

# INTENTIONALITY IN TRADE SECRET LAW

*Charles Tait Graves*<sup>†</sup>

## ABSTRACT

Trade secret law places more scrutiny on a party's intent—what it was thinking, what it considered, or what it should have considered—than other categories of intellectual property law. At inflection points across a range of possible disputes, the law inquires into the mindset of one party or the other. Embedded in the federal and state statutes is a legislative intent that absent wrongful intent—or at least constructive knowledge—there can be no misappropriation.

This focus on a party's state of mind comes as no surprise. Because trade secret rights are not registered with any government agency, there is no formal means by which they can be identified in advance. One encounters a trade secret in the wild, so to speak, and one may not always recognize it as such. There are no monopolies in trade secrets, and thus one may receive the same information from more than one source, rendering recognition of trade secret rights more difficult. For sound reasons, then, trade secret misappropriation is not a strict liability wrong.

Despite this statutory mandate, there has been little discussion of intentionality when it comes to questions of secondary liability. By secondary liability, we mean cases where a plaintiff seeks liability against one defendant for the act of another. This Article centers on such questions, because that is where the requirement that trade secret misappropriation be intentional most needs attention. There are three areas in particular where the law should better recognize intent-based defenses to secondary liability.

This Article offers three propositions. First, we will explore important language in the federal Defend Trade Secrets Act and the Uniform Trade Secrets Act which blocks liability in some instances where a defendant has received a trade secret from a third party by “accident or mistake.” This clause presents a statutory safe harbor, in certain instances, for using a trade secret without intent. Courts should rescue this clause from seeming oblivion and apply it where one defendant has innocently received a trade secret from a third party and used it without notice.

Second, we will explore vicarious liability in trade secret law, where an employer-defendant is held to account for the actions of an employee within the scope of his or her employment even though company management was unaware of, and may well oppose, such conduct. Courts have adopted vicarious liability under the trade secret statutes. But they have largely overlooked common law exceptions that could apply in many cases, especially where a new employer should not be accountable for a new hire's off-premises activity.

---

DOI: <https://doi.org/10.15779/Z38000018N>

© 2024 Charles Tait Graves.

† Partner, Wilson Sonsini, San Francisco, and adjunct faculty, UC College of the Law, San Francisco. I am grateful for comments and input on this Article, including at the January 2023 Trade Secret Workshop and the August 2023 Intellectual Property Scholars Conference, from Deepa Varadarajan, Camilla Hrdy, Sharon Sandeen, Mark Lemley, Tim Murphy, Elizabeth Rowe, Victoria Cundiff, T.J. Chiang, and Chris Seaman. Tazeen Hussain, UC Law SF Class of 2024, provided fantastic research assistance.

Third, this Article will analyze the statutory concept of willful and malicious misappropriation, where a defendant may face enhanced damages. Though courts apply relatively consistent standards to define this heightened level of wrongful intent, they have not distinguished between the differing levels of intent of an employer-defendant and an employee-defendant. There is a difference between top-down coordinated wrongdoing by company management and lower-level employees making ad-hoc decisions on their own. Highlighting different levels of intent in such cases could avoid the exaggerated damages claims so often seen in trade secret litigation.

## TABLE OF CONTENTS

<b>I.</b>	<b>INTRODUCTION .....</b>	<b>723</b>
<b>II.</b>	<b>MAPPING INTENTIONALITY ACROSS THE DTSA AND UTSA .....</b>	<b>729</b>
A.	THE STATE OF MIND NECESSARY TO ENGAGE IN MISAPPROPRIATION .....	729
B.	ACTUAL KNOWLEDGE VERSUS CONSTRUCTIVE KNOWLEDGE.....	732
1.	<i>Cases Finding Constructive Knowledge.....</i>	734
2.	<i>Cases Declining to Find Constructive Knowledge.....</i>	738
3.	<i>The Problem of Notice Letters and Constructive Knowledge .....</i>	739
C.	IMPUTED KNOWLEDGE IS NOT A SUBSTITUTE FOR ACTUAL OR CONSTRUCTIVE KNOWLEDGE.....	741
<b>III.</b>	<b>THE OVERLOOKED SAFE HARBOR FOR TRADE SECRET MISTAKES AND ACCIDENTS.....</b>	<b>744</b>
A.	THE DTSA/UTSA “ACCIDENT OR MISTAKE” SAFE HARBOR CLAUSE .....	744
B.	INTERPRETING THE STATUTORY SAFE HARBOR FOR ACCIDENTS AND MISTAKES .....	747
1.	<i>The UTSA’s Official Commentary.....</i>	747
2.	<i>The UTSA Drafting History .....</i>	748
3.	<i>The Restatement’s Unsatisfactory Examples.....</i>	751
4.	<i>Interpreting the Accident and Mistake Language for Real-World Scenarios .....</i>	752
C.	CASE LAW ON THE SAFE HARBOR REMAINS SCARCE.....	757
D.	REVIVING THE SAFE HARBOR AS A DEFENSE TO MISAPPROPRIATION CLAIMS .....	760
<b>IV.</b>	<b>VICARIOUS LIABILITY AS A SUBSTITUTE FOR INTENT—AND ITS EXCEPTIONS.....</b>	<b>761</b>
A.	THREE EARLY CASES ON VICARIOUS LIABILITY UNDER THE UTSA .....	761

B.	COURTS HAVE VIRTUALLY ALWAYS FOUND VICARIOUS LIABILITY AVAILABLE .....	764
C.	STATES USE DIFFERENT TESTS TO APPLY VICARIOUS LIABILITY IN TRADE SECRET CASES.....	767
D.	CONTEXTS WHERE VICARIOUS LIABILITY IS INAPPLICABLE .....	769
<b>V.</b>	<b>CORPORATE DEFENDANTS AND WAYWARD EMPLOYEES: THE QUESTION OF INTENT FOR ENHANCED DAMAGES ..</b>	<b>772</b>
A.	“WILLFUL AND MALICIOUS MISAPPROPRIATION” UNDER THE TRADE SECRET STATUTES .....	773
B.	DEFINING “WILLFUL AND MALICIOUS MISAPPROPRIATION” .....	774
C.	SEPARATING EMPLOYEE MALICE FROM MANAGEMENT INTENT....	778
<b>VI.</b>	<b>CONCLUSION .....</b>	<b>781</b>

## I. INTRODUCTION

Questions of a party’s intent or state of mind are pervasive in trade secret law. The controlling statutes call for an examination of the defendant’s state of mind—and, less often, the plaintiff’s state of mind—at a variety of points spanning the lifecycle of a lawsuit. When one reviews the text of the federal Defend Trade Secrets Act (DTSA) and the state-law Uniform Trade Secrets Act (UTSA), the number of points across these statutes where a party’s state of mind matters to the outcome is striking.<sup>1</sup>

But courts too often gloss over circumstances where a defendant’s actual or constructive knowledge is less clear, especially when it comes to secondary liability—meaning, where a trade secret plaintiff seeks liability, or enhanced damages, against one defendant for the conduct of another.<sup>2</sup>

Focusing on intent in trade secret cases matters. Doing so has important consequences for reining in overbroad or exaggerated lawsuits. To that end,

---

1. Our focus here is civil disputes. Questions of intent in criminal trade secret cases are different, because in that context attempted misappropriation itself is a crime. *E.g.*, 18 U.S.C. § 1831(a)(4) (federal economic espionage statute; one who “attempts to commit any offense” described therein has engaged in a criminal act).

2. “Secondary liability” can mean different things in different legal contexts. To frame the concept for purposes of trade secret law, we could coin some bespoke term, to emphasize what is unique about the disputes at issue here. But that would needlessly complicate things. As this author has noted elsewhere, words such as “property” and “standing” have meanings peculiar to trade secret law. When analyzing trade secret law, we should always define such terms immanently, as it were, and not import meanings found in patent law or other areas of law.

this Article examines three intent-based inflection points where greater judicial attention could have a significant impact on how trade secret cases are adjudicated. Each is a question of secondary liability. In these instances, courts have not done enough to separately analyze the intent of each defendant. Doing so in these three scenarios could reduce the cost and complexity of trade secret cases, which are notoriously expensive and time-consuming, and help illustrate when small infractions by employees on the move are used to inflate cases against competitors which hire them.

Increased attention to questions of secondary liability is one way to impose limits on a structural problem in trade secret law: the ease of filing suit against multiple defendants and imposing asymmetrical costs on a rival, independent of the merits. Trade secret law is an area where one can file a lawsuit against a competitor based on relatively minor conduct by someone other than the primary defendant.

A ubiquitous example is lawsuits filed against a new employer where a departing employee downloaded files from the prior employer before joining the new one. That act, carried out while the employee was still employed by the plaintiff, can be a “hook”—so to speak—to bring costly and wide-ranging claims against the hiring company, even if it was unaware of the download, and even if the downloaded files carried little value or were never used. In such cases, we should not assume that the new employer could be secondarily liable for such activity, or subject to enhanced damages, even if the employee in transit could be.

Separating the intent of the individual defendant from the intent of the new employer in such disputes is a powerful means of reducing the temperature. If courts understand that a new employer or other corporate defendant is not always in the know, and that its intentionality must be separately assessed in order to impose separate liability, or to consider enhanced damages, greater attention to questions of intent can reduce lawsuits filed or maintained for anticompetitive purposes.

Our study of intentionality in trade secret law has four Parts. First, in order to frame three propositions regarding secondary trade secret liability, we will map the standards for assessing a defendant’s intent as to “misappropriation” under the DTSA and the UTSA. That proves to be a complicated question, as trade secret law measures actual and constructive notice in a variety of contexts. We will explore the question of constructive knowledge in difficult instances, such as when a party receives a threat letter from a potential plaintiff. And we will probe whether or not imputed knowledge—a doctrine under which companies can be deemed to know what their executives know—can

substitute for actual and constructive knowledge where the executive remembers trade secrets from a prior job.

Then, with precise definitions of intentionality in trade secret law in hand, we turn to three underdeveloped areas of trade secret law where courts should pay greater attention to assessing intent when a plaintiff pursues secondary liability.

We begin with the “accident or mistake” language found in the DTSA and the UTSA. This is defensive language designed to reduce—or eliminate—one form of secondary liability for misappropriation. It provides a safe harbor from liability for misappropriation in situations where a defendant innocently received the plaintiff’s trade secret from some other person or entity, and then undertakes some act in reliance on it, before learning that the information is the plaintiff’s trade secret. Take, for example, a company which buys or licenses technology from a third party in an ordinary commercial transaction, believing that the seller or licensor has full rights to what it transfers. If the company then uses that information in reliance on its innocent acquisition, and only later learns of a trade secret problem, this statutory safe harbor could prevent (or at least limit) a finding of “misappropriation.”

This powerful clause in the DTSA and the UTSA has been overlooked by litigants and courts. Vanishingly few cases address it. This statutory safe harbor should be rescued from oblivion and restored it to its rightful place in the calculus of what acts constitute trade secret misappropriation. The “accident or mistake” clause should provide protection for unintentional—that is, accidental or mistaken—receipt of a trade secret from a third party such as a commercial licensor or seller where the defendant has materially changed its position such that it would be inequitable to impose liability for using the information, including at least some degree of future use. Doing so would solve lingering uncertainty in the case law regarding downstream liability for innocent receipt of someone else’s trade secret.

Second, we will examine a company’s vicarious liability for acts of trade secret misappropriation by its employees. Most courts agree that the common law doctrine of vicarious liability applies to the DTSA and the UTSA. But very few courts address exceptions to vicarious liability: situations where the employer is not liable for an employee’s acts outside the course and scope of employment. This is surprising because so many trade secret lawsuits turn on accusations that an employee downloaded files from the former employer when leaving the company, albeit without evidence that the files were used or transferred to the new employer. Because such cases can lead to anticompetitive attacks on smaller rivals, often simply to punish them for

hiring from the plaintiff, courts should be more attentive to limits to vicarious liability.

Third, we turn to enhanced damages for what the DTSA and the UTSA call “willful and malicious misappropriation.” Here, a defendant found liable for misappropriation may face up to treble damages if a court or jury finds this heightened level of wrongful intent. But the term begs the question: whose intent? Company executives? Or ad-hoc conduct of lower-level employees, where management may have been unaware of their acts? What if there are different intentions by different employees? And what if the employer has provided at least some degree of training or policies to employees in order to reduce the possibility of trade secret problems? Courts should pay more attention to the distinction between malice by a company and malice by an employee, and not conflate the two.

These three proposals regarding secondary trade secret liability fill a gap in the trade secret literature. The scholarly commentary is thin when it comes to intentionality in trade secret cases. Few articles directly address any facet of intentionality.<sup>3</sup> Some important articles indirectly raise questions of intent

---

3. See generally Michael L. Rustad, *The Negligent Enablement of Trade Secret Misappropriation*, 22 SANTA CLARA HIGH TECH. L.J. 455, 458, 518–521 (2005) (proposing, in the wake of the U.S. Supreme Court’s decision in *Metro-Goldwyn-Meyer Studios, Inc. v. Grokster, Ltd.*, 125 S. Ct. 2764, 2775 (2005), to allow an intentional inducement theory of copyright infringement liability against a peer-to-peer sharing tool, that trade secret law “be amended to give the corporate victims of espionage standing to file a statutory tort action against the primary wrongdoers as well as the software provider whose defective software frequently paves the way for economic or industrial espionage”; positing without empirical data that “[s]oftware vendors that market products with known vulnerabilities and online intermediaries who do not implement adequate security foreseeably enable cybercriminals to intercept data and misappropriate trade secrets”; commentator did not provide any data showing any such thing, adequately define a class of software vendors to which this would apply, or explain why someone using software to accomplish a misappropriation is any different than someone using a telephone or fax machine to that end). Cf. Robert G. Bone, *Secondary Liability for Trade Secret Misappropriation: A Comment*, 22 SANTA CLARA HIGH TECH. L.J. 529, 530, 535–41 (2005) (persuasive rebuttal to Rustad’s proposal noting, among other things, that the notion of a software maker’s “defect” that renders “secrets vulnerable to misappropriation” is a different context than Grokster-like tools that allow multiple acts of infringement by different people under no common control, but instead typically involve related groups of employees and a new employer, and that imposing potential liability on software makers on a theory that some third party would exploit the software for misappropriation could “chill software innovation”; see also Elizabeth A. Rowe, *Contributory Negligence, Technology, and Trade Secrets*, 17 GEO. MASON L. REV. 1, 26–33 (2009) (proposing that the reasonable security measures element a plaintiff must satisfy be construed in light of how the plaintiff acted with respect to technical security risks, akin to the contributory negligence defense seen in common law tort claims); Lynda J. Oswald, *The Role of “Commercial Morality” in Trade Secret Doctrine*, 96 NOTRE DAME L. REV. 125, 166 (2020) (although not directly about intentionality, solidly critiquing some courts’ recourse

when exploring particular aspects of trade secret law.<sup>4</sup> A new commentary by Tim Murphy focuses on the distinction between trade secrets that a former employee intentionally remembers from a prior job and information for which the employee does not recall the source.<sup>5</sup> Highlighting the DTSA and UTSA knowledge requirement, he proposes that courts be lenient with respect to the latter.<sup>6</sup>

Still, no article in the literature fully analyzes how the trade secret statutes define actual and constructive intent by a defendant and illuminates contexts where secondary liability matters to an outcome. This is surprising, because the trade secret statutes embed questions of intent to a much greater extent than do the Patent Act, the Copyright Act, and the Lanham Act—areas of intellectual property where innocent infringement can lead to direct liability.<sup>7</sup>

---

to notions of “commercial morality” to judge a defendant’s conduct under an ethical concept that “lack[s] a solid theoretical foundation.”)

4. See Deepa Varadarajan, *Trade Secret Precautions, Possession, and Notice*, 68 HASTINGS L.J. 357, 384–86 (2017) (in-depth exploration of the reasonable security measures element of a trade secret claim; explaining that such measures play a “notice” function, thus highlighting the intent of the party seeking to use such information; “[i]f observers cannot discern the boundaries of patented inventions, copyrighted works, and trade secret protected information, then they may be overly cautious in their inventive and creative endeavors for fear of inviting litigation.”); Camilla A. Hrды & Mark A. Lemley, *Abandoning Trade Secrets*, 73 STAN. L. REV. 1, 48, 56 (2021) (exploration of how companies might be deemed to have abandoned trade secrets with a proposal that former employees be permitted to use such abandoned information, thus raising the question how an intent to abandon might be recognized by a would-be user; potential factors include declining to enter a market).

5. See Timothy Murphy, *Can’t Get it Out of My Head: Trade Secrets Liability for Remembered Information*, 2023 WISC. L. REV. 1929, 1931 (2023).

6. See *id.* at 1934, 1962–66 (“As proposed here, courts should address remembered information as part of the misappropriation analysis, after the existence of a trade secret has been established. And thus, the issue of remembered information is closely tied to the defendant’s conduct, rather than whether a trade secret exists.”; outlining “a taxonomy of remembered information” to distinguish the degree to which an employee recalls the source of information in his or her memory).

