Santa Clara University School of Law

Santa Clara High Technology Law Journal

Volume 33 | Issue 4 Article 3

4-22-2017

Threatened Misappropriation of Trade Secrets: Making a Federal (DTSA) Case Out of It

David Bohrer

THREATENED MISAPPROPRIATION OF TRADE SECRETS: MAKING A FEDERAL (DTSA) CASE OUT OF IT

David Bohrer[†]

The majority of trade secret theft is an inside job; it is committed by employees or business partners departing to take a position with a competitive business. Typically, at the time of departure, there is a very real threat that trade secrets have already been stolen and will be shared with a competitor, but there is no evidence that any such theft has actually occurred. The preferred course of action in the eyes of the former employer who owns the trade secrets is to immediately obtain an injunction enjoining any future or continued misappropriation of its trade secrets and requiring the return of its protected material—if this relief is available.

Both state trade secret laws as well as the new federal law, the Defend Trade Secrets Act of 2016 ("DTSA"), offer injunctive relief for threatened trade secret misappropriation. As between state laws and the DTSA, there are significant advantages to bringing the action under the DTSA, including procedural efficiency, nationwide service of discovery, and reduced costs and time to resolution. The problem is that there is little federal precedent on the evidence needed to establish threatened misappropriation under the DTSA.

Because California trade secret law shares a pro-employee mobility philosophy with the DTSA, it is a likely source of decisional law for federal courts seeking guidance on resolving DTSA claims. From California cases, therefore, one can glean specific and practical examples that will support entry of an injunction enjoining threatened misappropriation under the DTSA. These examples are summarized at the conclusion of this article. The goal is to better inform the determination whether a former employer confronting the

† David Bohrer is the managing partner of Merchant & Gould's Silicon Valley office and is a member of the firm's Intellectual Property Litigation Group. He is a technology trial lawyer who has won trials, obtained significant money damages and injunctive relief, and secured favorable defense verdicts and rulings for his clients. He has significant experience handling trade secret misappropriation litigation and also focuses his litigation practice on patent, trademark, copyright, and other IP matters in federal and state courts, arbitrations and mediations across the country. He may be reached at dbohrer@merchantgould.com.

threat of insider trade secret theft has sufficient evidence to make a successful DTSA claim.

TABLE OF CONTENTS

INTRODUCTION

The great majority of intellectual property ("IP") theft is committed by departing employees or business partners. Until recently, the principal method of preventing such insiders from taking valuable company information to a competitor was for the employer to assert a state law claim for threatened trade secret

misappropriation.[1] Additional relief is now available due to the enactment of the Defend Trade Secrets Act of 2016 ("DTSA"),[2] which creates a federal cause of action for actual and threatened trade secret misappropriation.

There are compelling reasons why an employer faced with insider IP theft may want to bring a federal as opposed to state law claim for threatened misappropriation. But what evidence is required to prove threatened misappropriation under the DTSA? How does the former employer "make a federal case out of it?"[3]

While there are not yet enough cases applying the federal law to answer the question, certain state court decisions can serve as a good predictor of what will be required. Many state courts, mostly in California, refuse to enjoin new employment based on the inference that it is inevitable that sensitive and proprietary information known to a departing employee will be disclosed in the course of the new employment (the "inevitable disclosure doctrine"). California and other jurisdictions rejecting inevitable disclosure will not enjoin or restrict new employment based solely on what the departing employee *knows*, but instead require evidence of *words or conduct* sufficient to demonstrate an actionable threat.[4] The DTSA takes a

---

1. This article focuses on "threatened" rather than "actual" trade secret misappropriation, either of which may be enjoined. *See, e.g.*, Uniform Trade Secrets Act ("UTSA") issued in 1979 by the National Conference of Commissioners on Uniform State Laws, *available at* http://bit.do/UniformTradeSecretsAct. UNIF. TRADE SECRETS ACT § 2(a) (UNIF. LAW COMM'N, amended 1985) ("SECTION 2. INJUNCTIVE RELIEF. (a) Actual or threatened misappropriation may be enjoined.") [hereinafter UTSA]; *see also id.* § 3(a) (further explains both types of misappropriation). Most trade secret theft occurs when a departing insider joins a competing business. While the former employer does not know of any actual misappropriation of its trade secrets, it strongly believes this is likely to happen. Restricting the new employment or the use of any trade secrets by the competing business therefore depends on whether the threat of misappropriation is sufficient to warrant court intervention. The question of what proof is required to establish an actionable threat is the stepping-off point for this discussion.

2. Defend Trade Secrets Act of 2016, Pub. L. No. 114-153 (May 11, 2016) (codified at 18 U.S.C. §§ 1831 *et seq.*) [hereinafter DTSA].

3. The phrase "make a federal case out of it" has roots in efforts by railroads in the late 1800s to avoid local and state regulation by finding bases for taking disputes into federal courts. *See* Jane Anne Morris, *Making a Federal Case Out of It*, DEMOCRACY THEME PARK (Jan. 5, 2015), http://bit.do/FederalCaseOutOfIt. The phrase also can refer to exaggerating the seriousness of something, as in "[don't] make a federal case out of it." *Make a federal case out of*, THEFREEDICTIONARY.COM (2017), http://bit.do/FreeDictionaryFederalCase. As used in this article, the phrase works on both levels—insider IP theft, from the employer's perspective, is best addressed by avoiding local and state venues in favor of federal court, and is also a serious issue that is not over-exaggerated as requiring significant investment in developing more effective solutions.

4. Cent. Valley Gen. Hosp. v. Smith, 162 Cal. App. 4th 501, 527-28 (2008); Edifecs Inc.

similar approach and rejects "inevitable disclosure" as sufficient to show threatened misappropriation, so it is appropriate to look to these state cases as a guide.

In Section I, I use a hypothetical to introduce key background concepts, namely: a company's IP is often protectable as trade secrets; there are compelling policies behind the protection of trade secrets; and, that the majority of trade secret theft is by insiders, who, thanks to more recent and steadily advancing digital device and wireless communication technologies, can now steal more proprietary data and information, in less time, for less money, and more quickly than they ever could before. In short, insider theft poses a serious and as yet unresolved issue for many employers, particularly technology companies whose valuable assets are mostly intangible information.

Section II explains that the principal strategy for addressing insider IP theft is bringing a pre-trial motion early in the case to enjoin the threatened misappropriation of trade secrets. However, an employer who fails to sufficiently evaluate the strength of its misappropriation claim before commencing litigation risks incurring huge expenditures of time and money and getting nothing in return. These considerations dovetail with the discussion in Section III about how bringing a claim under the DTSA may reduce the employer's costs and increase the likelihood of a favorable result. Before choosing this option, an employer must address the uncertainty surrounding the lack of federal precedent on the proofs required to establish a threatened misappropriation under the DTSA.

Section IV argues that California state court decisions provide a reasonable basis for predicting the evidence required to establish threatened misappropriation under the DTSA because California trade secret law and the DTSA share a pro-employee mobility philosophy that rejects inevitable disclosure as a basis for establishing threatened misappropriation. Section V reviews specific California cases finding threatened misappropriation by a departing insider, and gleans from these cases examples of the specific evidence that is most likely necessary to make the same showing under the DTSA… or, in other words, how to "make a (successful) federal (DTSA) case out of it."

---

v. TIBCO Software, Inc., 756 F. Supp. 2d 1313, 1320 (W.D. Wash. 2010) (interpreting *Cent. Valley*). *See also* UTSA § 6, at 2 (further discussion of evidence required to establish threatened misappropriation).

I. IP THEFT BY INSIDERS DEPARTING FOR NEW EMPLOYMENT IS A SIGNIFICANT PROBLEM

It is another impossibly beautiful morning in Silicon Valley, and you arrive at the office imbued with energy and optimism regarding your company's position as a leading developer of self-driving vehicle technology. You are the manager of a high profile business unit that is developing a laser-based system, referred to as LiDAR, that uses the reflection of laser beams off objects to create a real-time 3D image of the world. The LiDAR images allow your company's autonomous vehicles to "see" their surrounding environment. LiDAR, like most of your company's technology, is powered in large part by non-public, trade secrets developed over thousands of research and development hours by leading engineers, designers and researchers. Sure, there is a frenzied race among dozens of companies and startups to commercialize self-driving technology, but your company's technology is better than that of any other competitor and you plan to keep it that way.

You get the text from your CEO before you have the chance to boot up your computer. You learn that the night before the CEO received an email from the technical director of the LiDAR business unit giving his two weeks notice. There was no prior indication that this employee was unhappy and he had recently received a sizeable salary increase and additional options and other incentives. As the manager of the employee's business unit, you are asked to follow up. You walk over to the employee's work station, where he too is in the process of booting up. You are told that the employee has taken a higher-paying and more senior position with a large foreign telecommunications company that announced a month ago that they are going to open a Silicon Valley innovation center focused on developing "smart device" technology. He says that he "does not expect to be working in the same area at the new place." He assures you that he will cooperate in any transition effort that you request. Per company policy, that same day, all company devices are collected, the employee signs written forms confirming both that he has returned all company data and devices and that he is aware of and has complied with previous employment agreements regarding the confidentiality of company information, and the employee is escorted from the office.

Notwithstanding the weather, the outlook is no longer sunny. The departing technical director has not just been privy to, but in many instances also helped develop highly sensitive technical and business information that you rightly think of as the intellectual

property (IP) assets of your company. Your company's competitive advantage would disappear quickly if the new employer, via your technical director, has immediate access to and use of your IP. The gross unfairness of a potential competitor avoiding the need to independently develop your IP, not to mention the significant risk to the new employer that at the end of the day their independent efforts might be unsuccessful, is maddening. You want to immediately block your technical director from taking the new job or at the very least restrict the employment sufficient to protect your IP.

Fortunately, a significant portion of your IP that is at risk most likely qualifies for protection under the law as trade secrets.

