. In addition, this safe harbor insulates lawyers advising potential whistleblowers about their options and serving as conduits for presenting evidence of allegedly illegal conduct to the government. The efficacy of the safe harbor is enhanced by requiring that NDAs prominently include notice of the law reporting safe harbor to ensure that those with knowledge of illegal conduct are aware of this important public policy limitation on NDAs and exercise due care with trade secrets in reporting such activity.

After Peter's article appeared just as the DTSA was gaining momentum in the fall, the Senate staff reached out to him to help craft appropriate language. The Leahy/Grassley amendment provides immunity under federal or state law against any claim for violation of an individual's nondisclosure obligations for disclosure, made in confidence, to (a) an attorney or government official, for the purpose of reporting or investigating a violation of law, or (b) a filing made under seal in a lawsuit "or other proceeding." In order to ensure that employees (a term that also includes contractors) know about their rights, employers are required to give an appropriate notice in the nondisclosure agreement (as is often done now with state inventor statutes), although this can be a reference to the company's separate policy document. A failure to comply with the notice provision would block any award of attorneys' fees or enhanced damages against an employee under the DTSA. Significantly – and this point was emphasized by Senator Feinstein at the hearing on January 28 – the whistleblower protection would not extend to any otherwise improper acts by the employee, such as hacking information in violation of the Computer Fraud and Abuse Act.

CONCLUSION

The DTSA in its current form is a strong bill, meeting its original objective of giving plaintiffs access to federal courts, which are better equipped to

handle cases of interstate or international misappropriation of trade secrets. In my opinion, all reasonable objections have been adequately addressed, and there are sufficient protections built in against abuse. Moreover, passage of this bill would substantially improve the environment for both plaintiffs and defendants, by making trade secret litigation more predictable, establishing a national standard for issues like “threatened misappropriation,” and striking the right balance of interests to promote responsible efforts by whistleblowers to report possible violations of law.

www.pooley.com