7. *E.g.*, 35 U.S.C. § 271(a) (Patent Act: “whoever without authority makes, uses, offers to sell, or sells any patented invention, within the United States . . . infringes the patent.”); *Playboy Ent., Inc. v. Frena*, 839 F. Supp. 1552, 1559 (M.D. Fla. 1993) (“Intent to infringe is not needed to find copyright infringement. Intent or knowledge is not an element of infringement, and thus even an innocent infringer is liable for infringement; rather, innocence is significant to a trial court when it fixes statutory damages, which is a remedy equitable in nature.”). The Patent Act does incorporate questions of constructive and actual notice regarding pre-lawsuit damages, centering on the issue of patent marking. See 35 U.S.C. § 287(a) (“In the event of failure so to mark, no damages shall be recovered by the patentee in any action for infringement, except on proof that the infringer was notified of the infringement and continued to infringe thereafter, in which event damages may be recovered only for infringement occurring after such notice. Filing of an action for infringement shall constitute such notice.”). The Copyright Act has a comparable term. See 17 U.S.C. § 401(d) (“If a notice

Patent law has seen a lively debate over the extent to which the patent regime is one of “strict liability.”<sup>8</sup> Likewise, commentators on copyright law have argued over whether copyright presents a strict liability standard or—especially as to the fair use defense—an intent-based standard.<sup>9</sup> Trademark law in particular has seen great attention to questions of secondary liability, perhaps due to the difficulties in suing counterfeiters.<sup>10</sup>

---

of copyright in the form and position specified by this section appears on the published copy or copies to which a defendant in a copyright infringement suit had access, then no weight shall be given to such a defendant’s interposition of a defense based on innocent infringement in mitigation of actual or statutory damages, except as provided in the last sentence of section 504(c)(2).” Cf. 17 U.S.C. § 504(c)(2) (noting that innocent infringement can lead to a reduction of statutory damages, and that a fair use defense can also mitigate damages). For its part, the Lanham Act contemplates direct liability for trademark infringement without any showing of intent, though it also includes a unique safe harbor for “innocent” violators who merely printed the infringing mark limiting the reach of injunctive relief. See 15 U.S.C. § 1114(1), (2).

8. E.g., Lynda J. Oswald, *The ‘Strict Liability’ of Direct Patent Infringement*, 19 VAND. J. ENT. & TECH. L. 993, 997 (2020) (arguing that using such terminology improperly turns attention away from the text of the patent act and improperly allows for consideration of “social policy concerns” for liability); Patrick R. Goold, *Patent Accidents: Questioning Strict Liability in Patent Law*, 95 IND. L.J. 1075, 1079 (2020) (advocating a negligence-based standard for patent law, where accidental patent infringement might be excused if the defendant exercised “all reasonable care to prevent any accidental patent infringement”); Saurabh Vishnubhakat, *An Intentional Tort Theory of Patents*, 68 FLA. L. REV. 571, 576 (2017) (noting that a “strict liability” regime leads to problems such as “indiscriminately impos[ing] liability on actions that are purely inadvertent or even unforeseeable”); Roger D. Blair & Thomas F. Cotter, *Strict Liability and its Alternatives in Patent Law*, 17 BERKELEY TECH. L.J. 799, 807 (2002) (noting, among other things, that “strict liability” is a misnomer in situations such as those where a patent owner does not mark the product and “damages only accrue from the date of actual notice”).

9. See e.g., Patrick R. Goold, *Moral Reflections on Strict Liability in Copyright*, 44 COLUM. J.L. & ARTS 123, 125–27 (2021) (noting that the “strict liability” standard in copyright is “entirely judge-made,” and considering “the moral side of accidental infringement” to propose reforms such as facilitating “the introduction of a negligence liability rule into copyright”); Apostolos G. Chronopoulos, *Strict Liability and Negligence in Copyright Law: Fair Use as Regulation of Activity Levels*, 97 NEB. L. REV. 384, 387–89, 466 (2018) (asserting that copyright law “constitutes a mixed system” of both strict liability and negligence standards, with the fair use doctrine centering the latter); Patrick R. Goold, *Is Copyright Infringement a Strict Liability Tort?*, 30 BERKELEY TECH. L.J. 305, 310 (2015) (arguing that copyright law “is in fact a fault-based tort” because mere infringement is insufficient and “it must be shown that the defendant’s copying was wrongful”); Steven Hetcher, *The Immorality of Strict Liability in Copyright*, 17 MARQUETTE INT. PROP. L. REV. 1, 2 (2013) (arguing that copyright is a “fault standard,” not a strict liability standard, “as a result of the emergence of the fair use doctrine”); R. Anthony Reese, *Innocent Infringement in U.S. Copyright Law: A History*, 30 COLUM. J.L. & ARTS 133 (2014) (providing a detailed examination of how early protections for innocent infringers shrank in recent decades).

10. See generally David S. Welkowitz, *Fault Lines in Trademark Default Judgments*, 22 GEORGIA J. INTELL. PROP. LAW. 101 (2014); Irene Calboli, Jane Ginsburg, Amy Cotton, Bob Weigel & Bruce Rich, *Proposed Secondary Liability Regimes for Trademark Infringement Online:*

To be sure, it is not clear that much can be transposed from debates in other fields of intellectual property law to trade secret law. The trade secret statutes contain unique language concerning intent. Moreover, trade secret cases often turn on contexts such as employee mobility that raise policy concerns not seen in other IP disciplines. We should debate questions of intentionality in trade secret law from scratch, as it were, to create best practices particular to this area of law.

In summary, questions of secondary liability in trade secret cases have seen little attention from courts and commentators despite their seeming utility in reducing unnecessary or exaggerated trade secret disputes. It is surprising that courts and defense attorneys have not often explored these possibilities. Ignoring that each plaintiff must establish intent as to each separate defendant allows plaintiffs to blend defendants together without satisfying their burden of proof as to each. By drawing an intent-based dividing line between different actors in trade secret cases, courts can reduce lawsuits filed, or over-litigated, for improper purposes.

## II. MAPPING INTENTIONALITY ACROSS THE DTSA AND UTSA

### A. THE STATE OF MIND NECESSARY TO ENGAGE IN MISAPPROPRIATION

The trade secret statutes do not contemplate strict liability for misappropriation. Nor is there liability for negligence. To the contrary, the DTSA and the UTSA structure their definitions of “misappropriation” with language that turns on the defendant’s intent—that is, actual or constructive knowledge that one has acquired, used, or disclosed a trade secret without authorization.

For that reason, courts have stated that “[m]isappropriation of trade secrets is an intentional tort.”<sup>11</sup> As the California Court of Appeal held in a

---

*Commentary*, 37 COLUM. J.L. & ARTS 621 (2014); John T. Cross, *Contributory Infringement and Related Theories of Secondary Liability for Trademark Infringement*, 80 IOWA L. REV. 100 (1994).

11. See *PMC, Inc. v. Kadisha*, 78 Cal. App. 4th 1368, 1382 (2000). Many other courts have used similar language, including *Successware, Inc. v. Servicetitan, Inc.*, No. CV 20-5179 DSF (PVCx), 2020 U.S. Dist. LEXIS 262181, at \*23–24 (C.D. Cal. Sept. 10, 2020) (quoting *PMC* on motion to dismiss); *Eddie Kane Steel Prods., Inc. v. Alabama Plate Cutting Co., Inc.*, Civil Action No. 18-15167 (MAS) (LHG), 2019 U.S. Dist. LEXIS 121758, at \*17 (D.N.J. July 19, 2019) (noting, on motion to dismiss and transfer, that “misappropriation of trade secrets is an intentional tort.”); *Eagle Oil & Gas Co. v. Shale Exploration, LLC*, 549 S.W.3d 256, 283 (Tex. Ct. App. 2018) (stating that “misappropriation of trade secrets is an intentional tort” in ruling on exemplary damages); *Mar Oil Co. v. Korpan*, No. 3:11CV1261, 2015 U.S. Dist. LEXIS 131755, at \*7 (N.D. Ohio Sept. 29, 2015) (in affirming finding of joint and several

2000 decision, “[u]se of a trade secret without knowledge it was acquired by improper means does not subject a person to liability unless the person receives notice that its use of the information is wrongful.”<sup>12</sup> This vocabulary, centering on “tort” concepts, reminds us of trade secret law’s origins in common law, before enactment of today’s statutory regimes.

Although the statutes are not models of clarity, the DTSA and the UTSA define the act of “misappropriation” in four, somewhat overlapping ways—each one requiring actual or constructive knowledge that one’s conduct flows from improper means or violation of a confidentiality duty.<sup>13</sup> First, one can wrongfully acquire a trade secret, or acquire it knowing that one’s source previously had acquired it by improper means, with actual or constructive knowledge of that wrongfulness: “Acquisition of a trade secret of another by a person who *knows or has reason to know* that the trade secret was acquired by improper means.”<sup>14</sup>

---

liability, noting that “liability for trade secret misappropriation, an intentional tort, is joint and several”); *Be In, Inc. v. Google Inc.*, No. 12-CV-03373-LHK, 2013 U.S. Dist. LEXIS 147047, at \*9 (N.D. Cal. Oct. 9, 2013) (stating intentional tort language on motion to dismiss); *Bovie Med. Corp. v. Livneh*, No. 8:10-cv-1527-T-24EAJ, 2010 U.S. Dist. LEXIS 134490, at \*18 (M.D. Fla. Dec. 20, 2010) (“Misappropriation of trade secrets in an intentional tort in the state of Florida.”); *Hagen v. Burmeister & Assoc.*, 633 N.W.2d 497, 503 (Minn. 2001) (noting that “misappropriation of trade secrets is an intentional tort” in case centering on vicarious liability); *Miller v. Abrams Inc.*, 156 F.3d 598, 603 (5th Cir. 1998) (“[M]isappropriation of proprietary information and misuse of trade secrets are generally considered to be intentional torts.”; remanding for determination of malice in case by former employer against bankrupt debtor); *Micro Data Base Sys, Inc. v. Dharma Sys., Inc.*, 148 F.3d 649, 654 (7th Cir. 1998) (stating same in choice of law dispute); *cf. Shell v. Henderson*, No. 09-cv-00309-MSK-KMT, 2013 U.S. Dist. LEXIS 129006, \*7 (D. Col. July 24, 2013) (noting, on motion for fees after successful motion to dismiss on jurisdictional grounds, that “[m]isappropriation of trade secrets is a tort, but not always an intentional tort”; noting that misappropriation can be based on constructive knowledge and apparently assuming that does not constitute intentional conduct).

12. *See PMC*, 78 Cal. App. 4th at 1383 (reversing trial court’s summary judgment ruling and finding a triable issue of fact as to whether investors “in anticipation of enormous corporate and personal profit, knowingly invested at a bargain price in a corporation whose sole business assets consisted of stolen confidential information and processes, and subsequently controlled the entity which was engaging in unlawful conduct”).

13. We will use California’s UTSA as an exemplar here. *See* CAL. CIV. CODE §§ 3426.1(a)–(b); 18 U.S.C. § 1839(5).

14. *See* CAL. CIV. CODE § 3426.1(b)(1) (emphasis added); 18 U.S.C. § 1839(5)(A). “Improper means” is defined as intentional wrongdoing to obtain someone’s trade secret: it “includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage.” CAL. CIV. CODE § 3426.1(a); 18 U.S.C. § 1839(6). In somewhat repetitive language, an adjacent subsection provides for liability for “[d]isclosure or use . . . by a person who . . . [a]t the time of disclosure or use, knew or had reason to know that his or her knowledge of the trade secret was: (i) Derived from or through a person who

Second, one can use or disclose a trade secret after wrongfully acquiring it, effectively engaging in a second (or third) type of misappropriation following the first: “Disclosure or use . . . by a person who . . . *Used improper means to acquire knowledge* of the trade secret.”<sup>15</sup>

Third, one can use or disclose a trade secret wrongfully, even if one’s original acquisition of the trade secret was lawful: “Disclosure or use . . . by a person who . . . At the time of disclosure or use, *knew or had reason to know* that his or her knowledge of the trade secret was: [ . . . ] (ii) Acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use.”<sup>16</sup>

The fourth type of misappropriation stands apart from the others: the “accident or mistake” clause. It provides for liability where there is “[d]isclosure or use . . . by a person who . . . Before a material change of his or her position, *knew or had reason to know* that it was a trade secret and that knowledge of it had been acquired by accident or mistake.”<sup>17</sup> In this instance, one can misappropriate a trade secret by straying outside the boundaries of a statutory safe harbor that protects use or disclosure of another party’s trade secret. Specifically, the DTSA and the UTSA allow for a safe zone whereby if one acquires a trade secret by accident or mistake and uses it without realizing (or constructively realizing) the truth, such use is not “misappropriation.” That said, once one has such a realization, the immunity might end at some point, depending on the degree of one’s use of the trade secret to that point.

Notably, all four forms of statutory “misappropriation” require that the defendant either know the trade secret, or acquire the trade secret. The latter possibility presumably envisions a situation where a party has obtained information but has not studied its contents. Thus, a defendant which has not learned or acquired the alleged trade secret cannot be liable under the text of the DTSA and the UTSA. For example, in a 2010 California case, a company which had licensed a software product from a licensor that had misappropriated software source code used to make the product was not liable because it had neither learned nor acquired that source code.<sup>18</sup> It had merely obtained a software product made from the trade secret, not the trade secret

---

had utilized improper means to acquire it; [ . . . ] or (iii) Derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use.” *See* CAL. CIV. CODE § 3426.1(b)(2)(B); 18 U.S.C. § 1839(5)(B)(ii).

15. *See* CAL. CIV. CODE § 3426.1(b)(2)(A) (emphasis added); 18 U.S.C. § 1839(5)(B)(i).

16. *See* CAL. CIV. CODE § 3426.1(b)(2)(B) (emphasis added); 18 U.S.C. § 1839(5)(B)(ii)(II).

17. *See* CAL. CIV. CODE § 3426.1(b)(2)(C); 18 U.S.C. § 1839(5)(B)(iii).

18. *See* *Silvaco Data Systems v. Intel Corp.*, 184 Cal. App. 4th 210, 222–23 (2010) overruled in part on unrelated ground, *Kwikset v. Superior Court*, 51 Cal. 4th 310, 337 (2011).

itself.<sup>19</sup> This type of downstream liability is not something the trade secret statutes contemplate. The absence of such liability for mere use of a product created from the licensor's misuse of trade secrets, while not the subject of the present study, reinforces the intent-based nature of the statutory term "misappropriation."<sup>20</sup>

## B. ACTUAL KNOWLEDGE VERSUS CONSTRUCTIVE KNOWLEDGE

Layered into the four types of statutory misappropriation is a distinction between actual knowledge that one has acquired a trade secret, or wrongfully used or disclosed it, and constructive knowledge. The phrase "had reason to know" (or, in the DTSA, "has reason to know") refers to the latter.

Presumably because a defendant's actual knowledge of wrongful conduct is often straightforward, there are not many cases addressing this type of intentional wrongdoing in detail. As one example, a 2020 case from the Southern District of New York found that where a departing employee copied the employer's trade secrets into a "personal directory" at work before leaving, and studied that information, this "satisfie[d] the knowledge requirement," as he knew that he was acquiring the employer's secrets by improper means, violating the terms of his employment agreement.<sup>21</sup> And in a 1997 case from the Central District of California, the court denied a defense motion for summary judgment which sought to contest the actual knowledge requirement.<sup>22</sup> In a case where the plaintiff alleged that the defendants had obtained and used customer-related information customarily treated as confidential, the court spent more effort than is typical in describing testimony from multiple employees of a corporate defendant showing their knowledge that the company had obtained information it knew came from the plaintiff in a context suggesting intent.<sup>23</sup>

---

19. *See id.*; *see also* Architectural Models, Inc. v. Neklason, 264 F. Supp. 312, 317, 322 (N.D. Cal. 1967) (trade secret claim failed where plaintiff could not establish that defendants had been exposed to a drawing that was claimed as the trade secret).

20. A different question would arise if a downstream consumer unknowingly licensed or purchased a product that did contain, or reveal knowledge of, a trade secret the manufacturer wrongfully took from the original owner. In that case, the consumer would indeed have acquired the trade secret, albeit without intent to do so. *See infra* Part III.D. As discussed in Section III.D below, this seems to be a paradigmatic instance where the "accident or mistake" safe harbor of the DTSA and UTSA should govern.

21. *See* KCG Holdings, Inc. v. Khandekar, No. 17-CV-3533 (AJN), 2020 U.S. Dist. LEXIS 44298, at \*33 (S.D.N.Y. Mar 12, 2020).

22. *See* Ernest Paper Prod., Inc. v. Mobil Chem. Co., CV 95-7918 LGB (AJAX), 1997 U.S. Dist. LEXIS 21817, at \*23-25 (C.D. Cal. Sept. 17, 1997).

23. *See id.*; *see also* Successware, Inc. v. Servicetitan, No. CV 20-5179 DSF (PVCx), Inc., 2020 U.S. Dist. LEXIS 262181, at \*23-24 (C.D. Cal. Sept. 10, 2020) (denying motion to dismiss

Of greater interest are cases wrestling with the degree of intentionality that constitutes a defendant's constructive knowledge. This second category of knowledge sufficient to trigger liability for misappropriation is less clear—as the DTSA and UTSA put it, liability applies only when a defendant had “reason to know” that what it received, used, or disclosed was someone else's trade secret.

We should unpack this dense concept. In order for constructive knowledge to exist, a defendant must know two things. First, the defendant must glean to at least some degree that the information at issue is a trade secret, which may not be clear. And it must also discern that the information belongs to someone else—which also may not be clear.<sup>24</sup> This can present a difficult conundrum. For example, imagine that a person learns information on the job that is similar to information that she saw in a university laboratory during graduate school. If she believes she can use the information lawfully, but a judge or jury disagrees, was she truly on notice? The trade secret statutes do not account for this type of mistake in one's judgment.