A. What Is a Trade Secret and Why Is It Protected?

Generally speaking, a trade secret is valuable, proprietary information or "know-how" that a business protects from use by competitors by taking reasonable efforts to maintain its secrecy.[5] The Supreme Court explained in *Kewanee Oil Co. v. Bicron Corp* that there are important public interests compelling protection of trade secrets.[6] *Kewanee* arose as a challenge by petitioners that trade secret law should be preempted as conflicting with federal patent law. The Court held there was no preemption based in significant part upon differentiating policies behind protection of trade secrets.[7] The Court

---

5. This definition reflects the definition used in several authoritative sources of trade secret law. Forty-eight state jurisdictions have modeled their trade secret laws on the UTSA, which states in pertinent part that "'[t]rade secret' means information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy." *Id*. § 1(4). California's version of the UTSA, which was enacted in 1985, dropped the requirement that a trade secret be not "readily ascertainable"—with the result that the defendant is required to specially plead this circumstance as an affirmative defense—but otherwise followed the UTSA definition. *See* California Uniform Trade Secrets Act ("CUTSA"), CAL. CIV. CODE §§ 3426-3426.11 (1984) (defining trade secrets as information as information that "[d]erives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use"," and "[i]s the subject of efforts that are reasonable under the circumstances to maintain its secrecy."). *Id.* § 3426.1(d)(1)-(2). The DTSA also follows the UTSA definition of a trade secret, providing in pertinent part that a trade secret is information which "the owner has taken reasonable measures to keep . . . secret"," and "derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information." 18 U.S.C. § 1839(3) (2016).

6. Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 482-83, 485-86 (1974).

7. *Id*. at 482-89.

said that trade secret law is grounded on "[t]he maintenance of standards of commercial ethics," and that there is an "inevitable cost to basic decency to of society when one firm steals from another."[8] It also is necessary to protect trade secrets for the "encouragement of invention."[9]

B. Trade Secrets in the Corporate Context

There is widespread recognition that trade secrets hold great value from a macro level, as a significant portion of IP in the US, and on a micro level, as the result of an employer's significant investment of time and resources.[10] In the early 2000s, economists estimated that theft of trade secrets costs companies as much as $300 billion per year.[11]

There is also compelling empirical evidence that the great majority of trade secret theft is committed by a company insider—an employee, contractor or business partner with authorized access to a company's IP.[12] In their 2010 statistical analysis of federal court trade

---

8. *Id*. at 481, 487.

9. *Kewanee* stands for the proposition that "[w]ithout guaranteed secrecy, businesses would be left to expensive self-help security measures that would disadvantage smaller competitors and discourage dissemination of information through sharing." James H. Pooley, *The Myth of the Trade Secret Troll*, 23:4 GEO. MASON L. REV. 1025, 1048-49 (2016) (citing *Kewanee*, 416 U.S. at 485-86).

10. Pooley*, supra* note 9, at 1067 ("And never have [trade secrets] been so valuable. As reported by Ocean Tomo, the share of public company value represented by intangible information leapt from 17 percent in 1975 to 68 percent in 1995 to 84 percent today. This means that industry in the span of a single generation has experienced a shift of historic proportions in the kind of property it uses to create value."); Sonya P. Passi, *Compensated Injunctions: A More Equitable Solution to the Problem of Inevitable Disclosure*, 27 BERKELEY TECH. L. J. 927 (2012) ("By their very definition, trade secrets hold great value, and employers often invest significant resources in their development and subsequent protection.") (citing Susan Street Whaley, *The Inevitable Disaster of Inevitable Disclosure*, 67 U. CIN. L. REV. 809, 816 (1999)).

11. David S. Almeling, et al., *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 GONZ. L. REV. 291, 292 (2010) (citing OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXECUTIVE, ANNUAL REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE—2002 vii (Feb. 2003), http://bit.do/ForeignEconCollectionIndustrialEspionage). Almeling et al. include the clarification that "[o]ther studies find different numbers, depending on the methodology used," and cite examples of studies from different time periods, different private and government agencies, breaking out direct vs. indirect costs, etc. 45 GONZ. L. REV. at 291 n.8. The core insight, whatever the exact estimate, is that the national cost of trade secret theft is extremely damaging to US companies—costing tens of billions of dollars at the very least.

12. "[A] malicious insider is defined as a current or former employee, contractor, or business partner who meets the following criteria: has or had authorized access to an organization's network, system, or data, . . . has intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems." GEORGE J. SILOWASH, ET AL.,

secret decisions issued over fifty-eight years, 1950-2008, David Almeling and his co-authors determined that in over 85% of the cases, the alleged misappropriator was either an employee or a business partner.[13] The following year, those researchers applied the same statistical methodology to state court trade secret decisions issued over the fourteen year period, 1995-2009, and determined that in over 93% of the cases, the alleged misappropriator was either an employee or a business partner.[14]

It has been the case for some time that corporate secrets are lost through insiders, but digital tools have dramatically increased the risk associated with this theft. Commentator James Pooley sums this up in a recent article: "With the arrival of ubiquitous digital devices with massive storage and robust wireless communications, the risk profile of holding trade secrets has been profoundly and irretrievably altered. Never have information assets been so vulnerable to loss."[15] Mr. Pooley continues, "The difference today is that digital tools make this kind of misappropriation easier, cheaper and harder to detect. . . . [t]hey make disappearance of the stolen property simpler and faster. And the destination is less likely to be a start-up company in the neighborhood. If an employee—or accomplice of an employee—slips a DVD into a purse or a USB into a pocket, it may be a matter of days or even hours before the perpetrator boards a plane out of the country."[16]

Returning to our hypothetical, your company, the employer, is suddenly confronting the high likelihood of an insider taking and sharing with your competitor valuable company LiDAR IP that is entitled to protection under state and federal trade secret law. It is not lost on you that the majority of IP theft is committed by insiders such as your technical director. Due to advances in digital transfer and storage technologies the technical director could have quickly and easily transferred from your possession into the hands of your competitor huge amount of data. You know the amount of time you have to block the use of your IP and collect what has been taken is extremely short.

SOFTWARE ENGINEERING INSTITUTE, COMMON SENSE GUIDE TO MITIGATING INSIDER THREATS xiii (Paul Ruggiero ed., 4th ed. 2012).

13. *See* Almeling et al., *supra* note 11, at 294, 302-303.

14. David S. Almeling, et al., *A Statistical Analysis of Trade Secret Litigation in State Courts*, 46 GONZ. L. REV. 57, 69 (2011).

15. Pooley, *supra* note 9, at 1066-67.

16. *Id*. at 1067.

Your primary legal option is to file a claim for misappropriation of your trade secrets. The other possible claims you could bring—most notably a breach of contract claim for failing to return and/or maintain the secrecy of your confidential and proprietary information, statutory claims for unfair competition, or state common law claims for breach of common law duties or other tortious conduct—can be more difficult for a former employer to assert and prove. Breach of contract claims asserted in connection with a departing employee taking a position with a competitor may be challenged as void and unenforceable on the grounds they violate section 16600 of the California Business and Professional Code, which states that "every contract by which anyone is restrained from engaging in a lawful profession, trade or business of any kind is to that extent void."[17] To the extent the Ninth Circuit and California courts have recognized that any such contractual restraints on competition may be enforced, it is based on excepting those contractual provisions deemed necessary to protect the former employer's trade secrets—effectively returning the focus of the litigation to trade secret misappropriation.[18] Furthermore, California courts and federal courts applying California law have held that California's trade secret law preempts or supersedes statutory and common law claims that share a common nucleus of facts with the misappropriation claim (as is the case in the hypothetical).[19]

So you focus on bringing a misappropriation claim. The next section discusses the elements of this claim under both federal law, the DTSA, and the California law and policies on which the federal law is modeled.

II. BLOCKING OR RESTRICTING NEW EMPLOYMENT BASED ON THREATENED MISAPPROPRIATION

A. Actual Misappropriation Is Not Required

As you watch your technical director drive out of your company's parking lot for the last time, you are struck by the

17. Cal. Bus. & Prof. Code § 16600 (1941); *see* Thomas Weisel Partners LLC v. BNP Paribas, No. 07–6198, 2010 WL 546497, at *4-5 (N.D. Cal. Feb. 10, 2010) (summarizing categories of employee agreements which may implicate a section 16600 violation).

18. *See* Henry Schein, Inc. v. Cook, No. 16-cv-03166-JST, 2016 WL 3418537, at *6 (N.D. Cal. June 22, 2016) (citing Asset Mktg. Sys., Inc. v. Gagnon, 542 F.3d 748, 758 (9th Cir. 2008); Muggill v. Reuben H. Donnelley Corp., 62 Cal. 2d 239, 242 (1965)).

19. Section III, *infra* (summarizing case authority on preemption by CUTSA of specific statutory and common law claims).

realization that notwithstanding your strong suspicions that a theft has occurred (or is about to occur), you have no evidence that your employee has retained possession of any confidential information or that he has divulged any company information—indeed, you have signed statements from the employee that he has not done these things. This does not end the inquiry, however. Court intervention is not limited to actual misappropriation.

The UTSA and the numerous state trade secret laws modeled on the UTSA authorize injunctions against "actual or threatened misappropriation."[20] Similarly, the DTSA states in pertinent part that "with respect to a misappropriation of a trade secret, a court may – (A) grant an injunction — (i) to prevent any actual or threatened misappropriation . . . ."[21] Courts have given force to this disjunctive language and interpreted "actual" as compared to "threatened" misappropriation as separate and distinct triggers of legal remedies. Actual misappropriation refers to a misappropriation that has already happened.[22] Threatened misappropriation occurs when, in the eyes of the law, misappropriation is likely enough to happen that a court will intervene.[23] But what is the likelihood of getting early injunctive relief on threatened misappropriation claim (i.e., does the employer

---

20. UNIF. TRADE SECRETS ACT § 2(a) (UNIF. LAW COMM'N, amended 1985) ("Actual or threatened misappropriation may be enjoined"); *see also* CUTSA, CAL. CIV. CODE, tit. 5, § 3426.2(a) (1984) (stating the same); Michigan Uniform Trade Secrets Act, MICH. COMP. LAWS § 445.1903(1) (1998) (stating the same); Texas Uniform Trade Secrets Act, TEX. CIV. PRAC. & REM. CODE § 134A.003(a) (2013) (stating the same). *Cf.* Wisconsin Trade Secrets Act, WIS. STAT. § 134.90(2) (1985) ("No person, including the state, may misappropriate or threaten to misappropriate a trade secret . . . .").

