How Courts Approach Trade Secret Identification: Part 1

By Mark Klapow, Julia Milewski and William Pellett
(July 10, 2018, 1:58 PM EDT)

Protecting intellectual property has never been more important. For S&P 500 companies, intangible assets like IP rights represent over 80 percent of their market value, up from just 17 percent in 1975.[1] And as patents become more difficult to enforce,[2] companies are increasingly turning to trade secrets to protect those assets, leading to an increase in trade secret litigation. But trade secret law has been slow to adapt to the changing realities of the global economy where new technologies and products cross borders and digital frontiers, employees more frequently transition between jobs, and IP includes business processes, techniques, and customer data.

Given this backdrop, courts and some legislatures have attempted to create uniform trade secret protections across venues to increase predictability and certainty for victims of trade secret misappropriation. At the center of these efforts is this threshold question: What are the trade secrets at issue and when and how should they be identified? There is no registration process for trade secrets ahead of litigation. And because a trade secret is one of the most elastic concepts in the law — virtually anything not generally known could be a trade secret if it has value from not being generally known[3] — a plaintiff must tell the defendant and the court what, exactly, is being litigated in a particular case. But when, and how, and with what level of specificity? These questions have yet to be uniformly addressed, and failure to do so increases the costs and uncertainty associated with trade secret litigation.

The first article of this two-part series focuses on the current state of early trade secret identification in courts and whether it comports with the goals of recent legislative efforts like the Defend Trade Secrets Act.

The Goals of Trade Secret Laws

The goals of trade secret laws are both to prevent the theft of trade secrets and provide companies with a means of recovery when their trade secrets are stolen. American companies bear the significant costs of trade secret theft. The Commission on the Theft of American Intellectual Property estimates that trade secret theft causes
Likewise, the Center for Responsible Enterprise and Trade and PwC estimate that the cost of trade secret theft to the American economy is equivalent to 1-3 percent of America’s annual GDP, or $160-$480 billion annually. Beyond financial losses, trade secret theft harms American competitiveness and innovation by decreasing incentives for investing in research and development.

State and Federal Trade Secret Law

Despite the high stakes, lack of uniformity has plagued trade secret cases for decades. The law governing misappropriation of trade secrets historically developed separately in each state. In 1979, the Uniform Law Commission passed the Uniform Trade Secrets Act to unify state law governing trade secrets and create predictability for parties litigating trade secret cases. But, key commercial centers like New York never passed the UTSA. Some jurisdictions passed modified, state-specific versions of the UTSA. And in still other jurisdictions, identical provisions of the UTSA were interpreted by courts differently. In short, the UTSA failed in its central mission — to achieve uniformity. This resulted in a patchwork of state trade secret laws with legally-significant differences for victims of trade secret theft. Companies lamented the high costs and slow pace of litigation when bringing claims under state UTSA laws. Commentators complained that state courts were not equipped to address trade secret dissemination across state and national borders, and in many cases, cannot provide cross-jurisdictional discovery or efficient remedies.

To address these concerns, in 2016, Congress passed the Defend Trade Secrets Act. Although it does not preempt the UTSA, the DTSA:

Provide a single, national standard for trade secret misappropriation with clear rules and predictability for everyone involved. Victims will be able to move quickly to Federal court, with certainty of the rules, standards, and practices to stop trade secrets from winding up being disseminated and losing their value.

American companies drove this change, demanding a solution to the problems posed by trade secret theft in today’s global, data-driven economy. The DTSA addressed many of the problems with inconsistent state-specific trade secret misappropriation claims, providing victims of trade secret theft with tools to protect trade secrets in the digital age.

Current State of Trade Secret Identification

Trade secrets are, by definition, secret. This creates a problem unique to trade secret litigation: The IP at issue cannot be identified in a public complaint without destroying its status as IP. Thus, trade secret law has evolved to require only the most basic description of the trade secrets in the complaint. The dispute over further identification of trade secrets is then left to be resolved in the litigation itself.

Thus, early trade secret identification at least could be an issue common to every single trade secrets case regardless of issue, size or jurisdiction. Nearly everyone agrees that the trade secrets at issue in the litigation must be identified. But when? And with what level of specificity? And what happens if they are not?

In practice, the process for early identification of trade secrets can devolve into a disparate, inconsistent morass without a single, unifying principle. The sheer variety of approaches among jurisdictions to this common issue proves this point: California and a few other states have codified a trade secret...
identification rule for every case and courts stay discovery if that rule is not satisfied. But litigants complain that, in practice, the rule is not consistently applied, resulting in lengthy delays. Many states have case law that supports an early identification practice, but often with few useful guideposts concerning the level of specificity that is required or the consequences for noncompliance. Some judges require early identification, but without the type of uniformity litigants hope for. Other jurisdictions and many individual judges decline to apply any trade secret identification rule at all.