To take a second example, companies frequently have attorneys send letters to former employees and business rivals warning of confidentiality obligations or potential trade secret misuse. But not every letter-sender may have researched whether the information claimed as a trade secret really is so—in fact, in at least some cases, the sender will be wrong. This author has seen letters claim trade secrets in information that the claimant itself had published on its website.

In such instances, is a defendant on constructive notice simply because someone has declared that information—or some undefined swath of information—includes trade secrets? Having notice of a potential trade secret, or a threat of trade secret litigation, is not the same thing as having reason to know that some specific thing truly qualifies as a trade secret. The same

---

where plaintiff alleged that when one defendant acquired a second defendant which possessed the plaintiff's trade secrets, the acquiring company began using a customer list to contact customers; finding that “information and belief” allegations that the acquiring company knew the customer list belonged to the plaintiff were sufficient due to the “value and rarity” of the list “considering the nature of the industry and target customer”).

24. At least one court has rejected the notion that a defendant must know whose trade secret is at issue, as opposed to more generally knowing (or having reason to know) that it is someone else's trade secret. *See* Columbus Steel Castings Co. v. King Tool Co., No. 08AP-385, 2008 Ohio App. LEXIS 5262, at \*20 (Ohio Ct. App. Dec. 4, 2008) (reversing summary judgment for defendant on trade secret claim where plaintiff alleged that defendant had obtained its trade secrets by working with a second defendant; rejecting defendant's argument that “it was necessary” that it know that the alleged trade secret at issue was the plaintiff's trade secret, as opposed to a trade secret of the second defendant; the court noted that the UTSA has no such requirement).

questions might be asked when a plaintiff sues over “inevitable disclosure”—that is, speculation that a newly-hired employee might someday misuse a trade secret, without evidence of actual misappropriation or a threat to misappropriate. In a lawsuit expressly grounded on speculation, who exactly is on notice of what?

The trade secret statutes do not provide definitional guidance for what “reason to know” means. While case law is sparse, the definition appears tethered to the common law concept of constructive knowledge. By way of example, California defines constructive notice by statute. It means “actual notice of circumstances sufficient to put a prudent [person] upon inquiry as to a particular fact[.]”<sup>25</sup> That definition focuses on what is enough to cause someone to start asking questions—not complete knowledge that some course of conduct is unlawful.

### 1. *Cases Finding Constructive Knowledge*

A 1990 California case, decided on facts pre-dating the UTSA, exemplifies what constructive notice means in the trade secret context. In *Ralph Andrews Productions, Inc. v. Paramount Pictures Corp.*, an employee of a television production company offered the defendant an idea for a television show.<sup>26</sup> He claimed that the idea was his own. The defendant knew that the employee worked for the production company. The defendant “was[also] explicitly given information which indicated another entity may have had rights to the concept.”<sup>27</sup> This was sufficiently concerning to cause the defendant to ask the employee for a responsive written statement, but the defendant proceeded to enter the deal even though the employee never provided the statement. On a motion for summary judgment, the court found a triable issue of fact on the question of constructive notice.<sup>28</sup>

The ruling makes sense. The buyer had notice that something was amiss. Also, under the state’s invention assignment statute, California employers own intellectual property rights in employee ideas that relate to the business.<sup>29</sup> Thus,

---

25. See CAL. CIV. CODE § 19.

26. *Ralph Andrews Prods., Inc. v. Paramount Pictures Corp.*, 222 Cal. App. 3d 676 (1990).

27. *Id.* at 685.

28. *Id.* at 682, 685 (constructive notice occurs where someone “is aware of facts which would make a reasonably prudent person suspicious”) (quoting *Hobart v. Hobart Estate Co.*, 26 Cal. 2d 412, 438 (1945)).

29. See CAL. LAB. CODE §§ 2870–72. For an early case under the California UTSA examining the “had reason to know” element, see *Speech Tech. Assoc. v. Adaptive Comm. Sys., Inc.*, No. C-88-2392-VRW, 1994 U.S. Dist. LEXIS 11660, at \*26 (N.D. Cal. Aug. 16, 1994) (a defendant obtained technology under an oral agreement to redesign it, but sold the redesigned product without paying royalties).

because the defendant knew the employee was working for a television production company, it had reason to suspect that he did not own the idea.

A more recent constructive knowledge case is also straightforward. In a 2018 Ninth Circuit decision arising from a case in Arizona, the appellate court reversed a summary judgment in favor of a defendant which had purchased the plaintiff's database of consumer records. The trial court had held that the defendant did not have reason to know that the data records "were either secret or stolen."<sup>30</sup> Because the defendant had paid "less than 1% of the market rate for a one-time license to obtain actual ownership of data," obtained ownership though a method "unusual in the industry," and had "prior experience that should have put [it] on notice of an improper acquisition," the Ninth Circuit found the defendant possessed "constructive knowledge" that it had acquired a trade secret.<sup>31</sup>

Similar issues of constructive notice were apparent in a 2016 case where a trial court denied a motion to dismiss. In *Joshua David Mellberg, LLC v. Will*, a magistrate noted that the plaintiff alleged that even though a corporate defendant did not employ all individual defendants accused of downloading and using trade secrets, the plaintiff sufficiently alleged that the corporate defendant knew or should have known that it acquired and used the plaintiff's trade secrets through its contacts with them, which demonstrated their plans to mirror the plaintiff's sales program, the similarity of websites they launched to the plaintiff's websites, and presentations that were nearly identical to those of the plaintiff.<sup>32</sup>

A 2017 case from Connecticut is also notable because the court offered a specific definition of constructive knowledge under trade secret law. But the decision nonetheless raises nettlesome questions. In *Dur-A-Flex, Inc. v. Dy*, a trial court ruled on a defense motion for summary judgment where a corporate defendant previously had used floor coating materials from the plaintiff, but subsequently switched to buying from a new business founded by a chemist who had recently left the plaintiff.<sup>33</sup> Notably, the corporate defendant tested the chemist's version during the brief period after he resigned from the

---

30. *Experian Info. Sols., Inc. v. Nationwide Mktg. Serv.*, 893 F.3d 1176, 1181 (9th Cir. 2018) (applying the Arizona UTSA).

31. *Id.* at 1189 (citing *Syntex Ophthalmics, Inc. v. Novicky*, No. 80 C 6257, 1982 U.S. Dist. LEXIS 14175, at \*2 (N.D. Ill. May 6, 1982) (finding that a \$20,000 payment for technology that cost a million dollars to develop was evidence of the defendant's constructive knowledge it had acquired another's trade secret)).

32. *See* No. CV-14-02025-TUC-CKJ (CRP), 2016 U.S. Dist. LEXIS 32412, at \*37-46 (D. Ariz. Jan. 22, 2016).

33. *See* No. X04HHDCV146049281S, 2017 Conn. Super. LEXIS 4241, at \*9-10 (Super. Ct. Aug. 14, 2017).

defendant, “but before he formally ended his employment.”<sup>34</sup> The court rejected the defendant’s argument that actual notice is necessary for UTSA liability, and defined constructive knowledge in the trade secret context as follows:

A defendant may have reason to know that information held by a third person is the trade secret of another when, based on the information in the defendant’s possession, a reasonable person would have been put on notice, and an inquiry pursued with reasonable diligence would have disclosed that the information provided to the defendant was actually wrongfully obtained from another.<sup>35</sup>

The trial court found that the corporate defendant “should have suspected” that the departing employee’s “newly-formulated floor product” “was likely to be based in some measure upon [the individual’s] experience gained in the research and development of floor products as [plaintiff’s] chemist, given that they “conducted tests[.]”<sup>36</sup>

Despite the ill-timed review of the chemist’s new product, this lower court ruling is ambiguous. Must everyone who conducts business with a former employee conduct an inquiry into potential trade secret misappropriation? What if the basics of the formula contains common ingredients? What if many market competitors offer similar products? Having “experience” and creating a competing product surely should not be sufficient—again putting aside the timing issue in this particular case, which resembles the fact pattern in *Ralph Andrews*<sup>37</sup>—to raise a question of constructive knowledge. Said differently, while the case holding makes sense because the chemist had apparently begun work on a competing product before leaving his job, an ordinary situation of competition by a former employee surely cannot serve as constructive notice of wrongdoing.<sup>38</sup>

---

34. *Id.* at \*3.

35. *Id.* at \*9.

36. *Id.* at \*10.

37. *See Ralph Andrews Prods., supra* note 26.

38. Because employees are permitted to transfer their general skills, knowledge, and experience from job to job, *see* Camilla A. Hrdy, *The General Knowledge, Skill, and Experience Paradox*, 60 B.C. L. REV. 2409 (2019), the exercise of such rights cannot in isolation be a trigger for constructive knowledge of misappropriation. Likewise, companies can hardly glean what may or not be a trade secret in the employment contract of an employee they hire from another company. As Camilla Hrdy and Chris Seaman have shown in a comprehensive study of such contract language, the confidentiality terms of employment agreements are generally vague about what is protectable and overbroad, encompassing unprotectable information as well. *See* Camilla A. Hrdy & Christopher B. Seaman, *Confidentiality Agreements that Act Like Noncompetes*, 133 YALE L.J. 669 (2023).

A 2014 case from Illinois was perhaps more attuned to such doubts. In *First Financial Bank, N.A. v. Bauknecht*, the court denied a defense motion for summary judgment where an employee who changed jobs was accused of using memorized customer information that his former employer claimed to be a trade secret.<sup>39</sup> As to the new employer, the court ruled that there was a triable issue of fact as to constructive knowledge because the new employer discussed the employee moving over customers from the plaintiff, and because it understood that customer information is “ordinarily confidential within the industry.”<sup>40</sup> But the court also cautioned that a jury might not find constructive knowledge; because if the information turned out not to be secret, the employee would have been free to call customers. The new employer thus would have “acted upon the assumption that [new employee] was complying with the law.”<sup>41</sup> This ruling at least recognizes the quandary in finding constructive knowledge where the very same facts could signal perfectly legal conduct.

In other cases, the constructive knowledge concept is sometimes used as something of a gap-filler where evidence of intent is lacking. For example, a 2001 case from the Middle District of Pennsylvania, the court found that a defendant should have known that a contractor who had worked for the plaintiff and was hired for the sole purpose of assisting with a bid used the plaintiff’s bid-related trade secrets. It reasoned that the defendant made no inquiry of the contractor and thus “may not hide improper acquisition of trade secrets behind a veil of willful ignorance.”<sup>42</sup> Other courts have implied a duty of confidentiality in circumstances where there was an expectation of such a duty. These decisions seem to fall within the concept of constructive knowledge rather than actual knowledge.<sup>43</sup>

---

39. *See* *First Fin. Bank, N.A. v. Bauknecht*, 71 F. Supp. 3d 819, 846–47 (N.D. Ill. 2014).

40. *See id.* at 846.

41. *See id.* at 847.

42. *See* *First Health Group Corp. v. Nat’l Prescription Adm’rs, Inc.*, 155 F. Supp. 2d 194, 227–28 (M.D. Penn. 2001) (“NPA should have known, because of its knowledge of the industry and previous PACE bids, that Norton’s contributions to its bid proposal included First Health’s trade secrets.”).

43. *See* *Mineral Deposits Ltd. v. Zigan*, 773 P.2d 606,608 (Col. Ct. App. 1989) (device lent to defendant for limited purpose; both defendants liable for using beyond that purpose through an “implied duty”); *see also* *Griff Machine Prod. Co. v. Griptron Sys., Inc.*, Civil Action No. C84-434, 1985 U.S. Dist. LEXIS 18462, at \*22 (N.D. Ohio June 27, 1985) (implying NDA for information obtained during “subcontract and sales negotiations” where defendants “should have known” of secrecy); *Wilkes v. Pioneer Am. Ins. Co.*, 383 F. Supp. 1135, 1142 (D.S.C. 1974) (implying NDA where defendant had obtained secret from plaintiff under conditions giving rise to expectation of confidentiality).

Courts also employ the concept when a new employer disclaims any knowledge that its new hire misappropriated the plaintiff's trade secrets. These courts look at facts suggesting that the new employer should have connected the dots between the employee's work product and his or her former job.<sup>44</sup>

Many cases addressing questions of constructive knowledge are older, dating from before the UTSA was enacted. In one, a defendant used a plaintiff's allegedly secret mold obtained under a confidentiality agreement to produce products for a second defendant. The court held that a trade secret claim was stated against the second defendant because, citing the Restatement formulation of trade secret law, a defendant who knows of a breach of confidentiality by another is liable, and a defendant who receives notice of a breach of confidentiality is liable from that point onwards "provided that he has not in good faith paid value for the secret."<sup>45</sup> In another, there was a question whether a defendant had a duty of inquiry notice about the provenance of a design it had obtained from a contractor. The court found a triable issue of fact under the Restatement approach, noting that the defendant had "a long history of attempting to gain intelligence about [plaintiff's] electro-mechanical feeders by surreptitious means."<sup>46</sup> Under these cases, the general rule appeared to be that if the facts amount to inquiry notice that a party is using someone else's trade secret, that party has a duty to investigate further.

## 2. *Cases Declining to Find Constructive Knowledge*

Cases finding insufficient facts for constructive knowledge appear to be few and far between. A 2012 case from the Northern District of California, for example, found that the plaintiff failed to allege that licensee/purchaser

---

44. *See* *Comput. Assoc. Int'l, Inc. v. Altai, Inc.*, 982 F.2d 693, 719 (2d Cir. 1992) (remanding on constructive notice issue where defendant disclaimed knowledge of its employee's theft of trade secrets); *Rohm and Haas Co. v. Adco Chem. Co.*, 689 F.2d 424, 431 (3d Cir. 1982) (where defendant knew that plaintiff had only method for certain process, and new employee immediately delivered process for making one of plaintiff's products, defendant had at least a duty of inquiry).

45. *See* *Colony Corp. v. Crown Glass Corp.*, 430 N.E.2d 225, 228 (Ill. App. Ct. 1981).

46. *See* *FMC Corp. v. Spurlin*, 596 F. Supp. 609, 616 (W.D. Penn. 1984). For other older cases, see *Curtiss-Wright Corp. v. Edel-Brown Tool & Die Co., Inc.*, 407 N.E.2d 319, 324 (Mass. Ct. App. 1980) (affirming jury verdict against defendant which obtained drawings from the Navy, which had a contract with the plaintiff, where the plaintiff had notified the defendant of its rights); *Metallurgical Indus., Inc. v. Fourtek, Inc.*, 790 F.2d 1195, 1204 (5th Cir. 1986) (finding a triable issue of act on a question whether a defendant had failed to investigate a possible misappropriation where it had purchased a third party entity, and was aware that the entity had been sued by the plaintiff for misappropriation; although the purchased entity told the defendant that the allegations were meritless, the court found that a reasonable jury would find that [defendant] should have inquired" because he "knew of possible problems but did nothing but rely on [third party's] dismissals").

knew or had reason to know that information it acquired from co-defendant included the plaintiff's trade secrets.<sup>47</sup>

In perhaps the most notable case, a 2007 decision from the Central District of California granted summary judgment on a trade secret claim and rejected the plaintiff's argument that the defendant was on constructive notice of an alleged misappropriation.<sup>48</sup> In that case, the court rejected a constructive knowledge argument even though the plaintiff alleged that the corporate defendant had acquired the information from an individual seller in order to frustrate password protection to the plaintiff's software and had been dishonest about curtailing its use of the plaintiff's software.<sup>49</sup> The court noted that the plaintiff's allegations were distinct from facts from which one could infer that the corporate defendant knew that the individual seller "was under a duty to maintain the confidentiality" of the information sold.<sup>50</sup>

Similarly, a 1998 Indiana case refused to imply an obligation of confidentiality or find the "had reason to know" requirement satisfied where a manufacturer disclosed drawings to a competitor, but did not mention the confidentiality of, mark the drawing as confidential, and where evidence of industry custom regarding confidential treatment of such information was inconclusive.<sup>51</sup>

### 3. *The Problem of Notice Letters and Constructive Knowledge*

As noted above, threat letters and so-called reminder letters are common in trade secret law; this author has seen hundreds over the decades. In many instances, a former employer simply sends a polite reminder about confidentiality to a former employee or his or her new employer. In others, the former employer complains of downloading or other file exfiltration and

---

47. *See* *Mediostream, Inc. v. Microsoft Corp.*, 869 F. Supp. 2d 1095, 1114 (N.D. Cal. 2012).

48. *See* *Unicom Sys., Inc. v. Farmers Group, Inc.*, No. CV 04-4604-GHK (AJWx), 2007 U.S. Dist. LEXIS 110825, at \*49–50 (C.D. Cal. June 12, 2007).

49. *See id.*

50. *See id.*

51. *See* *Flotec, Inc. v. S. Rsch., Inc.*, 16 F. Supp. 2d 992, 1006–07 (S.D. Ind. 1998) (finding no implied NDA where manufacturer disclosed drawings to competitor but never mentioned confidentiality, drawings were not marked, and evidence of industry customer not conclusive; should have known prong not satisfied). For similar rulings, see also *Tenax Corp. v. Tensar Corp.*, No. H-89-424, 1990 U.S. Dist. LEXIS 10671, at \*15 (D. Md. May 31, 1990) (no implied agreement where alleged disclosure took place in a context of free flow of information, and where plaintiff waited more than 10 years to assert a confidential relationship; thus, no finding that defendant "should have known"); *U.S. Plywood Corp. v. Gen. Plywood Corp.*, 370 F.2d 500, 508 (6th Cir. 1966) (finding that plaintiff who disclosed alleged secret to prospective licensees had extinguished any secrecy).

seeks remediation short of litigation. Yet others threaten litigation directly. All of this begs the question whether a defendant could be on constructive notice due to receipt of such a letter, especially given the variety of forms they take.