21. DTSA § 1836(b)(3)(A)(i)..

22. Whyte v. Schlage Lock Co., 101 Cal. App. 4th 1443, 1457 (2002) (actual misappropriation is "generally speaking, improper acquisition of a trade secret or its nonconsensual use or disclosure."); *see also* Passi*, supra* note 10, at 928 ("Actual misappropriation means that the trade secrets have already been divulged.") (citing Ecolab, Inc. v. Paolo, 753 F. Supp. 1100 (E.D.N.Y. 1991); Surgidev Corp. v. Eye Tech., Inc., 648 F. Supp. 661 (D. Minn. 1986)).

23. FLIR Sys., Inc. v. Parrish, 174 Cal. App. 4th 1270, 1279 (2009) ("'[T]hreatened misappropriation' means a threat by a defendant to misuse trade secrets, manifested by words or conduct, where the evidence indicates imminent misuse."); *see also Cent. Valley Gen. Hosp.,* 162 Cal. App. 4th at 525, 527. A related variation is that a party seeking to establish threatened misappropriation "must convince the court of the former employee's 'duplicity' by proffering evidence indicating a significant lack of candor or willingness to misuse trade secrets." Gene Codes Corp. v. Thomson, No. 09-14687, 2011 WL 611957, at *5 (E.D. Mich. Feb. 11, 2011) (citing and quoting from CMI Intern., Inc. v. Intermet Intern. Corp., 251 Mich. App. 125, 134 (2002) (citations omitted)); *see also* Passi*, supra* note 10, at 928 ("Threatened misappropriation occurs when the departing employee has demonstrated a bad-faith intent to divulge trade secret information.") (citing Clorox Co. v. S.C. Johnson & Son, Inc., 627 F. Supp. 2d 954 (E.D. Wis. 2009)).

have sufficient proof to justify the time and expense of bringing a claim)?

Any right-thinking litigant should know or at least want to know whether they have a strong case on the merits before they file a lawsuit. In the case of an employer considering suing a recently-departed employee and possibly the new employer/competitor, the need for an accurate and early evaluation whether there is sufficient proof of a threatened misappropriation is particularly acute.

The employer must plead in good faith facts sufficient to support a claim for threatened trade secret misappropriation or its pleading will be dismissed for failure to state a claim.[24] While courts deciding motions to dismiss directed to the sufficiency of the allegations in a pleading have significant discretion to dismiss the complaint without prejudice to amend,[25] the additional delay occasioned by amending and resubmitting the complaint adds weeks (if not months) to the earliest time by which the plaintiff employer could reasonably expect the court to address the merits, which is anathema to the employer who seeks relief from the court before the threatened misappropriation ripens into an actual misuse.

B. Employers Will Likely Seek Injunctive Relief

The plaintiff former employer, in most if not all instances, will also seek a temporary restraining order ("TRO")[26] or a preliminary injunction[27] enjoining the threatened misappropriation. They are compelled to do so by the fundamental risk that absent immediate injunctive relief their trade secrets will be disclosed to and misused by a competitor. Should matters progress to where an actual

---

24. *See, e.g.*, *Edifecs, Inc*., 756 F. Supp. 2d at 1320-21 (supporting its holding that the complaint failed to state a claim upon which relief could be granted for threatened misappropriation under California law, the court said that the allegations were speculative and insufficient to show the departing employee's words or conduct rose to the level of an actionable threat of trade secret theft).

25. This was the case in *Edifecs*. *Id*.

26. An injunction may be entered on a temporary and emergency basis prior to trial. Typically referred to as a temporary restraining order or "TRO," this form of injunctive relief is unique in that it may be entered ex parte, i.e., without first informing the opposing party, and lasts a very short time—only so long as is necessary to protect against irreparable harm leading up to consideration of a preliminary injunction. *See, e.g.*, CAL. CIV. PROC. § 527(d) (rules regarding entry of TRO without notice); FED. R. CIV. P. 65(b) (corresponding federal rules).

27. In comparison, a preliminary injunction is a provisional remedy, typically entered upon giving notice and an opportunity to be heard to the opposing party. It is intended to preserve the status quo and prevent irreparable harm up through final disposition of the litigation. *See, e.g.*, CAL. CIV. PROC., §§ 527(a), (e), and (f) (rules regarding preliminary injunctions); FED. R. CIV. P. 65(a) (federal rules on same subject).

misappropriation has occurred—or, should the former employer forego seeking early injunctive relief against threatened misappropriation—irreparable damage to the employer's business may have already occurred.[28] A core feature of state and now federal trade secret protection is that injunctive relief is available prior to the actual misappropriation of trade secrets.[29] Indeed, some commentators take this a step further and argue that "for trade secret protection to be effective, it must come prior to misappropriation."[30]

There are differences between the federal and state law regarding the requirements for issuing a preliminary injunction.[31] But whatever the variations, the likelihood of success on the merits is a key requirement in the court's determination whether to grant or deny an injunction.[32] To satisfy this requirement, the moving party will need to submit proof[33] sufficient to establish a threatened

---

28. Passi, *supra* note 10, at 939 ("In cases of actual misappropriation, the damage to the employer's business has already been done. No amount of monetary damages can restore the value of the trade secret.") (citing Jennifer L. Saulino, *Locating Inevitable Disclosure's Place in Trade Secret Analysis*, 100 MICH. L. REV. 1184, 1191, 1193 (2002)); *see also* Destinations to Recovery v. Evolve Initiatives LLC, B259011, 2015 WL 6755049, at 6 (Cal. Ct. App. Nov. 5, 2015) ("Defendants' reading would also mean that former employees would be able to exploit their former employer's trade secrets and confidential information without restraint, subject only to a later suit for damages after the fact. But a damages remedy will often come too late to protect those rights or to protect the employer. Trade secrets and proprietary information are valuable *because* they are confidential; once exploited by the former employee, a damages remedy is of little use to a defunct employer.") (emphasis in original).

29. Passi, *supra* note 10, at 939 ("[F]or trade secret protection to be effective, it must come prior to misappropriation.").

30. *Id.*

31. Under federal law, the standards for issuing a temporary restraining order (TRO) and preliminary injunction are the same. New Motor Vehicle Bd. of Cal. v. Orrin W. Fox Co., 434 U.S. 1345, 1347 n.2 (1977). A preliminary injunction is "an extraordinary remedy that may only be awarded upon a clear showing that the plaintiff is entitled to such relief." Winter v. Natural Res. Def. Council, Inc., 555 U.S. 7, 22 (2008). The plaintiff must show (1) that it is likely to succeed on the merits, (2) that it is likely to suffer irreparable harm in the absence of preliminary relief, (3) that the balance of equities tips in its favor, and (4) that an injunction is in the public interest. Stormans, Inc. v. Selecky, 586 F.3d 1109, 1127 (9th Cir. 2009) (citing Winter, 555 U.S. at 20). Compare the elements which must be satisfied to obtain a preliminary injunction in a California court, as described in *ReadyLink Healthcare v. Cotton*, 126 Cal. App. 4th 1006, 1016 (2005) ("A preliminary injunction is governed by the following principles: 'In deciding whether to issue a preliminary injunction, a trial court weighs two interrelated factors: the likelihood the moving party ultimately will prevail on the merits, and the relative interim harm to the parties from the issuance or nonissuance of the injunction.'") (quoting Whyte v. Schlage Lock Co., 101 Cal. App. 4th 1443, 1449-50 (2002)). The standards applicable to issuance of a TRO under California law are similar to those applicable to a preliminary injunction. San Diego Water Co. v. Pacific Coast S.S. Co., 101 Cal. 216, 218 (1894).

32. 126 Cal. App. 4th at 1016.

33. In view of the time constraints, federal courts generally permit counsel some leeway in demonstrating the factors relevant to issuing a preliminary injunction, which can be based on

misappropriation of trade secrets. In other words, early on—if not immediately upon commencing a trade secret case—the former employer will need not just good faith allegations but court admissible evidence sufficient to prove threatened misappropriation.

The practical consequence of the above need for compelling claim formation and supporting proofs early on in any trade secret litigation is that the former employer likely incurs fees and costs in the tens, if not hundreds, of thousands of dollars within months of filing a lawsuit. Even assuming there is a high value placed on obtaining injunctive relief from the court, the high costs associated with getting this result necessarily compel the former employer and his counsel to consider the risk of an adverse result. The less compelling the proofs to establish a threatened misappropriation, the less likely success on the merits or obtaining injunctive relief can be achieved, and simultaneously the greater the risk of an adverse result

---

evidence less complete than summary judgment or trial on the merits. *See* Six Clinics Holding Corp., II v. Cafcomp Sys., Inc., 119 F.3d 393, 400 (6th Cir. 1997) ("[A] preliminary injunction is customarily granted on the basis of procedures that are less formal and evidence that is less complete than in a trial on the merits. A party thus is not required to prove his case in full at a preliminary injunction hearing."); GSI Tech., Inc. v. United Memories, No. C 13-1081 PSG, 2013 WL 122172990, at *5 (N.D. Cal. Aug. 21, 2013) ("To prove a likelihood of success on the merits, a plaintiff need not prove its case to an absolute certainty—it only needs to show a reasonable probability, or at an "irreducible minimum," a "fair chance" of success on the merits."). A district court is still required to make findings of fact in supporting the issuance of a preliminary injunction. Sierra Club, Lone Star Chapter v. FDIC, 992 F.2d 545, 551 (5th Cir. 1993) ("Although the district court may employ informal procedures and rely on generally inadmissible evidence, the record must nevertheless support the district court's decision. Indeed, Rule 52 of the Federal Rules of Civil Procedure provides that 'in granting or refusing interlocutory injunctions the court shall similarly set forth findings of fact and conclusions of law which constitute the grounds for its decisions.'"). District courts will therefore conduct an evidentiary hearing, or, short of that, expect the moving party to submit proofs in the form of sworn declarations or deposition transcripts. *See id.* (discussing the need for an evidentiary hearing or, in the alternative, the option that "the district court can accept evidence in the form of deposition transcripts and affidavits"). In comparison, while preliminary injunction procedure varies among state courts, see for example, City of Los Altos v. Barnes, 3 Cal. App. 4th 1193, 1198 (1992) (because a hearing on a preliminary injunction was not the equivalent of a trial, a statement of decision was not required under California law), courts typically are required to make factual findings on the relevant factors, see for example, Fleishman v. Superior Court, 102 Cal. App. 4th 350, 356 (2002) ("Before issuing a preliminary injunction, the trial court must 'carefully weigh the evidence and decide whether the facts require . . . such relief.' The court evaluates the credibility of witnesses and makes factual findings on disputed evidence.") (citation omitted). Thus, similar to federal court procedure, state courts determining disputed factual issues raised by a preliminary injunction will receive evidence on these issues in the form of a verified complaint, sworn declaration, or deposition testimony. *See, e.g.*, ROBERT I. WEIL, ET AL., CALIFORNIA PRACTICE GUIDE: CIVIL PROCEDURE BEFORE TRIAL, Injunctions ¶ 9.581 (June 2016) (discussing how, in addition to a verified complaint, "[s]worn testimony or admissions contained in depositions, answers to interrogatories, or other discovery may also be used to prove facts supporting injunctions.").

that outweighs the return (value) on incurred costs. The sooner and better the evaluation as to whether there is sufficient proof of threatened misappropriation, the more likely it is that the employer avoids spending too much on litigation.