What Level of Detail Is Sufficient to Identify a Trade Secret?

How much a claimant needs to reveal to assert claims is open to debate, harming both claimants that want to proceed with discovery to prove up a trade secrets case and defendants who believe they have been unjustifiably accused.

Some courts have held that generic categories of information sufficiently identify the trade secrets at issue.[12] For example, in Aspen Marketing Services Inc. v. Russell, the court held defendant’s identification of “general areas of information” alleged to be trade secrets, including “unique, confidential business practices, models and data[,] customer lists ... [and] pricing and marketing strategies” was adequate.[13] Likewise, the plaintiff in Kelly Services v. Eidnes sufficiently identified its trade secrets by pointing to general information on “training methods and needs; [and] recruiting and resourcing details and information.”[14]

Other courts have chosen to eschew a clear trade secret identification rule altogether in favor of requirements that are “fact-specific” or determined on a “case-by-case” basis.[15] Such an approach, of course, undermines predictability even within a given jurisdiction and can increase costs and result in delay.

Still others have required plaintiffs to identify their trade secrets with “reasonable particularity.“[16] This standard generally focuses on whether (1) the defendant is placed on notice of the claims; (2) the plaintiff and the court are capable of assessing the relevancy of discovery and preventing fishing expeditions; (3) the plaintiff is prevented from crafting the alleged trade secrets based on confidential information learned from the other party; and (4) the court can prevent meritless litigation intended to harass the defendant.[17]

Others apply statutory standards governing trade secret identification. California, for example, has codified the “reasonable particularity” standard in Section 2019.210 of the California Code of Civil Procedure, providing that “before commencing discovery relating to the trade secret, the party alleging the misappropriation shall identify the trade secret with reasonable particularity subject to any [protective] orders.”[18] California courts have even gone so far as to describe this statute as “purposefully vague to permit ‘play in the joints.’”[19] As a practical matter, this standard has created a gating issue, potentially rewarding defendants’ bad behavior by delaying discovery and driving up costs for trade secret plaintiffs who must respond to repeated challenges or prove up their case before discovery begins in earnest.

When Is Identification Required?

There is further confusion around when this identification should occur. Defendants often raise the adequacy of a plaintiff’s trade secret identification on a motion to dismiss, as a prerequisite to discovery, or on a motion for summary judgment.[20] In some cases, defendants may repeatedly challenge the plaintiff’s identification with a series of motions to compel and protective orders, compounding the
And, given the different legal standards applicable to different phases of litigation, case law varies widely in articulating trade secret identification requirements. Indeed, courts frequently fault parties for citing trade secret identification case law inapplicable to a given case’s posture, turning early identification into a mini-trial on the format of trade secret identification rather than the validity of the claims.

Does the Current Model Make Sense?

Standardizing trade secret identification is key, but the data reveals a gap between goal and reality. Analytical data of thousands of federal trade secret cases suggest that trade secret identification falls far short of the speed, efficiency and clarity that Congress envisioned — and industry sought — when passing the DTSA for trade secret cases, even in states like California that have codified a statutory standard for doing so. Recent analytics across federal courts show that trade secret cases as a whole took 214 days to grant a permanent injunction, 161 days to reach the motion to dismiss stage, 612 days to reach the summary judgment stage, 808 days to reach trial, and 265 days on average to reach termination. It is not clear what portion, if any, of these time frames can be attributed to the delays surrounding trade secret identification. However, other forms of litigation proceed with greater speed when measured against the same analytics. On average, both patent and commercial litigation cases reached summary judgment and termination far sooner than trade secret cases. This is unsettling given that trade secret cases often involve preliminary relief, after which they may settle.

One thing is clear: There is a more consistent approach to trade secret identification that can be applied across all cases and jurisdictions to ensure swift and efficient adjudication of these trade secret cases while balancing competing interests. But what?

Stay tuned.


[11] Statement of Thomas Beall, supra note 9, at 4-5; Statement of Karen Cochran, supra note 9, at 3-5.


[23] See, e.g., Aspen Mktg. Servs., Inc., 2009 WL 4674061, at *7 (“Defendants incorrectly rely on summary judgment cases to support their motion to dismiss” premised on plaintiff’s insufficient trade secret identification); Medtech Prod. Inc. v. Ranir, LLC, 596 F. Supp. 2d 778, 790 (S.D.N.Y. 2008) (noting, on a motion to dismiss, that “the case principally relied on by Defendants for the proposition that specificity [of trade secret identification] is required in the Complaint granted defendants’ motion for summary judgment (and not a motion to dismiss)

[24] LexMachina’s trade secret platform provides insight into over 9,600 DTSA and state UTSA trade secret cases in federal court.