Case law is sparse. On a motion to dismiss in 2016, two corporate officers argued that the plaintiff did not state a claim against them for misappropriation, in addition to arguing that they could not be liable for acts of employees.<sup>52</sup> The court denied the motion after examining the DTSA's "reason to know" language.<sup>53</sup> It noted that the plaintiff had alleged that it sent the company a "cease and desist" letter, asking it to explain how it obtained certain customer contact information.<sup>54</sup> The plaintiff also alleged that it sent a second letter a week later, but that the defendants "denied possession of this information and, apparently, took no steps to prevent" the corporate defendant "from using this information." The court found that this sufficed to state a claim under a constructive knowledge theory.<sup>55</sup>

Two early cases from California also offer examples. A 1977 ruling found a director liable for an employee's misappropriation where he was aware of a letter accusing the employee of misappropriation and then, after the lawsuit was filed, undertook development of the technology at issue. The case states that an employer can be liable "provided that he utilizes the information with notice of the secret nature thereof and with notice that the employee has disclosed it in breach of his duty to the former employer."<sup>56</sup> This conclusion seems dubious: receiving a threatening letter plus continuing to do business cannot be enough for employer liability. People send threatening letters all the time, and not all such letters reflect a well-researched accusation. Similarly, a 1966 case found two directors liable for misappropriation because "they were notified . . . that the corporation of which they were directors was making unauthorized use of trade secrets improperly transmitted to it by . . . [others],

---

52. *See* *Solarcity v. Pure Solar Co.*, No. CV 16-01814-BRO (DTBx), 2016 U.S. Dist. LEXIS 199522, at \*12–14 (C.D. Cal. Dec. 27, 2016).

53. *See id.*

54. *See id.* For a case featuring a letter but a defendant further afield from the action, see *Smart Mort. Ctrs., Inc. v. Noe*, No. 21-cv-3606, 2022 U.S. Dist. LEXIS 49580, at \*21–22 (N.D. Ill. Mar. 21, 2022) (granting motion to dismiss as to corporate defendant where motion focused on "the state of mind required for DTSA trade secret misappropriation"; as to a downstream corporate defendant which worked with a primary defendant, the plaintiff alleged that someone associated with the primary defendant was an "undisclosed principal" of the downstream corporate defendant and alleged that he had received a legal letter notifying him of trade secret allegations; court found that plaintiff failed to plead that the downstream corporate defendant had acquired the alleged trade secrets as of the date of the letter, and thus dismissed the claim).

55. *See id.*

56. *See* *Cybertek Comput. Prods., Inc. v. Whitfield*, 203 U.S.P.Q. 1020, 1025 (1977).

their fellow directors. They and the corporation nonetheless continued to use these manufacturing processes. Thus they, too, are liable.”<sup>57</sup> This case is questionable for the same reason.

C. IMPUTED KNOWLEDGE IS NOT A SUBSTITUTE FOR ACTUAL OR CONSTRUCTIVE KNOWLEDGE

Because trade secret liability can turn on constructive knowledge—what one had reason to know—this raises the intriguing question of whether a business could be liable through the imputed knowledge of an executive who learned trade secrets at a former employer. The answer should be “no,” as otherwise the meaning of “misappropriation” would be stretched outside the DTSA/UTSA statutory boundaries into strict liability.

Imputed knowledge is a common law doctrine providing that, at least in the case of high-ranking employees, the company is deemed to know what that employee knows. The doctrine is a legal fiction; a person with imputed knowledge is deemed to have gained that knowledge by operation of law. For example, California law—which is governed by a statutory definition of imputed knowledge—classifies it as a form of constructive notice: “[i]mputed knowledge is constructive, not actual knowledge.”<sup>58</sup>

It is easy to see how a former employer might have an appetite for this theory in bringing a trade secret lawsuit. A plaintiff might argue that a competing business which hired one of its executives has imputedly learned its trade secrets, simply by hiring her. The former employer might accordingly argue that merely to hire the individual amounts to an unlawful acquisition of trade secrets. Or, such a plaintiff might even use the argument to bolster an argument for an “inevitable disclosure” injunction, which posits that a court should fire an employee from a new job on the premise that the employee will at some future point engage in a trade secret misappropriation that has not yet occurred.

All such theories should fail. To start, imputed knowledge clashes with the text of the UTSA, which provides—as described above—that constructive knowledge be premised on a finding that the defendant “had reason to know” that one was acquiring someone else’s trade secret without authorization to do so. Strictly speaking, imputed knowledge does not meet that test, even if it is

---

57. *See* *Components for Rsch., Inc. v. Isolation Prod., Inc.*, 241 Cal. App. 2d 726, 729–30 (Cal. Ct. App. 1966) (citing RESTATEMENT OF TORTS § 758[b]).

58. *See* *Cal. Ins. Guar. Assn. v. Workers’ Comp. Appeals Bd.*, 163 Cal. App. 4th 853, 863 (2008) (discussing Cal. Civ. Code § 2332). “And it has been held . . . that section 2332 of the Civil Code [defining when principal is “deemed to have notice” of agent’s notice] should not be applied to meet the requirement of actual knowledge.” *Rosenthal v. Garner*, 142 Cal. App. 3d 891, 895 (1983) (citing *Ismay v. Tyler*, 169 Cal. App. 2d Supp. 883, 885 (1959)).

described by some courts as a species of constructive knowledge. Rather than calling for a “had reason to know” inquiry, it could impose a finding of knowledge simply because someone remembers a trade secret, but never shares it with her new employer.

But even if a trade secret plaintiff could otherwise leverage imputed knowledge under the “had reason to know” language of the DTSA and the UTSA in order to buttress a claim of unlawful acquisition, the argument should still fall short. This is so because the common law has long recognized an important exception to the imputed knowledge: a principal is not deemed to know what which an agent is duty-bound not to disclose.

Although the cases are scattered across many decades, they are uniform in holding that where an agent has a duty to a third party to hold information in confidence, such information will not, as a matter of law, be imputed to the principal.<sup>59</sup> Some 150 years ago, the United States Supreme Court faced an argument that an agent had fraudulently acquired property, but the principal was unaware of the fraud and asserted that it was an innocent purchaser.<sup>60</sup> While applying the general rule of imputed knowledge against the principal, the court was careful to describe an exception. As the court explained, where “it is not the agent’s duty to communicate such knowledge, when it would be unlawful for him to do so, as, for example, when it has been acquired confidentially as an attorney for a former client in a prior transaction,” the general rule does not apply.<sup>61</sup> Cases since then, in a variety of circumstances, have examined and sometimes applied the exception the Supreme Court described.<sup>62</sup>

Given the temptation to short-cut the rules for finding intent in trade secret cases, it is unsurprising that trade secret plaintiffs have sought to impose

---

59. See cases cited *infra* notes 59, 61.

60. See *The Distilled Spirits*, 78 U.S. 356, 367 (1871).

61. See *id.* (“When it is not the agent’s duty to communicate such knowledge, when it would be unlawful for him to do so . . . the reason of the rule ceases; and in such a case an agent would not be expected to do that which would involve the betrayal of professional confidence, and his principal ought not to be bound by his agent’s secret and confidential information.”).

62. For various examples, see generally *In re Marriage of Cloney*, 91 Cal. App. 4th 429, 441 (2001) (finding information non-confidential as predicate to imputing it to principal); *Reininger v. Prestige Fabricators, Inc.*, 136 N.C. App. 255, 261 (1999) (refusing to impute third party confidential information to principal); *Davenport v. Correct Mfg. Corp.*, 24 Ohio St. 3d 131, 134 (1986) (“knowledge would not be imputed to the principal if the agent acquired it while acting in a position of confidentiality”); *Imperial Fin. Corp. v. Fin. Factors, Ltd.*, 53 Haw. 203, 207 (Haw. 1971) (“An exception to the general rule imputing knowledge from the agent to the principal is most frequently applied when . . . the agent acquires confidential information, creating a duty not to disclose such information to his principal.”).

liability through imputed knowledge. For example, the Ninth Circuit reversed a jury finding of misappropriation in a 1976 case where the corporate defendant's employee had received the plaintiff's allegedly confidential idea for the design of a backpack.<sup>63</sup> Although the defendant had hoped to pursue a defense of "subsequent independent invention" for the backpack design the plaintiff sued over, the court instructed the jury that "[i]t is not a defense to the corporation that [the employee] did not inform other officers" regarding his knowledge of the plaintiff's idea.<sup>64</sup>

This jury instruction imputed liability to the corporation by eviscerating its fact-based defense that others at the company who had not learned of the plaintiff's idea had independently designed the challenged backpack concept. The Ninth Circuit reversed, noting that despite the general rule of imputed knowledge under California law, "[i]n light of the emphasis in trade-secret law on unfair use, it is generally not appropriate to direct a jury to impute an agent's knowledge of a secret to the principal. Such an instruction would permit recovery even when the trade secret was not actually communicated to or used by the principal. The plaintiff is not entitled to a windfall when in fact there has been no invasion of those interests which trade-secret law seeks to protect."<sup>65</sup>

A 2016 case in Arizona rejected a trade secret plaintiff's argument for a finding of imputed liability. In *Joshua David Mellberg, LLC v. Will*, a magistrate judge faced a fact pattern where an employee had downloaded files from a prior employer.<sup>66</sup> The judge refused to impute knowledge of those files to the company, because the imputed knowledge doctrine generally does not apply regarding an agent's knowledge of "a secret to the principal" that has not been "actually communicated or used by the principal."<sup>67</sup>

The result would differ, however, where the agent/employee is not someone who merely remembers a trade secret from a former job, but learns a trade secret from a third party in the course of employment with the corporate defendant. In such straightforward scenarios—that is, outside the employee-mobility context—courts may indeed find imputed knowledge.<sup>68</sup>

---

63. See *Droeger v. Welsh Sporting Goods Corp.*, 541 F.2d 790, 792–93 (9th Cir. 1976).

64. *Id.*

65. *Id.*

66. *Joshua David Mellberg, Ltd. Liab. Co. v. Will*, No. CV-14-02025-TUC-CKJ (CRP), 2016 U.S. Dist. LEXIS 32412, at \*42 n.2 (D. Ariz. Jan. 22, 2016).

67. See *id.* (citing *Droeger*, 541 F.2d at 792–93).

68. See *Myerburg v. Medtronic, Inc.*, No. 03-20616-CIV-COOKE/MCALILEY, 2004 U.S. Dist. LEXIS 31385, at \*30–31 (S.D. Fla. Sept. 29, 2004) (where plaintiff alleged that defendant's agents met with him and heard his ideas, court agreed that agents' knowledge was imputed to the defendant, but that finding did not matter "since Plaintiff did not have a trade

### III. THE OVERLOOKED SAFE HARBOR FOR TRADE SECRET MISTAKES AND ACCIDENTS

We turn now from an examination of how trade secret law defines intentionality to questions of intent in three instances of secondary liability. Each is a situation where a plaintiff seeks to hold a company defendant liable (or seeks to enhance its liability) as a follow-on claim of misappropriation—that is, for the acts of employees or business partners. Each is a situation where the courts have not yet adequately defined exceptions to liability in these secondary contexts. Our first question focuses on DTSA and the UTSA statutory language which can foreclose, or limit, liability in certain cases of “accident or mistake.”

#### A. THE DTSA/UTSA “ACCIDENT OR MISTAKE” SAFE HARBOR CLAUSE

As described, each act of “misappropriation” in the UTSA and DTSA requires actual or constructive knowledge. This begs the question whether there could be liability where a party innocently obtains another’s trade secret without even constructive knowledge, and uses it under the belief that it has a right to do so.

The answer under the DTSA and the UTSA is “no,” at least where the use of the trade secret (or the preparation to use it) before receiving notice is “material.” Both statutes provide what we will term a safe harbor for defendants who use a trade secret without the required level of intent that doing so violates another party’s rights. The statutes expressly permit accidental or mistaken acquisition of a trade secret, and use of it. Specifically, the UTSA defines its third and final form of “misappropriation” to exclude such mistaken or accidental use:

b) “Misappropriation” means:

(1) Acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or

(2) Disclosure or use of a trade secret of another without express or implied consent by a person who:

---

secret” in the idea he shared); *see also* Darton Env’t, Inc. v. Fjuvo Collections, LLC, 332 F. Supp. 3d 1022, 1038 (W.D. Va. 2018) (denying motion to dismiss where two individual defendants had viewed plaintiff’s allegedly secret technology and each was accused of misusing it with two spin-off companies that each was involved with; court noted that “[a]t this stage, those two [corporate defendants] can be imputed the knowledge of their principals”).

- (A) Used improper means to acquire knowledge of the trade secret;  
or
- (B) At the time of disclosure or use, knew or had reason to know that his or her knowledge of the trade secret was:
- (i) Derived from or through a person who had utilized improper means to acquire it;
  - (ii) Acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or
  - (iii) Derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or
- (C) Before a material change of his or her position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.<sup>69</sup>

The DTSA contains nearly identical language.<sup>70</sup> This “accident or mistake” concept has an antecedent. Specifically, the 1939 Restatement of Torts—which provided the structure for the states’ adjudication of trade secret disputes before the UTSA’s gradual enactment—contained a largely similar clause. It stated that:

One who learns another’s trade secret from a third person without notice that it is secret and that the third person’s disclosure is a breach of duty to the other, or who learns the secret through a mistake without notice of the secrecy and the mistake

(a) is not liable to the other for a disclosure or use of the secret prior to receipt of such notice, and

(b) is liable to the other for a disclosure or use of the secret after the receipt of such notice, unless prior thereto he has in good faith paid

---

69. For two UTSA examples, see CAL. CIV. CODE § 3426.1(b) and WASH. REV. CODE 19.108.010(2)(b)(iii) (Washington); *see also* UNIFORM TRADE SECRETS ACT WITH 1985 AMENDMENTS § 1(2), <https://www.uniformlaws.org/viewdocument/final-act-128>. As discussed further below, a number of states’ UTSA enactments cross-reference this clause in the remedies sections of the statute with additional language that speaks to what remedies are (or are not) available when the safe harbor clause applies. Moreover, as the UTSA enactments vary somewhat from state to state, not every jurisdiction is uniform. New Jersey, for example, appears to provide a safe harbor for material reliance without notice that is broader than just accidents and mistakes; its version of the clause reads “before a material change of position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired through improper means.” N.J. REV. STAT. 56:15-2. Oregon, by contrast, omitted that clause entirely, while keeping the safe harbor limitations discussed below in its remedial sections. *See* OR. REV. STAT. §§ 646.461(2)(d); 646.463(2); 646.465(1).

70. *See* 18 U.S.C. § 1839(5)(b)(iii) (definitions of “misappropriation”).

value for the secret or has so changed his position that to subject him to liability would be inequitable.<sup>71</sup>

One notable difference between the Restatement's formulation and that of the UTSA and DTSA is whether there is protection for one "who has in good faith paid value for the secret" after acquiring it, but before receiving notice that it does not have a right to use the trade secret. Under the Restatement version, an innocent buyer faces no liability. As the Commentary to § 758 put it, "[o]ne who actually pays value in good faith for a trade secret prior to receipt of notice as stated in this Section is relieved of the duty to which receipt of notice would otherwise give."<sup>72</sup>

In other words, the Restatement made a sharp distinction between one who innocently purchased a trade secret and one who innocently received it for free. In the latter case, the Restatement did not provide complete immunity, and courts instead were to weigh the facts and balance interests: "But not every change of position prevents the recipient of a trade secret from being subjected to the duty not to disclose or use the trade secret after purchase. The issue is whether the imposition of a duty would be inequitable under the circumstances."<sup>73</sup>

The UTSA and DTSA present a more nuanced answer. They dropped the absolute protection for innocent purchasers, as no such language appears in either statute.<sup>74</sup>

---

71. See RESTATEMENT OF TORTS § 758 (1939). Another restatement expressed a similar principle. The Restatement of Agency noted that a party which obtains "confidential information" from an agent but does not have "notice of its confidential nature, although paying no value, is not subject to liability for revealing the secret to others; if before notice he has paid value for the information, he is not subject to liability to the principle for its subsequent use." See RESTATEMENT OF AGENCY (SECOND) § 312, cmt. c (1958); see also Note, *Protection and Use of Trade Secrets*, 64 HARV. L. REV. 976, 981 (1951) ("If through mistake or betrayal, disclosure is received innocently without paying value, liability should start only as of the time notice is received." (citing the Restatement)).

72. See RESTATEMENT OF TORTS § 758 cmt. e. (1939) ("[I]t is deemed fairer and more consistent with the general principles underlying the protection of the interests in trade secrets to permit him to enjoy the expectancies of the investment."). Notably, this language focuses on buyers, and not licensees, though there is no way to know if that was an intentional choice.