Further increasing the potential risk and costs of bringing a lawsuit is that a prevailing party may seek reimbursement of the fees and costs it incurred in the course of defending the action.[34] The field of trade secret litigation is littered with court decisions holding that threatened trade secret misappropriation has not been proven (or that the claim will likely not be successful), that trigger prevailing party motions for fees and costs.[35] These fee motions are themselves a separate and additional phase of the litigation that are time-consuming and expensive to process—to say nothing of the significant size of the fee award that may be assessed on the losing employer.[36]

III. WHILE BRINGING A DTSA CLAIM MAY HAVE ADVANTAGES OVER BRINGING A STATE TRADE SECRET LAW CLAIM, THERE IS NOT SUFFICIENT DTSA PRECEDENT TO PREDICT PROOF REQUIRED TO SHOW ACTIONABLE THREAT

A full analysis of the comparative benefits of filing a claim under the DTSA as compared to state trade secret law is best reserved until sufficient time has passed to allow consideration of a larger number of DTSA decisions. That said, even at this early stage in the development of DTSA precedent, it is apparent that there are compelling reasons why plaintiff employers should file their trade secret claims under the DTSA.

---

34. *See* UTSA § 4 ("Attorney's Fees. If (i) a claim of misappropriation is made in bad faith, (ii) a motion to terminate an injunction is made or resisted in bad faith, or (iii) willful and malicious misappropriation exists, the court may award reasonable attorney's fees to the prevailing party."); DTSA § 2(b)(3)(D) ("[I]f a claim of the misappropriation is made in bad faith, which may be established by circumstantial evidence, a motion to terminate an injunction is made or opposed in bad faith, or the trade secret was willfully and maliciously misappropriated, award reasonable attorney's fees to the prevailing party.").

35. *See, e.g.*, Conxall Corp. v. Iconn Sys., LLC, 61 N.E.3d 1081, 1088-89 (Ill. App. Ct. 2016); SASCO v. Rosendin Elec., Inc., 207 Cal. App. 4th 837, 843-44 (2012); *FLIR Sys., Inc*., 174 Cal. App. 4th at 1285-86; Contract Materials Processing, Inc. v. Kataleuna GmbH Catalysts, 222 F. Supp. 2d 733, 744-45 (D. Md. 2002).

36. *See, e.g.*, *FLIR Systems*, 174 Cal. App. 4th at 1286 (on appeal, the court affirmed award of $1,641,216.78 for attorney fees and costs to the party accused of trade secret theft); *SASCO*, 207 Cal. App. 4th at 843 (same in the amount of $484,943.46); *Contract Materials*, 222 F. Supp. 2d at 753 (same in the amount of $134,935).

The DTSA is aligned in many respects with the UTSA on which state trade secret laws are modeled.[37] More specifically, the DTSA includes definitions, remedies, and a statute of limitations substantially similar to the UTSA.[38] As Congress observed, "quite a few states have enacted customized versions of the UTSA, resulting in a lack of uniformity that makes [state trade secret statues] not wholly effective in a national and global economy."[39] A principal motivation behind the enactment of the DTSA was to provide a "single, national standard for trade secret misappropriation with clear rules and predictability for everyone involved."[40] While this policy is aspirational at this point, assuming the goal of creating a federal common law consistently applied across the country is ultimately realized, this means the DTSA provides plaintiff employers a more efficient and cost-effective platform for the protection of their trade secrets.[41]

The ability to bring a DTSA claim also gives trade secret owners the benefit of national service of discovery that is provided by federal courts (that hear DTSA claims) and the Federal Rules of Civil Procedure (that govern the processing of these claims by the federal courts).[42] The advantages to the trade secret owner of being able to serve nationwide subpoenas or to proceed with discovery anywhere in the country—as opposed to litigating in state court under a state-based statute and its attendant procedural hurdles and delays—in the words of commentator Mark Halligan, "cannot be overemphasized."[43] It is true that, prior to enactment of the DTSA (creating a federal cause of action giving the federal courts "federal question" subject

37. *Are You Ready for the Defend Trade Secrets Act?*, PRACTICAL LAW (May 2, 2016) http://bit.do/ReadyDefendTradeSecretsAct.

38. Adams Arms, LLC v. Unified Weapon Sys., Inc., No. 16-1503, 2016 WL 5391394, at *5 (M.D. Fla. Sept. 27, 2016) (citing H. REP. NO. 114-529, at 4-5, 12-14 (2016), as reprinted in 2016 U.S.C.C.A.N. 195-211).

39. H. REP. NO. 114-529 at 4 (2016).

40. *Id*. at 6.

41. *See* Pooley*, supra* note 9, at 1052 (referring to commentary that has "pointed out that economic advantages of federalization, particularly for small businesses, which rely more heavily on secrecy than on patenting . . .") (citing David S. Almeling, *Four Reasons to Enact a Federal Trade Secrets Act*, 19 FORDHAM INTELL. PROP. MEDIA & ENT. L. J. 769, 773-74 (2009)).

42. R. Mark Halligan, *Revisited 2015: Protection of U.S. Trade Secret Assets: Critical Amendments to the Economic Espionage Act of 1996*, 14 J. MARSHAL. REV. INTELL. PROP. L. 476, 493 (2015) ("This procedural advantage is critical in trade secrets litigation. Often the plaintiff resides in one state; the defendant resides in another; and the evidence of misappropriation and critical witnesses are in different states around the country.").

43. *Id*. at 494.

matter jurisdiction under 28 U.S.C. § 1331), a trade secret plaintiff could get its state-based trade secret claim heard in federal court, but this required (and still requires) the more difficult showing of complete diversity of citizenship between the parties under 28 U.S.C. § 1332 or that the state trade secret claim shares the same or similar operative facts with some other federal question claim allowing the federal court to exercise pendent jurisdiction under 28 U.S.C. § 1367.[44]

Another feature of the DTSA favoring trade secret plaintiffs is that it does not incorporate the requirement often applied in the course of state trade secret litigation that before commencing trade secrets discovery, the plaintiff must identify its relevant trade secrets with "reasonable particularity."[45] Requiring plaintiff to list the specific trade secrets that it is asserting prior to the parties engaging in discovery serves legitimate policies such as avoiding guesswork by defendant and the court about alleged trade secrets, allowing the court to set parameters on discovery and providing the defendants a fair opportunity to prepare their defense.[46] However, the requirement also creates logistical hurdles for the plaintiff and an opportunity for defendants to engage in motions practice that delays and sidetracks the disposition of the case on the merits.[47] In comparison, the DTSA, which does not impose the threshold determination, gives plaintiff a

---

44. *See id.* (citing Roy E. Hofer & Susan F. Gullotti, *Presenting the Trade Secret Owner's Case*, in PROTECTING TRADE SECRETS 1985, at 145, 159-61 (PLI Patents, Copyrights, Trademarks, & Literary Prop., Course Handbook Series No. 196, 1985)).

45. California has adopted legislation codifying this requirement. *See* Cal. Code Civ. Proc. § 2019.210 (in action alleging misappropriation of trade secret, before commencing discovery, party alleging misappropriation must identify trade secret with "reasonable particularity"). Courts in other states impose the requirement in the course of exercising their discretion to control trade secret discovery. *See, e.g.*, MSCI Inc. v. Jacob, 945 N.Y.S.2d 863, 865 (Sup. Ct. 2012) ("[T]he court is persuaded that the law requires that a trade secret plaintiff identify trade secrets with reasonable particularity early in the case.") (citing Xerox Corp. v. IBM Corp., 64 F.R.D. 367, 371 (S.D.N.Y. 1974)); Engelhard Corp. v. Savin Corp., 505 A.2d 30, 33 (Del. Ch. 1986) ("Where, as here, a plaintiff in a trade secret case seeks to discover the trade secrets and confidential proprietary information of its adversary, the plaintiff will normally be required first to identify with reasonable particularity the matter which it claims constitutes a trade secret, before it will be allowed (given a proper showing of need) to compel discovery of its adversary's trade secrets.")

46. *See* Computer Economics, Inc. v. Gartner Group, Inc., 50 F. Supp. 2d 980, 985 (S.D. Cal. 1999) (summarizing the purposes of the rule with citations to supporting authority).

47. *See* Advanced Modular Sputtering, Inc. v. Superior Court, 132 Cal. App. 4th 826, 831 (2005) (The court observed that there had been protracted briefing and argument by the parties regarding the sufficiency of plaintiff's thrice-amended trade secret complaint, concluding "[a]s a result, the parties have created a voluminous record, expended thousands of dollars on attorney fees and expert witnesses, and consumed considerable judicial resources *without ever even beginning to conduct discovery*") (emphasis added).

faster and easier path to discovery and injunctive relief—the primary sources of settlement leverage in a trade secret case.[48]

The DTSA also is expressly non-preemptive; it does not by its terms preempt or supersede common law state claims.[49] In contrast, states such as California have interpreted their versions of the UTSA as preempting or superseding non-contractual remedies that share a common nucleus of facts with a trade secret claim.[50] For example, claims of trespass to chattels,[51] unfair competition,[52] breach of fiduciary duty,[53] and interference with contract[54] have been held preempted by the California trade secret statute. Plaintiff trade secret owners could be highly motivated to bring suit under the DTSA, allowing them to bring a host of state law common claims heretofore deemed preempted under state court trade secret statutes.[55]

Unfortunately for the plaintiff employer convinced that filing under the DTSA is the way to go, there is little in the way of case precedent on the proof required to establish a federal claim for threatened misappropriation. Only a small number of decisions involving the DTSA have been issued since its enactment less than a year ago on May 11, 2016. And of this small available sample, only a limited number of the decisions granted early injunctive relief on a trade secret claim: *Engility Corp. v. Charles Aaron Daniels et al*.,[56] *Henry Schein, Inc. v. Jennifer Cook*,[57] *Earthbound Corp., et al. v.*

---

48. Warren Braunig & Andrea Nill Sanchez, *What the Defend Trade Secret Act Means for California*, THE RECORDER, July 18, 2016, at 9.