73. See *id.*

74. See UNIFORM TRADE SECRETS ACT WITH 1985 AMENDMENTS § 2 cmt., <https://www.uniformlaws.org/viewdocument/final-act-128> ("With respect to innocent acquirers of misappropriated trade secrets, Section 2(b) is consistent with the principle of 4 Restatement Torts (First) § 758(b) (1939), but rejects the Restatement's literal conferral of absolute immunity upon all third parties who have paid value in good faith for a trade secret misappropriated by another. The position taken by the Uniform Act is supported by *Forest Laboratories, Inc. v. Pillsbury Co.*, 452 F.2d 621 (CA7, 1971) in which a defendant's purchase of assets of a corporation to which a trade secret had been disclosed in confidence was not

At the same time, the UTSA and the DTSA preserved a before-and-after distinction for the period before one receives notice and the period after one receives notice seen in the Restatement, which used the phrases “prior to receipt” and “after the receipt.”<sup>75</sup> The Restatement made clear that an innocent acquiror’s activity before receiving notice would not subject it to liability.<sup>76</sup> For the period after receipt of notice, however, the innocent acquiror “is liable for a disclosure or use of the secret after notice,” unless “his position has changed prior to receipt of notice,” which “may relieve him from the effects which notice would otherwise have[.]”<sup>77</sup> The UTSA and the DTSA employ language that is less clear, but which recognizes the same constructs regarding the timing of receiving notice and the possibility that the innocent acquiror has undertaken a material change of position before receiving such notice.<sup>78</sup>

## B. INTERPRETING THE STATUTORY SAFE HARBOR FOR ACCIDENTS AND MISTAKES

This language offers one way to avoid, or to limit, secondary liability for trade secret misappropriation. But the “accident or mistake” language in the UTSA and DTSA requires some unpacking. The statutes do not define what acquisition by accident or mistake means, but the necessary implication is some form of receipt of the trade secret without actual or constructive knowledge of the information’s status. The statutes also do not define a “material” change of position, but again the necessary implication is some use of the trade secret where the bell would be difficult to unring.

### 1. *The UTSA’s Official Commentary*

The UTSA’s commentary on the “accident or mistake” clause is a model of poor writing; it does not explain what is most important about that clause. The comments tell us that the safe harbor clause is distinct from a situation where a party loses trade secret rights altogether by failing to use proper

---

considered to confer immunity upon the defendant.”); *see also* James Pooley, TRADE SECRETS § 2.03[3] at n.26 (“The Uniform Act “rejects the [First] Restatement’s literal conferral of absolute immunity upon all third parties who have paid value in good faith for a trade secret misappropriated by another.”). The other well-known trade secret treatise does not discuss this UTSA and DTSA language. As it was first written decades ago and so often is frankly outdated, it briefly notes the older Restatement formulation without much illumination. *See* MILGRIM ON TRADE SECRETS § 7.02[2][d].

75. *See* RESTATEMENT OF TORTS § 758 (1939).

76. *See id.*, cmt. c (“One is not liable for a disclosure or use prior to receipt of notice, under the rule state in Clause (a), whether he has paid value for the secret or received it free.”).

77. *See id.*, cmt. d.

78. *See* UNIFORM TRADE SECRETS ACT WITH 1985 AMENDMENTS § 1(2)(ii)I (“Before a material change of his or her position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.”).

security measures: “[t]he type of accident or mistake that can result in a misappropriation under Section 1(2)(ii)(C) involves conduct by a person seeking relief that does not constitute a failure of efforts that are reasonable under the circumstances to maintain its secrecy under Section 1(4)(ii).” This seems to say that a plaintiff’s sloppiness in guarding its trade secrets may lead to an accident or mistake on the part of another actor that does *not* result in “misappropriation” where the safe harbor might apply.<sup>79</sup> That would make sense, as plaintiff’s failure to use reasonable security measures simply negates trade secrecy, before a court would even reach the question whether there was misappropriation. Even so, this comment is notably unilluminating, and not merely because it is expressed in the negative.<sup>80</sup> It does not explain why the UTSA drafters felt it necessary to contrast the requirement that a trade secret holder employ reasonable security measures with this exception to the definition of “misappropriation.” It does not provide concrete examples to illustrate the point it struggles to make. It fails to tell us what kinds of “accidents or mistakes” the UTSA encompasses or what constitutes a “material” change in position. And it fails to specify the conditions under which a defendant which has materially changed its position may continue to use the trade secret after receiving notice: indefinitely, for some reasonable period of time, or not at all.

## 2. *The UTSA Drafting History*

By contrast, we find some clues as to the meaning of the “accident or mistake” clause in the 1970s committee proceedings that led to the UTSA. As early as 1972, for example, the drafters of what was tentatively called the “Uniform Trade Secrets Protection Act” expressed the safe harbor principle ultimately seen in the act:

The tentative proposal of the Special Committee is to limit the remedies available against a person who as acquired knowledge of a misappropriated trade secret in good faith, provided that person has materially and prejudicially changed his position prior to notice of misappropriation. On the other hand, if that person has not detrimentally relied on his innocently acquired knowledge, we would

---

79. *See* UNIFORM TRADE SECRETS ACT WITH 1985 AMENDMENTS § 1 cmt, <https://www.uniformlaws.org/viewdocument/final-act-128>. By contrast, the DTSA commentary does not offer insights regarding the accident-or-mistake term. *See* Report 114-220, Senate Committee on the Judiciary, Defend Trade Secrets Act of 2016, at 3 (Mar. 7, 2016) (noting that the DTSA’s definition of misappropriation is modeled on the Uniform Trade Secrets Act).

80. *See id.*

subject him, following notice, to the same remedies as a bad faith misappropriation[.]<sup>81</sup>

The committee further noted that “in other words, he can continue to use it himself, notwithstanding the notice,” where he had “materially and prejudicially changed his position prior to notice of misappropriation,” but might be enjoined from “further disclosure to third parties.”<sup>82</sup>

By 1978, the definition of “misappropriation” had a carve-out for acquisition by mistake without notice, but there was not yet language governing whether one would avoid liability for changing one’s position before receiving notice:

(1) “Misappropriation” means:

[ . . . ] (ii) Disclosure to others or use of a trade secret of another without the latter’s express or implied consent where a person:

[ . . . ] (B) At the time of disclosure or use, knew or had reason to know that:

[ . . . ] (III) Knowledge of the trade secret was acquired by mistake.<sup>83</sup>

Discussions at the time showed confusion over this language, and whether it was meant to refer to the trade secret holder’s failure to use reasonable security measures to protect it—a requirement that a valid trade secret exists in the first place. One committee member asked “Whose mistake are we talking about here? If it’s the mistake of the employer, certainly there should be no penalty in this going into the public domain.”<sup>84</sup> Another committee member asked a question along the same lines: “with reference to knowledge of a trade secret that’s acquired by mistake, I would be pleased to have a little more indication of what you mean by ‘mistake.’”

Supposing the person who develops the trade secret—and let’s say he’s the holder, or the owner, if you believe there’s property involved here—and he just goes and leaves written version of it around, and somebody picks it up, is that the kind of mistake that you are talking about?

---

81. Proceedings in Committee of the Whole, Uniform Trade Secrets Protection Act, Aug. 10, 1972, at 19.

82. *Id.* at 20.

83. *See* Proceedings in Committee of the Whole, Uniform Trade Secrets Protection Act, Aug. 3, 1978, at 11.

84. *Id.* at 13–14.

If it is the situation where he has sold the secret to somebody else, who is using it under some kind of arrangement, and that person is negligent?"<sup>85</sup>

In response, another committee member sought to clarify that the clause was intended to be distinct from the separate requirement that a valid trade secret be the subject of reasonable security measures:

I think we were thinking of the Restatement concept. Their illustrations typically involved misdelivered memos and letters. If a person is negligent in maintaining secrecy, under the definition of a 'trade secret'—if they are negligent enough, that can forfeit them protection. So if the negligence goes to the reasonableness of the efforts to maintain secrecy, you can lose protection. But if you just misdeliver something that you are trying to keep confidential, you can impose liability.<sup>86</sup>

The most important debate took place in the 1979 committee proceedings. By that time, the key phrase had been revised to read "at the time of the acquisition of the trade secret, knew or had reason to know, that it was a trade secret and that knowledge of it had been acquired by accident or mistake."<sup>87</sup> There was, as yet, still no language protecting the party which changed its position before receiving notice that the information it had acquired by accident or mistake was someone else's trade secret.

As with the 1978 proceedings, there was a question about what the clause meant, and an explanation that it was not the same as the requirement that the trade secret holder use reasonable security measures or lose its rights.<sup>88</sup> One committee member, however, noted that the concept of a mistake could apply to a downstream acquiror:

In this section [ . . . ] it is possible for someone to have acquired the information not directly from the person who had first acquired it by accident or mistake. There could be a channel through which this information could go. Or, alternatively, at the time the information was acquired by the person who was about to use it, they may not have been aware that their source had obtained it by accident or mistake.

Am I correct that if they are innocent of knowledge of it at the time of acquisition, but later learned that their source was tainted, in the

---

85. *Id.* at 23.

86. *Id.*

87. Proceedings of the Committee of the Whole—Uniform Trade Secrets Act, Aug. 6, 1979 at 3–4.

88. *See id.* at 8–9, 13–14.

sense of having acquired it by accident or mistake, but not by improper means, they are free to use the information without violation of the trade secret?”<sup>89</sup>

The response sought to clarify whether or not one has notice as the key issue in determining whether one acquiring the secret by accident or mistake would be deemed to have engaged in “misappropriation.”<sup>90</sup> Another commentator sought to differentiate “negligent conduct” by the trade secret holder, and receipt by accident or mistake.<sup>91</sup> And, finally, a commentator noted the risk that a party acquires a trade secret by accident or mistake without notice, and acts in good faith by using it:

You have a situation where there is a disclosure. A person starts to use this, and develops an alternate system. A person tools up prior to finding out that it is a trade secret. At what point are you going to protect the person who in good faith acted on this information, but has not yet put it on the market? At what point does ‘use’ cut it to protect this individual?”<sup>92</sup>

This question seems to have led the committee to draft the final language seen in the UTSA, with the concept that there is a safe harbor if one acquires a trade secret by accident or mistake, and before receiving notice, undertakes “a material change of his position.”<sup>93</sup> That said, there appears never to have been a clear statement speaking to all possibilities. As a committee member noted when explaining this language, “[a]nd the result of that is that if you acquire, knowing that you have acquired, by accident or mistake, then you are a misappropriator. If you acquire not knowing that, but know it before you disclose or use it, you are a misappropriator. But if you acquire and disclose or use before you know that it was by accident or mistake, you are not a misappropriator.”<sup>94</sup> However, this explanation does not define what happens in the case of a “material change of position,” especially after one subsequently receives notice that the information is a trade secret.

### 3. *The Restatement’s Unsatisfactory Examples*

These comments suggest that the UTSA drafters slowly worked toward a position that would protect defendants in cases of secondary liability, where the party has received the trade secret mistakenly and has already begun some

---

89. *Id.* at 14–15.

90. *See id.* at 15–17, 23–25, 27–28.

91. *See id.* at 19–20.

92. *Id.* at 38.

93. *See id.* at 116–117.

94. *Id.* at 117.

significant use of it without actual or constructive knowledge that the information belongs to someone else. However, neither these comments, nor the official comments to the final UTSA, offer much in the way of concrete examples.

By contrast, the 1939 Restatement did provide examples where an innocent acquiror could have avoided liability—though some seem whimsical through today’s eyes, and none are particularly useful for contemporary analysis. For example, it imagined a scenario where two potential buyers were trying to buy a trade secret, and the owner accidentally sent a letter revealing the secret to one of them with no strings attached.<sup>95</sup>

But some of its other scenarios of accident or mistake would be equally plausible today, especially where the innocent acquiror has materially changed its position by using the trade secret before receiving notice. In such circumstances, the Restatement invited readers to consider the equities where a party innocently obtained a trade secret, and before receiving contrary notice it (1) “makes a substantial investment in plant and machinery for the use of the secret”; (2) “liquidates another business in order to establish a new business on the basis of the secret”; or (3) “makes substantial expenditures in surveys and research preparatory to establishing the business in an effort to improve the secret process.”<sup>96</sup> The Restatement noted, as a counterweight, that a party who “merely makes up his mind to do something in the future or carries on negotiations with others [ . . . ] is not undergoing a change of position sufficient to relieve him from liability[.]”<sup>97</sup>

#### 4. *Interpreting the Accident and Mistake Language for Real-World Scenarios*

The DTSA/UTSA safe harbor, to be sure, is qualified: it does not apply if the defendant receives some form of notice or information that the plaintiff has rights in the trade secret, after accidental or mistaken acquisition, but before first doing anything with the trade secret. On the other hand, the language appears to state that if the defendant has materially changed its position when it lacked such notice, “misappropriation” does not exist. Presumably, in at least some circumstances, the defendant can continue the unintentional use it has made of the trade secret even after receiving notice.

But again, the statutes do not define what kind of notice would be sufficient to preclude the safe harbor. If a plaintiff sends a cease-and-desist letter, but the defendant reasonably disputes the claim, is that sufficient? The UTSA commentary—again with poor phrasing that seems contradictory—

---

95. See RESTATEMENT OF TORTS § 758, cmt. c., illus. 3 (1939).

96. See *id.*, cmt. e.

97. See *id.*

suggests both that notice “makes” one “a misappropriator” while simultaneously stating that a court can decline to enjoin that party after balancing the interests:

The prejudice to a good faith third party justification for withholding prohibitory injunctive relief can arise upon a trade secret owner’s notification to a good faith third party that the third party has knowledge of a trade secret as a result of misappropriation by another. This notice suffices to make the third party a misappropriator thereafter under Section 1(2)(ii)(B)(I). In weighing an aggrieved person’s interests and the interests of a third party who has relied in good faith upon his or her ability to utilize information, a court may conclude that restraining future use of the information by the third party is unwarranted.<sup>98</sup>

This tells the reader little about what type of notice would suffice to make one a “misappropriator,” much less what kind of notice would weigh more strongly than others in determining whether the innocent acquiror may continue to use the trade secret at issue. It also does not explain the statute’s “material change of position” language and how it might alter the conclusions expressed in the comment. Indeed, the statement “[t]his notice suffices to make the third party a misappropriator thereafter” does not explain whether that would be true for the defendant which has so changed its position in reliance on the information it innocently acquired.

More important than notice, then, what kinds of change of position are “material,” and which are immaterial? One can imagine a scenario where a defendant has only just begun using a trade secret in product development without wrongful intent—and another situation where the defendant has already launched a product into the market using someone else’s trade secret, and plans to continue to do so based on the business unit it has built for that purpose. Would both defendants receive safe-harbor protections, or only the latter? Either way, is such protection finite, or permanent—and would future use be subject to any payment by the defendant?<sup>99</sup>

---

98. *See* UNIFORM TRADE SECRETS ACT WITH 1985 AMENDMENTS § 2 cmt., <https://www.uniformlaws.org/viewdocument/final-act-128>.

99. It may be tempting to look at definitions of materiality, or reliance, in other areas of law for guidance. But these terms are used so often, and in so many different contexts, that it feels arbitrary to choose one or another to plug in for an analogy. For example, public companies have to decide what lawsuits and other legal events are material enough to include in SEC filings, reliance is a key aspect of fraud lawsuits, while § 2-209 of the Uniform Commercial Code speaks of weighing the effect of a “material change of position” on a waiver between contracting parties. U.C.C. § 2-209. Rather than attempting to cherry-pick words from some other, unrelated context to offer in some metaphorical sense, we should consider

Said differently, is the safe harbor an immunity lasting indefinitely, or a temporary protection that lasts solely until the defendant receives notice that the information is a trade secret? Either way, does the answer differ in different circumstances? The well-known Pooley treatise asserts that the language means the latter, and that receipt of notice even where one has used the trade secret as “a particular step in a complex manufacturing process” could “immediately” turn a party into a “misappropriator” “upon receiving notice of the facts.”<sup>100</sup> It similarly states that “when the recipient is put on notice, then he is prospectively liable for misappropriation.”<sup>101</sup>

But that position overstates the language in the UTSA and its official commentary. Certainly, the UTSA and the DTSA tell us that a defendant who receives notice after an accidental or mistaken receipt, but before use, is a misappropriator with respect to such use. But for those defendants who have materially changed their position in the meantime, a reading of the entire text suggests that there is a meaningful degree of allowance for the reliance the defendant made upon its good-faith belief that the information was available for its use—an allowance which should continue into the future to at least some degree. To that extent, use following a material change of position is not “misappropriation” or at least is not subject to the range of remedies available for ordinary misappropriation. The statutes suggest that this outcome is not a remote possibility, but instead an intended outcome.

If it were otherwise—that is, if one’s liability automatically kicked in upon notice, despite materially changing one’s position before receiving such notice, the material-change-of-position language in the DTSA and the UTSA would serve no purpose. The statute would instead refer to receiving notice, full stop, as the point at which “misappropriation” begins. It would not need to contemplate whether or not the defendant had materially changed its position before notice. Something close to strict liability for “misappropriation” would instantly arise once a defendant, who innocently acquired a trade secret and

---

circumstances common to trade secret disputes to determine how these statutory terms are best construed.

100. See James Pooley, TRADE SECRETS § 2.03[3] at n.25 (2021) (“In effect this means that an acquiror that had materially changed its position (for example, by including a particular step in a complex manufacturing process) in good faith would not be a “misappropriator,” but could become one immediately upon receiving notice of the facts. As the comment to § 2 points out, however, a court would take into account the circumstances and refuse to grant an injunction, and instead impose a reasonable royalty as consideration for continued use by the misappropriator.”). Of note, I was an editor on the Pooley treatise from 2006–2009 but did not write this portion of the text.

101. See *id.* § 6.04[1] (“Appropriation Without Knowledge of Secrecy”); see also *id.* § 6.04[2] (“The recipient is not subject to liability for use or disclosure unless and until he or she becomes aware that the disclosure was an accident.”).

innocently changed its position by using the trade secret, received notice of the trade secret. Under that reading, the material-change-of-position language would indeed be superfluous: a party without notice would not be liable, whether or not it changed its position before notice, and a party with notice would be liable for any use afterwards, whether or not it changed its position before notice.

The phrase “material change of position” speaks to a different vision. It contemplates some meaningful course of action by the defendant before receiving notice of the trade secret where consequences flowing from that action will continue past the point of notice, rather than a harsh outcome where one who innocently and materially changes its position in reliance on a belief that the information can permissibly be used must pay damages for any continuing use after notice. While a defendant’s new and distinct use or disclosure—one not linked to the material change of position—should be a different story, continuing conduct in line with that change of position would receive safe-harbor protection, to at least some significant degree.

Adding to these interpretive difficulties, some (but not all) states enacted a version of the UTSA that sheds some light on these questions. It contains modified language in the statutory section defining whether and when injunctive relief and monetary relief are possible in cases where the safe harbor clause protects a defendant. Specifically, in the version of the statute finalized in 1985, the remedial sections state that damages are not available when there has been “a material and prejudicial change of position prior to acquiring knowledge or reason to know of misappropriation,” but that in “exceptional circumstances” such as these, “an injunction may condition the defendant’s potential future use upon payment of a reasonable royalty” while a non-use injunction is “inequitable.”<sup>102</sup> In short: the 1985 version of the UTSA permits (but does not require) a court to order a royalty for future use of the trade secret, but damages for past use and a non-use injunction are not allowed when the safe harbor applies. But again, the official commentary does not explain

---

102. See UNIFORM TRADE SECRETS ACT WITH 1985 AMENDMENTS §§ 2–3, <https://www.uniformlaws.org/viewdocument/final-act-128> (see underlined text for changes to this version on these points regarding remedies). Vermont, Massachusetts, and South Dakota are examples of states which enacted this language. *E.g.*, VT. STAT. §§ 4602(b) (“exceptional circumstances” where an injunction can “condition future use” upon payment of a royalty “include a material and prejudicial change of position prior to acquiring knowledge or reason to know of misappropriation that renders a prohibitive injunction inequitable.”); 4603(a)(1) (“Except to the extent that a material and prejudicial change of position prior to acquiring knowledge or reason to know of misappropriation renders a monetary recovery inequitable, a complainant is entitled to recover damages for misappropriation.”); MASS. GEN. LAWS ch. 93 §§ 42A(b), 42B (same); S.D. CODIFIED LAWS. §§ 37-29-2, 37-29-3 (same).

when such a royalty should be ordered, or why, versus when it should not be.<sup>103</sup> And the DTSA, as well as some versions of the UTSA including in technology-heavy jurisdictions such as California and Washington, contain no such language.<sup>104</sup>

It is easy to imagine practical, real-world contexts where full safe harbor protection would make sense. A defendant in the midst of selling a product that contains an innocently-acquired trade secret can hardly hit pause immediately without harm to its business, and delays in redevelopment. The same is true of the hypothetical discussed above in the Pooley treatise, where an innocent acquiror includes a trade secret in a “complex manufacturing process” before receiving notice. Almost any use of a trade secret where the information is embedded into or made part of some larger product, process, or technology would be “material” simply because starting over and removing the information would create meaningful risk, uncertainty, and disruption to an innocent actor. The text of the DTSA and the different versions of UTSA seem to envision that there would be no “misappropriation” in such circumstances, or at least that the sole remedial option of a royalty order could be “inappropriate.”<sup>105</sup>

Certainly the UTSA and the DTSA do not adopt a bona fide purchaser theory where anyone who first obtains a trade secret is free to use it, even if notice comes before such use. The UTSA commentary expressly rejects that possibility, noting that the statute “rejects the Restatement’s literal conferral of

---

103. See UNIFORM TRADE SECRETS ACT WITH 1985 AMENDMENTS §§ 2–3, *supra* note 102.

104. See generally 18 U.S.C. § 1836(b)(3); CAL. CIV. CODE §§ 3426.2–3426.3; WASH. §§ 19.108.020.030.

105. The Pooley treatise points to the language in the 1985 UTSA commentary stating that, after receiving notice, a party could be liable for misappropriation but merely would have to pay a royalty instead of being enjoined. See James Pooley, TRADE SECRETS § 2.03[3] at n.25. The commentary, however, is nuanced. It makes clear that in some cases, at least, a royalty also might be as “inappropriate” as an injunction in such circumstances: “When Section 2(b) applies, a court has discretion to substitute an injunction conditioning future use upon payment of a reasonable royalty for an injunction prohibiting future use. Like all injunctive relief for misappropriation, a royalty order injunction is appropriate only if a misappropriator has obtained a competitive advantage through misappropriation and only for the duration of that competitive advantage. In some situations, typically those involving good faith acquirers of trade secrets misappropriated by others, a court may conclude that the same considerations that render a prohibitory injunction against future use inappropriate also render a royalty order injunction inappropriate.” See UNIFORM TRADE SECRETS ACT WITH 1985 AMENDMENTS §§ 2–3, <https://www.uniformlaws.org/viewdocument/final-act-128>. To be sure, the language is ambiguous. It is unclear whether it is speaking about a situation where party which has innocently acquired a trade secret has received notice before use, after immaterial use, or after a truly material change in condition. Indeed, the problem with the UTSA commentary as a whole is that it does not define or explain the consequences that flow from a defendant’s material change of position before receiving notice that the information is a trade secret.

absolute immunity upon all third parties who have paid value in good faith for a trade secret misappropriated by another.”<sup>106</sup> The result is a more nuanced safe harbor, where the innocent acquiror who commits to using the trade secret into the future, before receiving notice, is granted latitude for at least some measure of continuing use, in recognition of the difficult position it is in.

### C. CASE LAW ON THE SAFE HARBOR REMAINS SCARCE

Case law is exceedingly sparse as to any of these questions.<sup>107</sup> It is almost as if litigants shy away from litigating the mistake-or-accident clause of the DTSA and UTSA. Perhaps the unwieldy thicket of statutory text and UTSA comments scare courts and parties away.

In *Myers v. Williams*, the defendant, a convicted inmate, had argued that his criminal conduct resulted from using a treatment for a sleeping disorder.<sup>108</sup> He submitted a Freedom of Information Act request for information disclosed to regulators about the treatment, and the FDA mistakenly sent him a “document containing the chemical formula for the manufacture” of the treatment.<sup>109</sup> A few months later, the FDA informed the manufacturer, which then requested

---

106. See UNIFORM TRADE SECRETS ACT WITH 1985 AMENDMENTS § 2 cmt., <https://www.uniformlaws.org/viewdocument/final-act-128> (“With respect to innocent acquirers of misappropriated trade secrets, Section 2(b) is consistent with the principle of 4 Restatement Torts (First) § 758(b) (1939), but rejects the Restatement’s literal conferral of absolute immunity upon all third parties who have paid value in good faith for a trade secret misappropriated by another. The position taken by the Uniform Act is supported by *Forest Laboratories, Inc. v. Pillsbury Co.*, 452 F.2d 621 (CA7, 1971) in which a defendant’s purchase of assets of a corporation to which a trade secret had been disclosed in confidence was not considered to confer immunity upon the defendant.”); see also James Pooley, TRADE SECRETS § 2.03[3] (“The sixth type of misappropriation arises from accidental or mistaken disclosure. Liability for damages for disclosure or use is imposed if, before a material change of position, the defendant knew or should have known that the information was a trade secret and that it had been acquired by accident or mistake. Although Section 1 of the Act does not specifically address the issues, the official comments in Section 2 of the Act state that providing notice to a previously innocent acquiror ‘suffices to make the third party a misappropriator thereafter.’ This is a departure from the common law as defined in the *Restatement of Torts*, which excused a good faith user from any liability.”).

107. Indeed, commentary by academics or practitioners on the “accident or mistake clause,” or any kind of treatment in the case law, is almost non-existent, even though some versions of the UTSA have been in force for more than 40 years. An occasional case will mention the clause as dicta, or in a passing reference, but not in the context of an innocent acquiror. *E.g.*, *Compulife Software, Inc. v. Newman*, 959 F.3d 1288, 1313 (11th Cir. 2020) (noting, when remanding a case where two of the defendants obtained knowledge of a database, that the trial court could have decided that if their receipt was an accident or mistake, they were on notice and use thus would have been misappropriation).

108. *Myers v. Williams*, 819 F. Supp. 919, 920–21 (D. Or. 1993)

109. *Id.*

that the inmate destroy all copies.<sup>110</sup> The defendant refused, and “instead attempted to sell” the formula to other pharmaceutical companies.<sup>111</sup>

On this extremely unusual set of circumstances, the court granted a preliminary injunction under the Oregon UTSA, and found that the statute’s accident-or-mistake clause did not apply.<sup>112</sup> The court reasoned that the defendant was aware he had received the trade secret formula by mistake, and that there was “no evidence that [he] had undergone a material change in position since acquiring” it, and instead “persisted” in threats to disclose it to others.<sup>113</sup>

In a more apposite fact pattern, the Eastern District of New York faced a 1981 case where a game manufacturer received a game idea via a solicitation from a trusted source.<sup>114</sup> Unbeknownst to the defendant, the game idea originated with the plaintiff and had wrongfully been taken.<sup>115</sup> Although the defendant primarily won judgment as a matter of law because it established that it had independently developed its own game, it also won under § 758 of the Restatement (the predecessor to today’s DTSA/UTSA safe harbor clause). Specifically, the court found that even if the defendant had received notice that the game idea was the plaintiff’s trade secret and even if it had used the idea, it had changed its position by spending on “tooling and other production components, for advertising, and possibly some inventory.”<sup>116</sup> Thus, under § 758 it could not be liable because liability would subject it to loss “for action taken when there was no such duty.”<sup>117</sup> This appears to be the only fully-developed case to apply the safe harbor principle for a use of trade secrets before receiving notice.

A 1971 case, also under the Restatement, was later cited by the Uniform Act’s drafters.<sup>118</sup> In *Forest Labs, Inc. v. Pillsbury Co.*, the defendant had purchased assets from a third party which had been subject to a confidentiality agreement

---

110. *Id.*

111. *Id.*

112. *Id.*

113. *See id.* at 921.

114. *See Vantage Point, Inc. v. Parker Bros., Inc.*, 529 F. Supp. 1204, 1214–15 (E.D.N.Y. 1981).

115. *See id.* at 1208.

116. *Id.* at 1215.

117. *Id.* at 1216.

118. UNIFORM TRADE SECRETS ACT WITH 1985 AMENDMENTS § 2 cmt., <https://www.uniformlaws.org/viewdocument/final-act-128> (“The position taken by the Uniform Act is supported by *Forest Laboratories, Inc. v. Pillsbury Co.*, 452 F.2d 621 (CA7, 1971) in which a defendant’s purchase of assets of a corporation to which a trade secret had been disclosed in confidence was not considered to confer immunity upon the defendant.”).

with the plaintiff.<sup>119</sup> The plaintiff alleged that the third party had divulged its trade secret to the defendant in a manufacturing process, via the asset purchase.<sup>120</sup> However, the asset purchase did not transfer the third party's liabilities to the purchaser, because the defendant was not a successor to the third party.<sup>121</sup>

This begged the question whether the defendant, as an innocent acquiror, could be liable under Wisconsin's pre-UTSA, Restatement-based trade secret common law. The Seventh Circuit thus analyzed § 758.<sup>122</sup> Although the defendant had paid for the assets its purchased, the court evaded the good-faith-purchaser exception in § 758 by finding that there was no evidence that the defendant "paid value for [plaintiff's] trade secret" as opposed to a more general asset purchase, and on that basis found that it "remained liable to [plaintiff] for using the trade secret after receipt of notice."<sup>123</sup> The court was not called upon to consider whether the defendant had materially changed position before receiving notice of the trade secret. The decision is unsatisfactory, and feels forced, because the court introduced a self-created notion—separating the purchase of assets including the trade secret from a purported separate value of the trade secret—to impose liability. That outcome is not consonant with the DTSA and UTSA statutory text and thus should have little purchase today.

In a case with some similarities but key differences, a court in 1980 declined to apply the Restatement's § 758 safe harbor where a firm providing account management services for a defendant obtained copies of backup tapes containing the plaintiff's trade secrets in a complicated fact pattern where it at first did not know that its receipt was improper.<sup>124</sup> However, it did not pay any value for those tapes and thus could not rely on § 758 of the Restatement to avoid liability.<sup>125</sup>

Finally, while the Alabama Supreme Court once held that a defendant could be liable under that state's Trade Secrets Act for continuing to use a trade secret after receiving notice, the statute in question notably differs from the UTSA and the DTSA by not including an exception for those who have

---

119. *See* *Forest Labs., Inc. v. Pillsbury Co.*, 452 F.2d 621, 624–25 (7th Cir. 1971).

120. *Id.*

121. *Id.* at 625–26.

122. *See id.* at 626–627.

123. *Id.* at 627.

124. *See* *Comput. Print Sys., Inc. v. Lewis*, 422 A.2d 148 (Pa. Super. Ct. 1980).

125. *See id.* at 151, 155–56.

materially changed position before receiving such notice.<sup>126</sup> It thus sheds no light on interpretive questions in other jurisdictions.

D. REVIVING THE SAFE HARBOR AS A DEFENSE TO MISAPPROPRIATION CLAIMS

Because the case law regarding the “accident or mistake” clause is almost nonexistent, it is not clear exactly what one must do to sufficiently change position before receiving notice in order to avoid liability. Notwithstanding the dearth of cases construing it, the plain purpose of the DTSA/UTSA safe harbor is to protect defendants—whether completely or to some meaningful degree—who innocently receive trade secrets, get entangled through material reliance by using the trade secret before receiving notice, and then face litigation.

Indeed, there are countless everyday contexts where the DTSA/UTSA safe harbor clause could protect an innocent defendant which has used a trade secret by accident or mistake. Consider that in many business-to-business transactions, the seller or licensor provides representations and warranties—and even a promise of indemnification—that it is providing information or technology it has a right to provide. Absent some indicia that something is amiss, an ordinary buyer or licensee is entitled to rely on such representations, and in fact must do so in order to engage in such transactions. To that end, indemnity clauses protecting the buyer are not constructive notice as they are common and agnostic to the circumstances. That a good attorney negotiates for such a clause is not constructive notice that anything is amiss.

It is easy to imagine parties such as a licensee of source code, a licensee of a semiconductor design, a party which outsources chemistry work to a contracted entity for a life sciences pharmaceutical development project using what they receive—indeed, materially relying on an innocently-received trade secret by embedding or commingling it—as just one part of a larger development or design. In such cases, it is also easy to imagine that it would be difficult, disruptive, and expensive to unring the bell and remove such information and replace it. Thus, if such a party were to receive notice (whether convincing or not) that a plaintiff claimed trade secret rights in what the third party provided, the DTSA/UTSA safe harbor clause should be raised as not only a defense to misappropriation, but as a basis to continue such use.<sup>127</sup>

---

126. See *IMED Corp. v. Sys. Eng'g Assoc.*, 602 So.2d 344 (1992) (construing Alabama's trade secret statute (ALA. CODE. § 8-27-3)).

127. This is not to suggest that applications of “accident or mistake” should be limited to such business transactions, only that this seems the most likely instance when litigants and courts should be attuned to the statutory safe harbor.

#### IV. VICARIOUS LIABILITY AS A SUBSTITUTE FOR INTENT—AND ITS EXCEPTIONS

We turn now to the question of vicarious liability, where a trade secret plaintiff seeks to hold a new employer liable for the acts of an employee who has switched jobs. A question of intentionality looms large here, especially in lawsuits where a former employer alleges that a departing employee downloaded (or retained) files from the job and uses that accusation to engage in wide-ranging and costly discovery into the hiring company's development efforts. As the deep pocket, the corporate defendant also potentially faces monetary remedies for the individual's download. But while some such downloading episodes are significant, many are trivial. Nonetheless, even the latter is a low barrier to entry, so to speak, where a former employer files suit against the new employer and impose millions in discovery costs on an opponent. So it is notable that defendants in such cases have not explored exceptions to vicarious liability more robustly, as a means to limit at least some such cases.

Because so many trade secret cases feature employees who have changed jobs, and because so few trade secret cases feature accusations that company management knowingly colluded with newly-hired employees, courts have often had to grapple with questions of a company's vicarious liability for the actions of employees. These problems of secondary liability arise when company management does not know or suspect what an employee has done, such that the ordinary rules of actual and constructive knowledge under the DTSA/UTSA—as discussed above—would not result in liability for the corporate defendant.

Because the UTSA does not mention vicarious liability, courts have had to decide if the doctrine applies in misappropriation cases. Notwithstanding one prominent exception, almost all courts have agreed that traditional common law rules that govern whether an employer is liable for the act of an employee apply in trade secret cases. That said, few have gone further, and asked when the doctrine does not apply to an employer which lacked intent to engage in wrongdoing. The question matters because separating employee liability from the liability of a new employer can be an important tool to thwart overreaching lawsuits filed by former employers.