49. The DTSA does not "preempt any other provision of law." S. 1890, 114th Cong. § 2(f) (2016).

50. Angelica Textile Servs., Inc. v. Park, 220 Cal. App. 4th 495, 505-06 (2013).

51 NetApp, Inc. v. Nimble Storage, Inc., No. 13-05058, 2015 WL 400251, at *16 (N.D. Cal. Jan. 29, 2015).

52. SunPower Corp. v. SolarCity Corp., No. 12-00694, 2012 WL 6160472, at *16 (N.D. Cal. Dec. 11, 2012).

53. Mattel v. MGA Ent., Inc., 782 F. Supp. 2d 911, 989 (C.D. Cal. 2011).

54. K.C. Multimedia, Inc. v. Bank of Am. Tech. and Operations, Inc., 171 Cal. App. 4th 939, 960-61 (2009).

55. In addition to the features already discussed, the DTSA also provides that a trade secret owner can apply ex parte for a court order "providing for the seizure of property necessary to prevent the propagation or dissemination of the trade secret that is the subject of the action. *See* 18 U.S.C. § 1836(b)(2)(A)(i). This was a hotly contested provision and by its own terms is available only in "exceptional circumstances." *Id.* at (3)(A)(iii). So exceptional are the preconditions to obtaining this relief that it is the opinion of many commentators, present company included, that it will rarely, if ever, be awarded. Indeed, to-date there are no reported decisions discussing—let alone imposing—the ex parte seizure order.

56. Engility Corp. v. Charles Aaron Daniels et al., No. 16-2473, 2016 WL 7034976, at *14 (D. Colo. Dec. 2, 2016) (granting motion for preliminary injunction in part).

57. *Henry Schein, Inc*., 2016 WL 3418537, at *10-11 (granting motion for preliminary

MiTek USA, Inc.,[58] *OOO Brunswick Rail Mgmt. v. Sultanov,*[59] and *Prot. Techs., Inc. v. Ribler*.[60] It is difficult to discern trade secret rules and evidence specific to federal DTSA claims in four of these cases, *Engility Corp.*, *Henry Schein, Inc.*, *Earthbound Corp.*, and *Prot. Techs., Inc.*, because in each case the plaintiff also asserted state law trade secret claims and the court did not differentiate between state and federal trade secret law as the basis for its findings. The decisions in *Henry Schein, Inc.*, *Earthbound Corp.*, and *OOO Brunswick Rail Mgmt.* are also distinguished in that they involve actual as opposed to threatened misappropriation.[61]

Closest to the mark is *Engility Corp*., in which the federal court entered a preliminary injunction imposing a one-year ban on defendants competing with the plaintiff former employer based upon the court's finding that there was persuasive evidence that defendants "retain[_] some portion of [plaintiff's] trade secrets" and that there was evidence demonstrating "a propensity [on the part of defendants] for making surreptitious copies of the relevant data."[62] While *Engility* might provide at least one example of proofs sufficient to show threatened misappropriation under the DTSA, its precedential

---

injunction in part); *see also* Henry Schein, Inc. v. Jennifer Cook, 191 F. Supp. 3d 1072, 1079-80 (N.D. Cal. June 10, 2016) (granting application for temporary restraining order in part).

58. Earthbound Corp., et al. v. MiTek USA, Inc., No. 16-1150, 2016 WL 4418013, at *11-12 (W.D. Wash. Aug. 19, 2016) (granting application for temporary restraining order).

59. OOO Brunswick Rail Mgmt. v. Sultanov, No. 5:17-CV-00017-EJD, 2017 WL 67119, at *3 (N.D. Cal. Jan. 6, 2017) (granting application for temporary restraining order).

60. Prot. Techs., Inc. v. Ribler, No. 317CV00144LRHWGC, 2017 WL 923912, at *1 (D. Nev. Mar. 8, 2017) (granting application for temporary restraining order).

61. *See Henry Schein, Inc.*, 191 F. Supp. 3d at 1077 (the court determined that plaintiff former employer was likely to succeed on allegations "that Cook has *already misappropriated* HSI's customer information and south to solicit and divert customers") (emphasis added); *Earthbound Corp.*, 2016 WL 4418013, at *10 (the court found that "there is strong circumstantial evidence *that Defendants misappropriated the trade secrets* in question," citing, among other things, evidence that that defendants, while still employed with plaintiff, established relationships with a primary competitor and shared plaintiff's confidential information with this competitor) (emphasis added); *OOO Brunswick Rail Mgmt.*, 2017 WL 67119, at *1 ("Brunswick's evidence shows that Sultanov and Ostling improperly disseminated confidential information—e.g., by emailing documents to their personal accounts *and then disclosing this information to third parties*") (emphasis added).

62. *Engility Corp*., 2016 WL 7034976, at *11. *See also Prot. Techs., Inc.*, 2017 WL 923912, at *1 (the court entered a TRO requiring the departing employee to return confidential information and refrain from soliciting prior employer's customers where there was no apparent evidence of actual misappropriation – the employee had downloaded confidential information to a private drive and emailed the information from his company email account to himself; however, given the sparse nature of the evidence taken by the court on what was an *ex parte* TRO petition, it was not clear whether the employee had acted without authorization or improperly disclosed or used the information).

strength is diluted by ambiguity whether the court deemed the conduct at issue actual or threatened misappropriation (in addition to the previously-mentioned absence of any discussion whether the relief awarded was based on either state or federal trade secret laws).

The lack of federal precedent is explained not just by the recent enactment of the DTSA, but also because the DTSA, by its express terms, is limited to an "act" of misappropriation that "occurs on or after the date of enactment."[63] This is not to say the plaintiff employer does not have options pending development of DTSA precedent. As discussed in the following sections, certain state trade secret jurisdictions, most notably California, are based on the same pro-employee mobility policy as the DTSA. The plaintiff employer can reasonably look to these like-minded state jurisdictions and their court decision to predict the level of proof required to establish threatened misappropriation under the DTSA.

IV. PROOF OF THREATENED MISAPPROPRIATION UNDER THE DTSA WILL LIKELY FOLLOW CALIFORNIA DECISIONS

A. California Is Pro-Employee Mobility and Rejects the "Inevitable Disclosure Doctrine"

The inevitable disclosure doctrine permits a plaintiff to prove trade secret misappropriation by showing that the defendant's new employment will inevitably lead to reliance on plaintiff's trade secrets.[64] Injunctions granted on the basis of inevitable disclosure presuppose that "the employee will necessarily rely—consciously or unconsciously—upon knowledge of the former employer's trade secrets in performing his or her new job duties."[65] In other words, the

---

63. Section 2(e) of the DTSA provides in pertinent part: "(e) EFFECTIVE DATE.--The amendments made by this section shall apply with respect to any misappropriation of a trade secret . . . for which any act occurs on or after the date of the enactment of this Act." DTSA § 2(e). *See* Adams Arms, LLC, No. 16-1503, 2016 WL 5391394, at *6 (M.D. Fla. Sept. 27, 2016) ("the Court finds that [plaintiff] may state a plausible claim for relief, if [plaintiff] sufficiently alleges a prohibited 'act' occurring after May 11, 2016."). It is ambiguous whether the DTSA applies to misappropriation activity that began before the enactment of the DTSA but continues thereafter; Congress omitted from the DTSA the provision in the UTSA that it does not apply to continuing activity that commenced prior to the effective date of the UTSA, thus leaving the door open to infer that the DTSA would apply in this situation. *Id.* Suffice it to say that at this early stage in the life of the DTSA the potential for jurisdictional challenges to claims directed to pre- and post- enactment continuing activity may have had the temporary effect of dissuading parties from filing claims under the DTSA—as time passes, this particular risk will become moot.

64. PepsiCo, Inc. v. Redmond, 54 F.3d 1262, 1269 (7th Cir. 1995).

65. *Id.*

employee is enjoined from taking the new job just because of what he or she knows.

California, however, rejects the inevitable disclosure doctrine. The California appellate court in *Whyte v. Schlage Lock Co.*[66] rejected the argument that the inevitable disclosure doctrine was an alternative to proving actual or threatened misappropriation. The gist of the court's rationale was that application of the doctrine results in the after-the-fact imposition by the court of a covenant not to compete that unduly infringes California's strong policies favoring employee mobility:

> The decisions rejecting the inevitable disclosure doctrine correctly balance competing public policies of employee mobility and protection of trade secrets. The inevitable disclosure doctrine permits an employer to enjoin the former employee without proof of the employee's actual or threatened use of trade secrets based upon an inference (based in turn upon circumstantial evidence) that the employee inevitably will use his or her knowledge of those trade secrets in the new employment. The result is not merely an injunction against the use of trade secrets, but an injunction restricting employment.[67]
>
> Business and Professions Code section 16600 generally prohibits covenants not to compete, and California public policy strongly favors employee mobility. Business and Professions Code section 16600 protects a person's right to "follow any of the common occupations of life" and to pursue the "'business or profession he may choose.'" We agree the doctrine of inevitable disclosure "creates a de facto covenant not to compete" and "runs[s] counter to the strong public policy in California favoring employee mobility."[68]

The court in *Whyte* acknowledged that California law also protects trade secrets and that a non-compete agreement may be enforceable notwithstanding the general prohibition of such covenants where necessary to protect the employer's trade secrets. But in the court's view this does not save the inevitable disclosure doctrine:

> The chief ill in the covenant not to compete imposed by the inevitable disclosure doctrine is its after-the-fact nature: The covenant is imposed *after* the employment contract is made and therefore alters the employment relationship without the employee's consent. When, as here, a confidentiality agreement is in place, the inevitable disclosure doctrine "in effect convert[s] the confidentiality agreement into such a covenant [not to compete]." Or, as another federal court put it, "a court should not allow a plaintiff to use inevitable disclosure as an after-the-fact

65. Whyte v. Schlage Lock Co., 101 Cal. App. 4th 1443, 1458-59 (2002).

66. *Id.* at 1461-62.

67. *Id*.

68. *Id*. at 1462 (internal citations omitted).

> noncompete agreement to enjoin an employee from working for the employer of this or her choice."[69]

California's rejection of inevitable disclosure is often described as the minority position.[70] It is difficult to discern with any degree of precision the jurisdictions that are in the majority or minority on this question due to the treatment of inevitable disclosure in some jurisdictions as one form of threatened misappropriation,[71] while others, such as California,[72] view threatened misappropriation as a separate alternative to actual or threatened misappropriation. In addition, within the so-called "majority jurisdictions" that reject inevitable disclosure, there is significant variation in their respective requirements for applying the doctrine, creating a spectrum of cases imposing proof requirements that blur the lines demarcating where inevitable disclosure ends and threatened misappropriation begins.[73] There also are states such as Florida, Iowa, South Carolina and Wisconsin whose highest courts have not addressed inevitable disclosure as a means of proving misappropriation.[74] What can be

---

69. *Id*. at 1462-63 (internal citations omitted). *See also* Avery Dennison Corp. v. Juhasz, 924 F. Supp. 2d 893, 901 (N.D. Ohio 2013) (applying California law) ("The doctrine of inevitable disclosure is not the law in California.") (citing *FLIR Systems, Inc*., 174 Cal. App. 4th at1277).

70. *See* Passi, *supra* note 10, at 930, 933.

71. *See, e.g.*, Interbake Foods, LLC v. Tomasiello, 461 F. Supp. 2d 943, 973 (N.D. Iowa 2006) (Interpreting Iowa law, the court stated "the inevitable disclosure doctrine is just one way of showing a threatened disclosure in cases where additional evidence showing the existence of a substantial threat of impending injury is unavailable to the movant.").

72. *See Cent. Valley Gen. Hosp.,* 162 Cal. App. 4th at 525.

73. *See* Passi, *supra* note 10, at 930 (The commentator observes that "the majority of states, recognize this doctrine, albeit with varying understandings of 'inevitability.'"); *see also* Dearborn v. Everett J. Prescott, Inc., 486 F. Supp. 2d 802, 820 (S.D. Ind. 2007) (court declined to award injunction based on inevitable disclosure doctrine due to lack of evidence of bad faith); Tactica Intern., Inc. v. Atlantic Horizon Intern., Inc., 154 F. Supp. 2d 586, 608 (S.D. N.Y. 2001) (applying New York law, conditioned application of inevitable disclosure doctrine on whether the departing employee had sufficient seniority); H & R Block Eastern Tax Services, Inc. Enchura, 122 F. Supp. 2d 1067, 1075 (W.D. Mo. 2001) (applying Missouri law, required that departing employee actually participated in the creation of the trade secret as compared to simply having knowledge of it.).

74. *See* Clorox Corp. v. S.C. Johnson & Son, Inc., 627 F. Supp. 2d 954, 967 (E.D. Wisc. 2009) ("The parties have yet to cite a Wisconsin court that has addressed whether the inevitable disclosure theory is viable under Wisconsin's trade secret laws."); *Interbake Food, LLC*, 461 F. Supp. 2d at 957 ("Although the Iowa Supreme Court has not affirmatively ruled on the viability of such a doctrine in Iowa, at least one federal court in Iowa has determined that the Iowa Trade Secrets Act provides protection from the inevitable disclosure of trade secrets."); Del Monte Fresh Produce Co. v. Dole Food Co., 148 F. Supp. 2d 1326, 1337 (S.D. Fla. 2001) (district court refused to apply inevitable disclosure doctrine because the Florida state courts had neither expressly adopted or rejected the doctrine); Nucor Corp. v. Bell, No. 06-02972, 2008 WL 9894350, at *15 (D.S.C. Mar. 14, 2008) (in the course of choice of law analysis, district court

said is that California is at the forefront of the very few state jurisdictions that have rejected inevitable disclosure—the others being Maryland and Virginia.[75]

B. The Defend Trade Secrets Act Is Also Pro-Employee Mobility and Rejects "Inevitable Disclosure"

Coming into the recent Senate Judiciary Committee hearings, the DTSA was amended to close the door on inevitable disclosure in much the same fashion as has been done in California. Senator Dianne Feinstein of California successfully proposed the following amendments expressly confirming that threatened misappropriation may not be established merely by the importance of the information that someone knows. The relevant portions of her amendment are emphasized below:

> (3) REMEDIES.—In a civil action brought under this subsection with respect to the misappropriation of a trade secret, a court may—
>
> ***grant an injunction*** –
>
> ***To prevent any*** actual or ***threatened misappropriation*** described in paragraph (1) on such terms as the court deems reasonable, provided the order does 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***; or…" [76]

Lest anyone not appreciate that these amendments adopt California's robust policy favoring employee mobility (i.e., the policy compelling California courts to reject inevitable disclosure to being with), Senator John Cornyn of Texas added an amendment expressly incorporating the general prohibition in California and other like-minded states against restrictive employment covenants and similar restraints of trade:

> (3) REMEDIES.—In a civil action brought under this subsection with

---

determined that "South Carolina has not addressed the issue.")

75. LeJeune v. Coin Acceptors, Inc., 381 Md. 288, 322 (2004) (referring to the California Supreme Court's decision in *Whyte*, the Maryland appeals court said "[w]e find this reasoning persuasive, especially as applied to the circumstances in the case before us. Maryland has a policy in favor of employee mobility similar to that of California. . . . For these reasons, we conclude that the theory of "inevitable disclosure" cannot serve as a basis for granting a plaintiff injunctive relief under MUTSA."); Gov't Technology Services, Inc. v. IntelliSys Tech. Corp., No. 160265, 1999 WL 1499548, at *1 (Va. Cir. Oct. 20, 1999) ("Under the [Virginia Trade Secrets Act], only actual or threatened misappropriation may be enjoined. Virginia does not recognize the inevitable disclosure doctrine.").

76. DTSA, *supra* note 2.

> respect to the misappropriation of a trade secret, a court may—
>
> grant an injunction—
>
> to prevent any actual or threatened misappropriation described in paragraph (1) on such terms as the court deems reasonable provided the order does 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; or
>
> ***otherwise conflict with an applicable State law prohibiting restraints on the practice of a lawful profession, trade, or business***;" [77]

The district court's recent decision in *Engility*, discussed above, implicitly interprets these provisions of the DTSA as rejecting inevitable disclosure. There, the court said that it could not enjoin the defendant from performing work for the former employer's customer under the DTSA based solely on the defendant's alleged knowledge of sensitive trade secrets.[78] The court stated in the pertinent part:

> Under the DTSA, the Court cannot grant an injunction that "prevent[s] a person from entering into an employment relationship," and the Court can only place conditions on employment "based on evidence of threatened misappropriation and not merely on the information the person knows."[79]

Engility's implicit interpretation of the DTSA as rejecting inevitable disclosure in favor of employee mobility is supported by the great weight of DTSA commentary.[80]

---

77. *Id*. (quoting 18 U.S.C. § 1836(b)(3)(A)(i)(I)).

78. *Engility*, 2016 WL 7034976, at *10.

79. *Id.*

80. *See, e.g.*, Lily Li & Andrea W. Paris, *Help! What Are My (Immediate) Defenses to A Federal Trade Secret Claim?*, ORANGE CTY. LAWYER MAGAZINE, Sept. 2016, at 52 ("The DTSA's rejection of the inevitable disclosure doctrine, which prevents an employee from working for a competitor merely because disclosure of trade secrets is a likely possibility, is notable."); Bailey King & Whit Pierce, *The Defend Trade Secrets Act of 2016 Is Here, and It's a Big Deal*, 58 DRI'S FOR DEF. 42 (July 2016) ("The DTSA does away with this line of attack, expressly providing that an injunction cannot 'prevent a person from entering into an employment relationship.' It further adds that any 'conditions placed on such employment shall be based on evidence of threatened misappropriation and not merely on the information the person knows.'" This provision should negate any 'inevitable disclosure' argument that a plaintiff attempts to make against a defendant employee."); ECONOMIC ESPIONAGE ACT, U.S.C. §1831 (2013) ("The Act also rejects application of the 'inevitable disclosure' doctrine."); Raymond T. Nimmer, LAW OF COMPUTER TECHNOLOGY § 3:2.30 (2016) ("The first of these exclusions apparently rejects the 'inevitable disclosure' rule, which courts in some states have used in some cases to grant injunctions against an employee moving to another company on the basis that the employee would inevitably disclose secrets of the prior employer. The DTSA balances this issue in favor of the employee's right of mobility."); Joseph D. Mornin, *What You Need To Know About the Defend Trade Secrets Act*, 28 INTELL. PROP. & TECH. L.J. 20 (2008) ("The DTSA requires "evidence of threatened misappropriation," that is, it requires an employer

C. Threatened Misappropriation Under the DTSA Will Follow California Precedent

California decisions, at least for now, provide the go-to precedent for federal courts to use when deciding what proof is required to show an actionable threat of misappropriation under the DTSA. Currently, there is limited to no federal court precedent on the question.[81] Faced with the same lack of federal precedent on the meaning of "trade secret" under the DTSA, federal courts have relied upon state court precedent to define this term, suggesting they will do the same thing regarding the standards for defining and proving "threatened" misappropriation under the DTSA.[82] They will not rely upon state court precedent generally, however, because only California and a couple other like-minded states share the DTSA's goal of protecting employee mobility (and the consequent rejection of enjoining employment based upon inevitable disclosure doctrines).[83] Moreover, looking to California precedent for guidance on the application of the DTSA is consistent with the DTSA mandate to provide a uniform body of federal trade secret law applied consistently across the country.[84] Uniformity cannot be achieved if

---

to show more than that a departing employee knows sensitive information. In this respect, state law will continue to play an important role in trade secret litigation.").

81. *See supra* Part III.