##### A. THREE EARLY CASES ON VICARIOUS LIABILITY UNDER THE UTSA

Two early cases set the tone. Notably, and importantly for the proposals this Article will advance, both suggested that vicarious liability was not automatic, and that there are defenses an employer can raise against it. A 2001 decision in the Eastern District of Virginia was perhaps the most influential

case to grapple with the application of vicarious liability under the UTSA. *Newport News Industries v. Dynamic Testing, Inc.* held that the Virginia UTSA does not displace the common law of vicarious liability, but instead merely allows for a defense to vicarious liability when the employer has innocently made a material change of position before receiving notice of the misappropriation.<sup>128</sup>

In reaching its holding, the *Newport News* court reviewed the history of the UTSA and compared vicarious liability for other torts and statutory violations. It also examined the preemption clause of the Virginia statute, which states that it “displaces conflicting tort, restitutionary, and other law of this Commonwealth providing civil remedies for misappropriation of a trade secret.”<sup>129</sup> The court reasoned that vicarious liability is not a conflicting cause of action or remedy that would be preempted by the UTSA, but instead “it is a legal precept that presupposes the existence of an underlying claim and assesses liability not because of the act giving rise to the claim but because of a certain status.”<sup>130</sup>

The court also considered the possibility that an employer might escape liability where it did not reasonably have notice of an employee’s act of misappropriation. It held open the possibility of a defense to liability on such ground, noting that “[c]ontrary to the Defendants’ position, the exception for a material and prejudicial change in position before discovery of the misappropriation in both the injunction and damages sections [of the UTSA] does not preclude respondeat superior liability, but instead provides a *defense* to

---

128. See *Newport News Indus. v. Dynamic Testing, Inc.*, 130 F. Supp. 2d 745, 754 (E.D. Va. 2001).

129. *Id.* at 751.

130. *Id.* The court added that one cannot bring an independent tort claim for vicarious liability, to distinguish it from the type of claims preempted by the UTSA, and noted that the Virginia UTSA does not expressly preclude vicarious liability. Subsequent Virginia UTSA cases have held that vicarious liability is available, albeit without such detailed statutory analysis. See generally *Microstrategy, Inc. v. Business Objects, S.A.*, 331 F. Supp. 2d 396, 418 (E.D. Va. 2004) (“The defendant contends that respondeat superior is inapplicable in this case because its employees signed an employment agreement forbidding them from obtaining or using confidential information from competitors. This argument is unavailing. One can act in the scope of one’s employment even if the specific acts performed are explicitly forbidden by the employer, so long as the act was intended to further the employer’s interests rather than being wholly motivated by personal interest. Moreover, the employer need not even be aware of its employee’s activity.”); *Tao of Sys. Integration, Inc. v. Analytical Serv. & Materials, Inc.*, 299 F. Supp. 565, 575 (E.D. Va. 2004) (stating rule and holding that claim was properly stated against employer); *Physicians Interactive v. Lathian Sys., Inc.*, No. CA-03-1193-A, 2003 U.S. Dist. LEXIS 22868, at \*28–29 (E.D. Va. Dec. 5, 2003) (granting request for preliminary injunction and holding that plaintiff had shown a likelihood that employee was acting in course and scope of his employment for apparent misappropriation, and thus vicarious liability argument likely to succeed).

vicarious liability for innocent employers.”<sup>131</sup> With respect to such a defense, the court explained that “[o]ne can imagine that an employer could be liable for the wrongful acts of his employee, but could not qualify for the exception because it has not yet made a ‘material’ or ‘prejudicial’ change of position.”<sup>132</sup>

Minnesota courts also faced the question of vicarious liability under the UTSA early on, and also focused on limits to liability under such a theory. In *Hagen v. Burmeister & Associates*, an insurance salesperson reached an apparent agreement with his former employer allowing him to solicit certain customers but not others. The new employer was aware of the agreement, but not the details, and it was aware that the salesperson began soliciting many customers of the former employer, which duly sued for claims including trade secret misappropriation.<sup>133</sup>

After a 1999 appellate decision ruled that vicarious liability is available in misappropriation cases—pointing to its availability for intentional torts more generally—the state supreme court accepted that premise for purposes of appeal.<sup>134</sup> The lower courts had struggled with the question of vicarious liability where the new employer believed that its newly-hired salesperson had an agreement with the former employer allowing some degree of customer solicitation.<sup>135</sup> The high court held that in the case at issue, the employer was not vicariously liable for the acts of its employees, where Minnesota’s version of the theory requires that “the tort is related to the employee’s duties” and is “foreseeable” in the sense that the act is the type of “well-known industry hazard” that should fairly be allocated to a company’s costs of doing business.<sup>136</sup> That was so because, under the Minnesota law of vicarious liability, the plaintiff had failed to show that the act of misappropriation was foreseeable because it did not introduce any evidence to establish that “the risk of employees misappropriating trade secrets is a well-known hazard in the

---

131. See *Newport News*, 130 F. Supp. 2d at 752 (emphasis in original).

132. *Id.* at 754 n.4.

133. See *Hagen v. Burmeister & Assoc., Inc.*, 633 N.W.2d 497, 500–02 (Minn. 2001).

134. See *id.* at 504; see also *Hagen v. Burmeister & Assoc., Inc.*, C8-98-864, 1999 Minn. App. LEXIS 85 (Minn. Ct. App. Jan. 26, 1999) (intermediate appellate decision). The state supreme court noted that it accepted that vicarious liability is available under the Minnesota because the appellate court had so ruled, and because the corporate defendant did not specially appeal that ruling. See *Hagen*, 633 N.W.2d at 504; see also Tanya Dobash, *Trade Secret Theft & Employer Vicarious Liability in Hagen v. Burmeister & Assoc., Inc.*, 29 WM. MITCHELL L. REV. 375 (2002) (providing detailed case analysis).

135. See *Hagen*, 633 N.W.2d at 501–02 (explaining lower court history).

136. *Id.* at 505 (explaining state’s “scope-of-employment” test, which also includes whether the “tort occurs within work-related limits of time and place”).

insurance industry.”<sup>137</sup> Like *Newport News*—the other early, foundational case on UTSA vicarious liability—*Hagen* pointed to the limits of vicarious liability, and a defense to it.

By contrast, there is only one major court ruling holding that the Uniform Trade Secrets Act does not provide for vicarious liability. In *Infinity Products v. Quandt*, an Indiana appellate court found that a departing employee took documents with him relating to customer contact information.<sup>138</sup> When the employee arrived at his new employer, he immediately began contacting those customers and using pricing information to negotiate sales. The trial court had found that there was insufficient evidence that the new employer was vicariously liable.<sup>139</sup> The appellate court looked to the rulings in Virginia and Minnesota discussed above finding that vicarious liability is available under the UTSA, held that it was likewise available under the Indiana version, and reversed the trial court.<sup>140</sup>

But the state supreme court decided otherwise. The Indiana high court held that the UTSA displaces the common law of vicarious liability because the statute’s express terms (regarding actual or constructive knowledge in order to engage in misappropriation) require “scienter” by the employer.<sup>141</sup> The court also placed emphasis on the UTSA’s preemption clause, which is typically used to eliminate overlapping tort causes of action, and held that it applied to vicarious liability as well.<sup>142</sup>

## B. COURTS HAVE VIRTUALLY ALWAYS FOUND VICARIOUS LIABILITY AVAILABLE

Notwithstanding *Infinity Products*, seemingly every court since has taken the majority approach, leaving Indiana as an outlier. For example, in a 2017 case applying the Ohio UTSA, the District of Minnesota explained that “[n]early every UTSA jurisdiction has held that similar provisions suggest vicarious liability,” and noted that the UTSA’s preemption clause that displaces

---

137. *Id.* at 505 (“We will not assume, absent introduction of some evidence, that UTSA violations are a common hazard in the insurance industry.”).

138. *Infinity Prod., Inc. v. Quandt*, 775 N.E.2d 1144, 1147–48 (Ind. Ct. App. 2002) (overruled by state supreme court decision discussed below).

139. *Id.* at 1152.

140. *See id.* at 1152–53.

141. *Infinity Prods., Inc. v. Quandt*, 810 N.E.2d 1028, 1034 (Ind. 2004).

142. *Id.*; There does not appear to have been much law on the issue in Indiana since. *E.g.*, *Patriot Homes, Inc. v. Forest River Housing, Inc.*, No. 3:05-CV-471 AS, 2007 U.S. Dist. LEXIS 70697, at \*11 (N.D. Ind. Sept. 20, 2007) (noting the *Quandt* standard and stating that, although vicarious liability is unavailable under the Indiana UTSA, the plaintiff can still seek to show that the new employer is directly liable; finding that because the new employer “turned a blind eye as to what was happening,” a defense motion for summary judgment failed).

conflicting tort remedies does not apply to a remedy that is not a free-standing cause of action.<sup>143</sup> Similarly, a 2013 case in the Northern District of California rejected a defense argument that the doctrine did not apply. It held that “[t]he majority view, however, is that the UTSA does not preempt the *respondeat superior* doctrine,” and that a defendant “cannot prevail at summary judgment merely by arguing that it was not aware of the acts of its employees[.]”<sup>144</sup> Many others have followed suit.<sup>145</sup>

The same is true for the only state without a trade secret statute, New York. A New York trial court denied a motion to set aside a jury verdict in a case where a former law firm associate, used impersonation to access confidential client information from his former firm..<sup>146</sup> As to vicarious liability, the court affirmed the jury’s findings that the associate’s conduct took place within the scope of employment and that the employer had ratified the conduct because the associate had brought in an extraordinary number of new clients, whose client intake forms a partner had signed.<sup>147</sup> It noted that a jury could correctly have found that the firm “should have conducted a more thorough inquiry as to where the clients were coming from.”<sup>148</sup>

---

143. *See* *Deluxe Fin. Serv., LLC v. Shaw*, No. 16-3065 (JRT/HB), 2017 U.S. Dist. LEXIS 122795, at \*10–12 (D. Minn. Aug. 3, 2017) (“Because OUTSA’s statutory provisions align with the majority of UTSA jurisdictions, the Court believes the Ohio Supreme Court would follow the majority approach.”).

144. *Language Line Serv., Inc. v. Language Serv. Assoc., Inc.*, 944 F. Supp. 2d 775, 783 (N.D. Cal. 2013) (denying motion for summary judgment where defendant argued it could not be liable under the California UTSA for acts of employees).

145. *See e.g.*, *Navigation Holdings, LLC. v. Molavi*, No. 19-CV-02644-LHK, 2020 U.S. Dist. LEXIS 154268, at \*10 (N.D. Cal. Aug. 25, 2020) (denying motion to dismiss where defendant alleged plaintiff failed to plead vicarious liability; citing cases for proposition that an employer can be vicariously liable for trade secret misappropriation committed within the scope of employment, and at least in part to benefit the employer, even if the employer has forbidden it); *Brain Injury Ass’n of Cal. v. Yari*, No. CV 19-5912-MWF (JCx), 2020 U.S. Dist. LEXIS 120201, at \*17–18 (C.D. Cal. Apr. 30, 2020) (same); *Solarcity Corp. v. Pure Solar Co.*, 2016 U.S. Dist. LEXIS 199522, at \*14–15 (same); *MTG Guarnieri Mfg., Inc. v. Clouatre*, 2010 Okla. Civ. App. LEXIS 52, at \*33–34 (Okla. Ct. App. June 17, 2010) (noting, in reversing summary judgment, that employer might be liable for misappropriation for acts of its employees under *respondeat superior*, defined as “willful torts of an employee acting within the scope of employment in furtherance of assigned duties”); *Thola v. Henschell*, 164 P.3d 524, 528–529 (Wash Ct. App. 2007) (holding that UTSA did not displace common law rules of vicarious liability).

146. *Rosenberg, Minc & Armstrong v. Mallilo & Grossman*, 8 Misc. 3d 394, 398, 399 (N.Y. Sup. Court Mar. 24, 2005). The plaintiff brought claims including “misappropriation” which appears to have been more or less equivalent to a trade secret misappropriation claim, as the court noted it was based on “confidential information.”

147. *Id.* at 400.

148. *Id.*

Because many companies use contractors—as distinct from full-time employees—questions also arise about vicarious liability for trade secret misappropriation by a contractor. The Missouri Supreme Court considered such a question in 2014.<sup>149</sup> In that case, someone signed an agreement as an “independent contractor” which also stated that the contractor had no right to bind the company by his actions.<sup>150</sup> He was accused of misappropriating the plaintiff’s customer list and using it for the benefit of the defendant, but the defendant never accessed the list and had no way of knowing it had been pilfered.<sup>151</sup> Because the plaintiff had not alleged any kind of employer/employee or principal/agent relationship, the court affirmed a finding that there was no vicarious liability.<sup>152</sup>

That outcome begs the question of the result when the plaintiff is careful enough to allege an agency relationship against a company which hired a contractor accused of misappropriation. While trade secret case law appears sparse,<sup>153</sup> common law principles indicate that contractor liability may well be possible in a similar manner to vicarious liability, but it is less clear. Taking California as an example, principle/agent liability questions turn on factors such as the principal’s selection of the contractor and the degree to which the contractor’s work was observable and influenceable. At the same time, courts may consider whether the contractor’s duty is of a type found to be nondelegable.<sup>154</sup> This type of test is hardly an automatic endorsement of liability for a contractor’s actions but indicates that such liability is possible.

---

149. *See* Cent. Trust and Invest. Co. v. Signalpoint Asset Mgm’t, LLC, 422 S.W.3d 312, 322 (Mo. 2014).

150. *Id.* at 323.

151. *Id.* at 322.

152. *See id.* at 323.

153. *See* Great Am. Opportunities, Inc. v. Cherrydale Fundraising, LLC, No. 3718-VCP, 2010 Del. Ch. LEXIS 15, at \*81–85 (Del. Ch. Jan. 29, 2010) (unpublished) (in a case with claims including misappropriation of trade secrets, finding no vicarious liability as to one company for actions of another, where “scant” evidence did not establish either a “servant” relationship or sufficient evidence of control over an independent contractor).

154. *See* Barry v. Raskov, 232 Cal. App. 3d 447, 453 (1991) (“Today, however, the exceptions have so overwhelmed the “general rule” it is more accurate to say the employer of an independent contractor will generally be held liable for the contractor’s torts and that nonliability is the exception.”). *Barry* was not a trade secret case but noted that liability for the acts of an independent contractor is commonplace despite an earlier common law rule to the contrary. *See id.*; *see also* Vargas v. FMI, Inc., 233 Cal. App. 4th 638, 646–50 (2015) (discussing factors for agency liability with independent contractors).

C. STATES USE DIFFERENT TESTS TO APPLY VICARIOUS LIABILITY IN TRADE SECRET CASES

In deciding whether vicarious liability applies as a general rule—as opposed to whether it is theoretically available under the trade secret statutes—courts apply the existing common law test in each state.<sup>155</sup> Such tests can differ. Taking California as an example, that state provides that an employer is liable for torts committed by an employee who acts within the scope of their employment, regardless of whether the employee acted in excess of their authority, or contrary to instructions they received.<sup>156</sup> In turn, whether an act was committed within the scope of employment depends on (1) whether the act was required by, or incident to, the employee’s duties; or (2) whether the act could reasonably be foreseen as an outgrowth of the employee’s duties.<sup>157</sup> That test puts at least some weight on an employer’s expectations.

Applying these principles, in *Cisco Systems, Inc. v. Chung*, the Northern District of California defined vicarious liability as a rule where employers are liable for torts of employees, committed within the scope of their employment, including intentional, unauthorized torts, as long as there is a causal nexus between the wrongful act and the employee’s work, and the act was undertaken at least in part to benefit the employer.<sup>158</sup> The court also noted that an

---

155. One might wonder why we focus here on the UTSA, rather the federal DTSA. The DTSA does not speak to vicarious liability, and it does not preempt state law (which is why a plaintiff can bring both DTSA and UTSA claims together in the same lawsuit). See 18 U.S.C. § 1838 (“Except as provided in section 1833(b), this chapter shall not be construed to preempt or displace any other remedies, whether civil or criminal, provided by United States Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret[.]”). Generally speaking, when federal statutes are silent as to vicarious liability, state law fills the gap. See *Meyer v. Holley*, 537 U.S. 280, 285 (2003) (analyzing the Fair Housing Act, which “says nothing about vicarious liability”; “[T]he Court has assumed that, when Congress creates a tort action, it legislates against a legal background of ordinary tort-related vicarious liability rules and consequently intends its legislation to incorporate those rules.”). Thus, especially where a trade secret plaintiff can already bring a parallel UTSA cause of action, a DTSA claim would seemingly incorporate the same vicarious liability rules as the state law governing the UTSA claim.

156. See Witkin, SUMMARY OF CALIFORNIA LAW § 115 (collecting many cases); see also Judicial Council of California, CACI 3700, 3720 (jury instructions for “vicarious responsibility” and scope of employment).