82. *See, e.g.*, *Henry Schein*, 2016 WL 3418537, at *4 (the court noted that the DTSA and CUTSA included similar definitions of "trade secret" and proceeded to apply California decisions interpreting the term); *Earthbound Corp*., 2016 WL 4418013, at *9 ("In this case, for the reasons discussed by Plaintiffs, the Court agrees that detailed information about Earthbound's current and prospective customers, pending projects, bids, pricing, product design, and other elements of its business constitute trade secrets under the UTSA. . . . The same evidence demonstrates a likelihood of success on the merits on Plaintiffs' claim for violation of the Economic Espionage Act, as amended by the Defend Trade Secrets Act, 18 U.S.C. § 1831 et seq. ("EEA").); Berkeley Risk Adm'rs Co. v. Accident Fund Holdings, Inc., No. 16-2671, 2016 WL 4472943, at *2 (D. Minn. Aug. 24, 2016) ("The definition of 'trade secret' in the federal statute and MUTSA are substantially similar. *Compare* 28 U.S.C. § 1839(3) *with* MINN. STAT. § 325C.01 Subd. 5. Therefore, the court will construe them as coextensive for purposes of this case.").

83. Practically speaking, while precedent from Maryland and Virginia—the other jurisdictions rejecting inevitable disclosure—is also relevant, the focus is on California precedent because it is a more highly-developed decisional law regarding threatened misappropriation in the context of rejecting inevitable disclosure.

84. The UTSA failed to achieve its primary objective of correcting the uneven and highly varied state court trade secret laws that pre-dated its enactment. In the course of adopting the UTSA, states often departed from the official text and/or there was unduly high variation across courts regarding the standards governing the application of the UTSA. Federal lawmakers believed the country would benefit from a federal trade secret law uniformly applied across the country, and enacted the DTSA with this objective in mind. *See* Sen. Rep. No. 114-220, 114th Cong., 2d Sess. (2016).

federal courts draw indiscriminately from jurisdictions recognizing inevitable disclosure as well as from those that do not in the course of determining threatened misappropriation under the DTSA.

Pending the development over time of federal court precedent on the issue, California cases are the best resource for predicting what evidence is required to make a DTSA threatened misappropriation case. The following section gleans from relevant California precedent the proofs most likely to make a federal case for the hypothetical introduced in Section I.

V. PROVING THREATENED MISAPPROPRIATION IN CALIFORNIA

A. The Hypothetical Demonstrates the Employer's Concern that Disclosure of its Trade Secrets Is Inevitable

Returning to our hypothetical, your CEO has asked you, the manager of the affected business unit, for advice whether to pursue formal court action against the recently departed technical director. You've got a couple hours before the CEO wants to meet on the subject. You crack open your laptop and try to organize your thoughts. *You type the following notes:*

> What we know about ex-technical director of our LiDAR unit:
>
> - Insider
>
> - Senior level position provided broad access to business strategy
>
> - High level technical knowledge
>
> - Access to, exposed to, and helped develop, confidential information and trade secrets
>
> - Going to what (we believe) is a direct competitor
>
> - Competitor greatly accelerates development if he shares what he knows or is in his possession
>
> - Says he has returned all company devices
>
> - Acknowledges confidentiality agreement, says he has complied ("kept nothing," he says)
>
> + BIG fear is that he is still in possession of highly-sensitive company trade secrets and proprietary information, most importantly LiDAR IP
>
> ? But . . . we do not have any evidence right now that he has used or disclosed any of our this IP

On behalf of the company, you send a quick email to company counsel soliciting their advice. In your email, you share your thoughts on the technical director's departure. You also ask whether the company should make a claim under the new federal trade secret law based on your understanding that the federal law may be more favorable to parties asserting trade secret rights and that it also may be less costly as compared to litigating under the state court trade secret law. *Company counsel responds by email*:

> Based on what you have told me so far, we do not have enough evidence - whether we bring claim under California or federal law, we can't rely on argument that theft is inevitable (which is what we could argue based on what you've given me).

B. But Additional Evidence Beyond Inevitable Disclosure Is Needed To Establish Threatened Misappropriation

Your quick reply to counsel:

Ok, so what more do I need?

The question, in other words, is given that inevitable disclosure is not a recognized means of establishing a threat of misappropriation, what evidence will be enough to establish such a threat? This question was addressed in the California decision *Central Valley General Hospital v. Smith,*[85] which came before the court as an appeal of an injunction intended to protect against the improper use and disclosure of trade secrets. The appeal required the court to resolve the question whether the California Supreme Court's earlier decision in *Whyte v. Schlage Lock Co.* rejecting inevitable disclosure meant that an injunction may not be based on threatened misappropriation.[86] The court rejected this argument on the grounds that threatened misappropriation is properly conceptualized as a separate and alternate theory for obtaining relief for trade secret misappropriation.[87] But this begged the question how the proof of threatened misappropriation differed from inevitable disclosure.

In response, the court in *Central Valley* described three "variations" or fact patterns establishing threatened misappropriation of trade secrets. The first involves retention of the trade secrets by a departing employee who has misused some of the trade secrets in the

85. *Cent. Valley Gen. Hosp.*, 162 Cal. App. 4th at 526-528.

86. *Id.* at 524.

87. *Id*. at 525.

past.[88] The court cited to *ReadyLink Healthcare v. Cotton*[89] as an example.[90] In *ReadyLink*, the departing employee had been caught attempting to steal records regarding his employer's finances, clients, employee contacts, payroll practices and business methodology.[91] The employee had attempted to use this information both before and after his employment to solicit clients and otherwise set up a competing business.[92] Even though the employee no longer worked for a competitor at the time the injunction was issued, the court in *ReadyLink* concluded that "there remained an imminent threat of him using the trade secret information to solicit ReadyLink's employees and customers."[93]

The second variant described by *Central Valley* involves continued retention of the trade secrets under circumstances establishing that the departing employee intends to use or disclose them in the future.[94] The injunction entered in *Technical Industries, Inc. v. Banks*[95] was cited as an example.[96] In *Technical Industries*, the employer's trade secrets consisted of a proprietary method of inspecting oil field pipes to derive unique data.[97] The departing employee said he intended to use a different software program to derive similar data, but his testimony convinced the court that he could not act as proposed without using elements of his employer's proprietary pipe inspection system.[98] Accordingly, the court found there was a threatened misappropriation based upon circumstances reflecting the intent to use at least some of the trade secrets in the future.[99]

The third variant described by *Central Valley* is that a threatened misappropriation occurs where "a defendant possesses trade secrets and wrongly refuses to return the trade secrets after a demand for

88. *Id.* at 527.
89. *ReadyLink Healthcare*, 126 Cal. App. 4th at 1006.
90. *Cent. Valley Gen. Hosp.*, 162 Cal. App. 4th at 527.
91. *Read Link Healthcare*, 126 Cal. App. 4th at 1013.
92. *Id.*
93. *Id*. at 1101.
94. *Cent. Valley Gen. Hosp*., 162 Cal. App. 4th at 528.
95. Technical Industries, Inc. v. Banks, 419 F. Supp. 2d. 903, 913 (W.D. La. 2006).
96. *Cent. Valley Gen. Hosp.*, 162 Cal. App. 4th at 528 (citing Technical Industries, Inc. v. Banks, 419 F. Supp. 2d. at 913 (entering preliminary injunction enjoining threatened trade secret misappropriation)).
97. *Technical Industries*, 419 F. Supp. 2d at 911.
98. *Id*. at 913.
99. *Id*.

their return has been made."[100] The court expressly distinguished these circumstances from "a plaintiff merely show[ing] a defendant is in possession of trade secrets."[101] In *FLIR Systems, Inc. v. Parrish*,[102] the court relied upon this same distinction in finding that there was no threatened misappropriation of trade secrets by a departing engineer who had downloaded his employer's database onto a personal hard drive and retained this information following his employment.[103] In the eyes of the court, the engineer had a reasonable explanation for downloading the data (due to slow computer network he needed to work from home), plus the engineer destroyed the hard drive prior to filing of the lawsuit.[104] There was no evidence that the engineer had accessed or used the data in connection with his new business venture before the drive was destroyed.[105] Accordingly, nothing more than mere possession of a trade secret by a departing employee had been shown, and this was not sufficient to establish threatened trade secret misappropriation.[106] The court said that to hold otherwise would mean "an employer could bring a trade secret action after an employee downloads a company document and deletes the document from his or her laptop computer at home. A similar action could be brought where company messages are left on the employee's e-mail or phone answering machine and deleted after the employee changes jobs."[107]

Central Valley, through these "variants," essentially distinguishes threatened misappropriation as requiring evidence of *bad behavior* by the departing employee, separate and additional to anything they may *know*.[108] The court in *FLIR Systems* cited *Central Valley* as support for construing "threatened misappropriation" as "a threat by a defendant to misuse trade secrets, *manifested by words or conduct*, where the evidence indicates imminent misuse."[109] Mr.

---

100. *Cent. Valley Gen. Hosp.*, 162 Cal. App. 4th at 528.

101. *Id*. at 528-29.

102. *FLIR Systems Inc.*, 174 Cal. App. 4th at 1279.

103. *Id.* at 1278.

104. *Id*.

105. *Id*. at 1279.

106. *Id*.

107. *Id*.

108. *Cent. Valley Gen. Hosp*., 162 Cal. App. 4th at 527-528.

109. *FLIR Systems*, 174 Cal. App. 4th at 1279 (citing with approval the trial court's construction of the meaning of "threatened misappropriation" in § 3425.2 of California's version of the UTSA) (emphasis added); *see also Edifecs Inc*., 756 F. Supp. 2d at 1320 (applying California law) ("In California, 'threatened misappropriation' means a threat by a defendant to misuse trade secrets, manifested by words or conduct, where the evidence indicates imminent misuse." (citing *Cent. Valley Gen. Hosp.*, 162 Cal. App. 4th at 527).

Pooley further explains in a recent post that the evidence demarcating actionable threats from nonactionable inevitable disclosure is that the former "focus[es] on the employee's behavior" and whether this behavior shows the employee "can't be trusted to honor the integrity" of the previous employer's trade secrets, while the latter is "established merely by the importance of the information that someone knows."[110]

Decisions in which the courts have entered preliminary injunctions based upon a finding of threatened misappropriation under California law provide further insight into the different types of "words or conduct" that can be used to make such a claim.

In *Wyndam Resort Dev. Corp. v. Bingham*,[111] a former employee of a company that managed timeshare properties attempted to sell to a competing timeshare company the names of 40,000 timeshare owners whose properties were managed by his former employer. The court entered a preliminary injunction enjoining further solicitations based upon the finding that this conduct was actionable threatened misappropriation.[112] The customer information at issue was deemed a protectable trade secret.[113] The former employee was also contractually obligated to maintain the confidentiality of this information.[114]

In *Shippers v. Fontenot*,[115] the employee's suspicious conduct leading up to departure "constitute[d] strong circumstantial evidence that Defendants are in possession of Shippers' confidential information and that they are likely to use that information to lure customers away from Shippers."[116] The suspicious pre-departure included the employee's "refus[al] to disclose to Shippers that he was leaving his employment to join AtMet, a direct competitor, instead claiming that he had no immediate plans for new employment and

110. Dennis Crouch, *What You Need to Know About the Amended Defend Trade Secrets Act,* PATENTLY-O BLOG (Jan. 31, 2016), http://bit.do/CrouchAmendTradeSecretsAct.

111. Wyndham Resort Dev. Corp. v. Bingham, No. 10-01556, 2010 WL 2740158, at *6 (E.D. Cal. July 9, 2010).

112. *Id*. at *5-6 ("Bingham's attempt to sell Plaintiffs' customer list to one of Plaintiffs' competitors constitutes threatened misappropriation since Bingham attempted to disclose Plaintiffs' customer list when he was contractually obligated maintain the confidentiality of such information. Plaintiffs, therefore, have shown that they are likely to prevail on their claim that Bingham threatened to misappropriate their trade secrets").

113. *Id.* at *5.

114. *Id.*

115. Shippers, a Division of Illinois Tool Works, Inc. v. Fontenot, No. 13-1349, 2013 WL 12092056, at *4-5 (S.D. Cal. Sept. 23, 2013).

116. *Id*. at *5.

that he expected to take some time off after his departure."[117] Investigation revealed several extraordinary activities over the month leading up to departure. The court stated in pertinent part:

> Fontenot then spent his final month at Shippers rummaging through Prairie Tools, Shippers' proprietary customer database, to obtain sensitive information regarding Shippers' clients, including contact persons, "ship to" names, "bill to" names, addresses, telephone numbers, and pricing and order history. Fontenot conducted 494 inquiries in Prairie Tools during his last month, a vast increase from his regular use of the database. . . . Indeed, Fontenot's searches included 285 pricing queries, more than twice as many as conducted by any other Shippers sales representative during the same time period. . . . Most suspiciously, the overwhelming majority of Fontenot's searches targeted customers located outside of his sales territory.[118]

The defendant's business managers and IT staff testified that the employee did not need to access and use internal databases as had in fact occurred in order to fulfill his job duties, thus contradicting the employee's explanation that his search activity had a legitimate business motivation.[119]

In *Lighthouse Worldwide Sols., Inc. v. Giandomencio*, a senior executive who set up a competing business within approximately thirty days of his departure was enjoined from soliciting customers and competing for certain business.[120] Following his termination, the executive retained a particle counting device whose design and specifications were protected as trade secrets and computer hard drives that contained confidential information.[121] Shortly after his departure, the executive published a press release in which he announced his new company and offered for sale a very similar product the 3010R, which, as advertised, appeared identical to the Remote 3010 sold by the former employer. "A comparison of the data sheets for the Remote 3010 and the 3010R showed that the descriptions of eleven of twelve '[f]eatures,' eight of eight '[b]enefits,' and eleven of twelve '[a]pplications' were identical."[122]

---

117. *Id*.

118. *Id*. (citations to trial record omitted).

119. *Id*.

120. Lighthouse Worldwide Solutions, Inc. v. Giandomencio, No. 06-7706, 2008 WL 256974, at *3 (Cal. Ct. App. Jan. 31, 2008) (while this is a nonpublished opinion whose citation is restricted under Cal. Rules of Court, Rule 8.1115, the facts underpinning the court's entry of injunctive relief may be helpful to the practitioner evaluating the strength of a possible claim for threatened misappropriation.).

121. *Id*.

122. *Id*. at *8.

"Some Lighthouse customers expressed confusion regarding the relationship between Lighthouse and Adams Instruments and whether Adams Instruments released the 3010R in collaboration with Lighthouse."[123] The combination of the executive having taken confidential information directly relevant to his new, competing business, that he was able to offer a competing product within a very short time of departure, and the solicitation of his former employer's customers under circumstances engendering confusion regarding the source the new company's products, demonstrated substantial evidence of a threatened misappropriation.[124]

Fitspot Ventures, LLC v. Bier[125] involved the departure of the lead coding engineer from a technology company developing a mobile application. The engineer used subscription based "cloud platforms" to house and develop the source code on which he was working. The plaintiff company's customer data and other essential proprietary applications code were stored on these platforms as well. Upon his termination, the engineer, contrary to company instructions, deleted data from his company provided computer and network accounts.[126] In addition, the engineer accessed and disabled the links between the "cloud platforms" and the company's network, effectively cutting off the company from its customers and the ability to manage their accounts.[127] Forensic analysis revealed that the engineer had downloaded company data onto a personal hard drive prior to departure.[128] In addition, the engineer took a position with another technology company that potentially benefitted from the on-demand and real time functions of the former employer's source code.[129] After considering these circumstances, the court determined that the customer information and source code were protectable as trade secrets and that the engineer's conduct demonstrated at least threatened if not actual misappropriation.[130] Based on these findings, the court entered a temporary restraining order prohibiting the disclosure and use of all customer data and source code, the return of all access codes, the return of all data previously deleted from the

123. *Id*.

124. *Id*.

125. Fitspot Ventures, LLC v. Bier, No. 15-06454, 2015 WL 5145513, at *3 (C.D. Cal. Sept. 1, 2015).

126. *Id*.

127. *Id*.

128. *Id*.

129. *Id*.

130. *Id*. at *5.

employee's laptop, reestablishing links with the cloud-based development platforms and prohibiting the employee from using or disclosing the customer information and source code.[131]

C. Some Practical Guidelines for Determining Whether There Is Sufficient Proof of Threatened Misappropriation

It's time for your meeting with the CEO, and as you push back from your computer *the following email arrives from counsel*:

> You've asked:
>
> - Ok, so what more do I need?
>
> The answer, based on California trade secret cases, is that the following types of misconduct by a departing employee, either separately or in some combination, give the company a high likelihood of success of showing threatened misappropriation under the DTSA (the new federal law):
>
> ***
>
> Unusual or excessive transfers of company data to personal devices, personal email or personal cloud-based storage accounts
>
> ***
>
> Previously tried to steal IP and use it to set up competing business and has retained possession of key business and customer information
>
> ***
>
> Retained data on personal devices or personal storage accounts, and, following departure, failed to delete it
>
> ***
>
> Retained data following departure and there is evidence that this data was improperly accessed or copied before it was deleted
>
> ***
>
> Retained data and expressed intent to take action that would require use or disclosure of trade secrets
>
> ***
>
> Former employee has approached competitors and offered to share confidential information
>
> ***

131. *Fitspot Ventures*, 2015 WL 5145513 at *6.

> Fails to acknowledge leaving to take employment with competitor, i.e., they are not forthcoming about taking employment with competitor
>
> ***
>
> Excessive use and downloading of information from proprietary databases leading up to departure
>
> ***
>
> Accesses proprietary company databases without any legitimate business motivation for doing so
>
> ***
>
> Sets up competing business offering same or similar products to previous employer's products having design and specifications protected as trade secrets
>
> ***
>
> Unlikely that competing business could have been established so quickly without using prior employer's confidential information and trade secrets
>
> ***
>
> Unfair solicitation of prior employer's customers via misleading statements on web site and press releases
>
> ***
>
> Deleting data from company devices or network files contrary to preservation protocols
>
> ***
>
> Disabling and withholding access codes and passwords to company accounts containing proprietary data
>
> ***

It is now twenty-four hours after your meeting with the CEO, who encouraged you to conduct an expedited investigation whether any of the guidelines supplied by counsel might be applicable to the departure of your engineer. You've since met with other business managers, as well as the personnel responsible for IT, Security and HR functions within the company. Your email to company counsel sums up where things stand, most notably the facts that you believe provide a ***high likelihood of success*** on a claim against your technical director for ***threatened misappropriation*** of trade secrets. *Your email concludes, as follows:*

> Forensic analysis of returned devices shows significant deletions of data as well as transfer to personal email and cloud accounts. These deletions are contrary to

> instructions given to him at exit interview. No legitimate business motivation for this conduct. Highly likely this employee is still in possession of confidential data and trade secrets. Particularly suspicious is installation of applications on his laptop that are intended to mask deletion and downloads from his computer.
>
> Called the employee earlier today and demanded return of any data that he has retained. He did not deny that he was still in possession of the data. Refused to come in or commit to time to return anything. Said he would get back to me. His new employer issued a press release this morning that its first project is a self-driving application employing LiDAR technology that we have had in highly confidential development for past 9 months—are they using our IP to get head start? *I know we don't have evidence the employee is using or has disclosed our IP, but CEO says* ***we're authorized to seek immediate injunctive relief to address threat that a theft has occurred***. Next steps?

VI. CONCLUSION

The great majority of trade secret theft is committed by insiders who depart to take positions in competitive businesses. Typically, as of the time of the departure, there is a significant threat of misappropriation, but there is no evidence of actual use or disclosure of the trade secrets. Injunctive relief is available for both threatened and actual misappropriation under state trade secret laws as well as the new federal law, the DTSA.

There are advantages to the former employer who wants to assert a claim for threatened misappropriation of filing under the DTSA. However, there is little federal precedent on the proofs required to make such a claim, creating uncertainty and increasing the risk of an expensive misjudgment about the strength of the case. The solution is to refer to cases applying California trade secret law on threatened misappropriation to predict the proofs required on the same claim under the DTSA. This makes sense because the DTSA shares with California a pro-employee mobility philosophy that rejects inevitable disclosure as a means of establishing an actionable misappropriation claim.

California cases differentiate claims of threatened misappropriation from claims of "inevitable disclosure" based on the former requiring proof of words or conduct manifesting a threat of imminent misuse of trade secrets as compared to the latter's inference

merely from what is known that a threat may exist. Employers holding trade secrets and proprietary information, their former employees, business partners and contractors, and counsel representing any of these persons or parties, can glean from these cases specific and practical guidelines for evaluating whether the evidence is sufficient to obtain an injunction enjoining threatened misappropriation under the DTSA. These guidelines better inform the determination whether a former employer seeking to prevent an insider from stealing its IP has what it takes to "make a federal case out of it."