157. See *id.*

158. 462 F. Supp. 3d 1024, 1056–57 (N.D. Cal. May 26, 2020) (on motion to dismiss, finding that plaintiff stated misappropriation claim under vicarious liability theory).

employer can be directly liable where it ratifies an employee's act even if the act was originally unauthorized.<sup>159</sup>

Similarly, in a case where the court issued a preliminary injunction over a customer list, it enjoined the new employer as well as individual employees based on a vicarious liability theory.<sup>160</sup> The court noted that “California and federal courts have allowed vicarious liability claims under the UTSA,” and found evidence that the new employer was aware that the employees stated that they would bring business with them from the plaintiff.<sup>161</sup>

Other states' tests appear to place little if any weight on the employer's state of mind. For example, where employees of a corporate defendant obtained and used documents that clearly contained the plaintiff's confidentiality markings, a court found in a bench-trying case that the corporate defendant was vicariously liable under the Pennsylvania UTSA.<sup>162</sup> The court noted that “[t]he near unanimous consensus of federal and state courts holds that the Uniform Trade Secret Act . . . does contemplate vicarious liability when state law otherwise provides the cause of action.”<sup>163</sup> It applied Pennsylvania's common law test—which asks whether the employee's wrongful act was similar in kind to the job the employee was hired for, whether it occurred substantially within the time and space boundaries of the employer, and was motivated at least in part to benefit the employer—and found all elements present.<sup>164</sup>

Under Georgia law, a 2011 case applied that state's test—“courts will hold an employer responsible for the conduct of its employee if the employee acted in the course of the employer's business and with a desire to benefit the employer”—in finding a likelihood of vicarious liability to support a preliminary injunction.<sup>165</sup> Three employees, whom the corporate defendant had hired, took files containing trade secrets and used them to solicit healthcare facilities their former employer worked with.<sup>166</sup> A new co-worker

---

159. *Id.* at 1057 (finding that plaintiff stated a claim under this theory because it alleged that defendant's executives did not reprimand the employee for making disclosures or caution him against doing so).

160. *Extreme Reach, Inc. v. Spotgenie Part., LLC*, No. CV 13-07563-DMG (JCGx), 2013 U.S. Dist. LEXIS 201300, at \*20–21 (C.D. Cal. Nov. 22, 2013).

161. *Id.*

162. *Advanced Fluid Sys., Inc. v. Huber*, 295 F. Supp. 3d 467, 486 (M.D. Pa. 2018).

163. *Id.* at 472.

164. *Id.*

165. *Amedisys Holding, LLC v. Interim Healthcare of Atlanta, Inc.*, 793 F. Supp. 2d 1302, 1314 (N.D. Ga. 2011) (noting that there would be no vicarious liability for a purely personal act by an employee).

166. *Id.* at 1309.

had asked “when we meet can u please brng ur cheat sheet lol u have from [former employer].”<sup>167</sup>

#### D. CONTEXTS WHERE VICARIOUS LIABILITY IS INAPPLICABLE

Although early, foundational cases regarding vicarious liability under the UTSA—*Newport News* and *Hagen*—pointed to situations where the doctrine would not apply, cases addressing exceptions to vicarious liability appear to be rare.

There should be many situations where vicarious liability does not apply.<sup>168</sup> Indeed, given the frequency of lawsuits filed against departing employees and new employers, it is surprising that litigants seem to have only rarely argued such points, and that courts have been inattentive to these issues. There may be practical explanations, of course: intellectual property practitioners may be less familiar with doctrines based in employment law, a distinct field. And at a more mundane level, law firm associates tasked with writing briefs are more likely to work from existing trade secret cases found in online databases, rather than crafting less-familiar arguments anew.

---

167. *Id.* at 1314.

168. Although vicarious liability is recognized in other areas of intellectual property law, the fact patterns generally involve third parties the defendant is able to control, and thus offer trade secret law little by way of analogy. *See, e.g.,* *Sentius Int'l, LLC v. Apple Inc.*, 2020 U.S. Dist. LEXIS 192203, \*12-13 (N.D. Cal. Oct. 2015) (collecting authorities; noting that because “[p]atent infringement is a tort action . . . [p]atent law thus presumptively incorporated vicarious liability principles,” but noting that in both patent and copyright law, the doctrine is about control over the actions of third parties); *Kilina Am., Inc. v. SA & PW, Inc.*, No. CV 19-03786-CJC (KSx), 2019 U.S. Dist. LEXIS 230737, at \*5–6 (C.D. Cal. Aug. 27, 2019) (same; granting motion to dismiss on claim for vicarious copyright infringement where plaintiff did not sufficiently allege that one business had control over another accused of infringing pattern designs); *Luvdarts, LLC v. AT&T Mobility, LLC*, 710 F.3d 1068, 1071–72 (9th Cir. 2013) (affirming motion to dismiss where plaintiff alleged that mobility messaging network was vicariously liable for messages sent on its networks that allegedly infringed copyrights; explaining that vicarious copyright liability requires both the right and ability to supervise the infringing activity and a direct financial stake in that activity); *Louis Vuitton Malletier, S.A. v. Akanoc Sol. Inc.* 591 F. Supp. 2d 1098, 1113 (N.D. Cal. 2008) (noting that vicarious trademark infringement requires that the defendant and the infringer have a partnership or apparent partnership with the ability to bind one another or exercise joint ownership over the infringing product; granting summary judgment where website provider had no such relationship with infringer); *cf. Cambridge Univ. Press v. Becker*, No. 1:0B-CV-1425-ODE, 2010 U.S. Dist. LEXIS 149486, at \*43–44 (N.D. Ga. Sept. 30, 2010) (in a copyright case turning on whether employees acted within the scope of employment for purposes of vicarious liability, finding that university instructors who used copyrighted materials outside the boundaries of fair use were acting within the scope of employment unless they engaged in “egregious” violations of university’s copyright policy).

One situation with potentially broad application is the fact pattern where a departing employee downloads files from the prior employer before leaving the company. That action—which takes place when the individual is still employed by the former employer, and before they commence work for the new employer—raises the question whether vicarious liability could apply to such acts by employees in transit between jobs, especially if nothing further happens to the downloaded files. If, for example, a departing employee shares company files containing trade secrets to a personal cloud storage account when leaving the company, but then never transfers the files to the new employer’s storage networks, such actions would have taken place entirely outside, and antecedent to, the course and scope of work for a new employer.

An unpublished Washington case from 2014 suggests one approach. In *Kassa Insurance Services, Inc. v. Pugh*, an employee took a customer list containing trade secrets when leaving his prior job.<sup>169</sup> The court noted that “[u]nder the doctrine of respondeat superior, an employer or principal is vicariously responsible for the torts of an employee or agent who is acting on the employer’s or principal’s behalf.” But it also noted that, in contrast, if the employee is pursuing a personal objective, the employer is not liable unless, under a theory of ratification, “the employer accepts the benefits of the acts with full knowledge of the facts.”<sup>170</sup> The court affirmed a trial court finding that the employer was not vicariously liable, explaining that the employer had “no control over” the actions of the individual defendant “when he compiled the client list and e-mailed it to himself” before his new employment started, and because the plaintiff failed to establish that the employer knew the client list originated from the plaintiff.<sup>171</sup>

Similarly, a 2023 ruling on a motion to dismiss in the Northern District of California also points the way to robust attention to the limits of vicarious liability. In *Alert Enterprise, Inc. v. Rana*, the individual defendant allegedly downloaded 2600 files, moved additional files to a personal drive, and took steps to “destroy evidence of his actions.”<sup>172</sup> The plaintiff sued the new employer as well, but did not include fact allegations that it received or used the asserted trade secrets the individual had taken.<sup>173</sup> Most important for present purposes, the court found that the plaintiff failed to plead a vicarious liability theory because it did not plausibly allege that the individual was acting

---

169. Nos. 31196-1-III, 31300-0-III, 2014 Wash. App. LEXIS 1036, at \*39–40 (Apr. 29, 2014).

170. *Id.*

171. *Id.* at \*40–42.

172. *Alert Ent., Inc. v. Rana*, No. 22-cv-06646-JSC, 2023 U.S. Dist. LEXIS 44590, at \*2–3 (N.D. Cal. Mar. 16, 2023).

173. *Id.* at \*6, \*13.

as the employer's agent "when he took the trade secrets," or that the new employer ever ratified that act.<sup>174</sup>

It is surprising that rulings like that seen in *Kassa* and *Alert Enterprise* are not more common. If the new employer has never received downloaded files (and thus never acquired or learned any trade secrets within them), if they were downloaded before the employment relationship began, and if the new employer never ratified the downloading, then a trade secret plaintiff seemingly would have to clear significant hurdles to establish a misappropriation by the new employer. On one hand, an employer with some inkling that a new hire was using illicit information would be at least on constructive notice, likely leading to a finding of vicarious liability. On the other, a mere download by an employee leaving the plaintiff's employment seems hardly a basis for liability against the new employer.

Not all employee downloads are the same. That is, not every case where a former employee possesses files from the prior employer is one where the employee downloaded the material with intent to use it in the future. Given the multiplicity of accounts and devices employees use, it is unsurprising that employees often inadvertently retain emails, photos, files, and other documents in personal accounts or devices that were collected in the ordinary course of work, and then forgotten.<sup>175</sup>

In such cases, questions of vicarious liability may not arise at all because the individuals' passive, inadvertent possession is not grounds for trade secret liability against the employee—much less the new employer. For example, in a 2020 case involving Apple, the company hired an employee who "retained [the former employer's] technical information, accessed it while in Apple's employ, and gave misleading statements about how much of it they retained."<sup>176</sup> The court granted summary judgment to Apple on the trade secret claim, reasoning that "showing that employees had the information is not

---

174. *Id.* at \*10–13. Another 2023 ruling addressed a trade secret claim against a distributor which was accused of working with a company founded by the plaintiff's former employees. The court dismissed the claim because the plaintiff alleged no facts that the distributor acquired the alleged trade secrets. More important, it added that the plaintiff "has cited no authority which would support that a distributor which sells a competitor's product, even taking as true that the competitor here engaged in misappropriation of trade secrets, can also be liable for misappropriating trade secrets."; *see Sysco Machinery Corp v. DCS USA Corp.*, No. 5:23-CV-134-BO-RJ, 2023 U.S. Dist. LEXIS 204845, at \*6–7 (E.D.N.C. Nov. 15, 2023) (citing cases referring to conspiracy claims and stating "the weight of the authority supports that there can be no conspiracy or secondary liability for DTSA claims").

175. My personal experience over the years with engineers, scientists, and salespersons suggests that such inadvertence is common.

176. *See Hooked Media Grp., Inc. v. Apple Inc.*, 55 Cal. App. 5th 323, 332 (2020) (affirming summary judgment in favor of defendant).

sufficient to establish that Apple improperly acquired or used it,” and that “by itself, a lack of candor regarding the amount of confidential information the employee kept [does not establish] use or acquisition by Apple.”<sup>177</sup> The court emphasized that “mere possession of information is not enough to establish improper acquisition of a trade secret.”<sup>178</sup> The decision was consistent with earlier California cases which had deigned to find individuals liable for such mere possession of a former employer’s trade secrets.<sup>179</sup>

In sum, while the courts appear to have substantially adopted theories of secondary liability in situations where a company defendant’s management is unaware of misappropriation by an employee, they have not scratched the surface of the limitations to vicarious liability in trade secret practice. Applying the limits to vicarious liability is one way to avoid or reduce the costly discovery and wild accusations against new employers that often result from individual acts of downloading that never make their way to the company. Courts and practitioners should pay closer attention to such limitations given commonplace accusations of downloading against departing employees.

## V. CORPORATE DEFENDANTS AND WAYWARD EMPLOYEES: THE QUESTION OF INTENT FOR ENHANCED DAMAGES

Our third exploration of intentionality in trade secret law focuses on the question of secondary enhanced damages. The DTSA and the UTSA both provide that a defendant can be liable for up to treble damages—and in some jurisdictions, fees and costs as well—for engaging in “willful and malicious misappropriation.” This too is a question of intent, or the defendant’s state of mind. And, as with vicarious liability, interpretive questions arise when a trade secret plaintiff seeks exemplary damages against a corporate defendant for the acts of non-executive employee-defendants.

---

177. *See id.*

178. *See id.* at 333.

179. *See* FLIR Sys., Inc. v. Parrish, 174 Cal. App. 4th 1270, 1279 (2009) (cited by *Hooked Media*, stating rule regarding passive retention in case where former executive possessed a hard drive where he had attempted to download files from a company system in the course of working there, but download did not work and he had drilled holes in the drive to disable it); Gibson-Homans Co. v. Wall-Tite, Inc., 26 U.S.P.Q.2d 1867, 1871 (C.D. Cal. 1992) (finding that employee’s mere possession of notebook containing former employer’s trade secrets not a “threat” of misappropriation under California law); Golden State Linen Serv., Inc. v. Vidalin, 69 Cal. App. 3d 1, 8 (1977) (noting that injunctions against a former employee who competes with his former employer can reach only the “use” of trade secret information, and “not to his mere possession or knowledge of it”).

For example, a court might ask what the employer knew, and with what level of wrongful intent, versus whether the individual employee acted with malice. The company's knowledge and intent might differ from that of the employee. Such different intent could lead to a different outcome, especially where the employee acts without coordinated, top-down instruction. In addition, courts might consider training and policies the company had in place, relative to the size and maturity of the division or department at issue. Specifically, if a company has provided reasonable guidelines or training, in context, to avoid the misuse of trade secrets from former employers and business partners, and if an ordinary employee maliciously engages in misappropriation notwithstanding such reminders, this could be an additional factor discounting the possibility that such malice could be attributed to the corporate defendant.

A. "WILLFUL AND MALICIOUS MISAPPROPRIATION" UNDER THE TRADE SECRET STATUTES

Under the DTSA and most UTSA enactments, a plaintiff can win up to trebled damages if it establishes that the defendant acted with a higher level of wrongdoing: "willful and malicious misappropriation."<sup>180</sup> For example, California's UTSA states that "If willful and malicious misappropriation exists, the court may award exemplary damages in an amount not exceeding twice any award made under [the UTSA damages provisions]."<sup>181</sup>

These formulations show that some heightened level of improper intent is required to obtain enhanced damages beyond simply engaging "misappropriation" by "improper means."<sup>182</sup> Some courts require that this additional showing satisfy a higher burden of proof, namely clear and convincing evidence.<sup>183</sup>

---

180. *See* 18 U.S.C. § 1836(b)(3)(C); UNIFORM TRADE SECRETS ACT WITH 1985 AMENDMENTS at 10, <https://www.uniformlaws.org/viewdocument/final-act-128>.

181. *See* CAL. CIV. CODE § 3426.3. California's version of the UTSA also permits recovery of costs, not just fees. Not every UTSA version is identical. Vermont, for example, provides that "[i]f malicious misappropriation exists, the court may award punitive damages," which is seemingly not capped at treble damages. *See* Vt. St. Ch. 143 § 4603(b).

182. *See* *PetroChoice Holdings, Inc. v. Orobono*, No. 2:19-cv-06152-JMG, 2022 U.S. Dist. LEXIS 7380, at \*13 (E.D. Pa. Jan. 14, 2022) (noting that simply because a party improperly engaged in misappropriation, that does not necessarily mean that it acted willful and maliciously).

183. *See, e.g.,* *Advanced Fluid Sys., Inc. v. Huber*, 295 F. Supp. 3d 467, 493 n.9 (M.D. Pa. 2018) (noting split in case law on this point and finding that it would not matter in that case because the evidence supported a finding of willful and malicious misappropriation "under either standard."); *see also* *Mattel, Inc. v. MGA Ent't, Inc.*, 801 F. Supp. 2d 950, 952 (C.D. Cal. 2011) ("Though the existence of willful and malicious misappropriation is ordinarily

## B. DEFINING “WILLFUL AND MALICIOUS MISAPPROPRIATION”

The meaning of “willful and malicious” acts can vary. Pennsylvania defines the term in its version of the UTSA: it means “intentional acts or gross neglect of duty as to evince a reckless indifference of the rights of others on the part of the wrongdoer, and an entire want of care so as to raise the presumption that the person at fault is conscious of the consequences of his carelessness.”<sup>184</sup> That is an exception, however, as the DTSA and most states do not define the term within the statute or in legislative history.<sup>185</sup> Indeed, as the Fourth Circuit noted in 2021, it could find “not cases that define that term in the context of” the DTSA, while UTSA cases “offer competing definitions, each based on how ‘malice’ is defined in other contexts under the relevant state’s laws.”<sup>186</sup> The court affirmed a trial court jury instruction that the term, under the DTSA and Texas trade secret law, meant an intent to cause injury or harm. Based on the lack of consensus among courts construing the UTSA, it rejected the trade secret claimant’s argument that the instruction should have required a lesser showing of a conscious disregard for the rights of another.<sup>187</sup>

Unlike Pennsylvania, UTSA jurisdictions generally do not define “willful and malicious misappropriation.” As a result, and as the Fourth Circuit noted, a slew of recent cases around the country have imported state common law as a gap-filler to define the term. For example, in *Caudill Seed & Warehouse Co., Inc. v. Jarrow Formulas, Inc.*, the Sixth Circuit affirmed a jury finding of exemplary damages under the Kentucky UTSA.<sup>188</sup> In that case, the defendant’s CEO knowingly asked a newly-hired research scientist from the plaintiff to send a zip file of confidential information, where the scientist told co-workers he had

---

considered a fact that a jury must find by clear and convincing evidence, the court calculates the amount of exemplary damages.”); *Yeti by Molly Ltd. v. Deckers Outdoor Corp.*, 259 F.3d 1101, 1111 (9th Cir. 2001) (finding error in jury damages version over standard; “Nothing in the MUTSA suggests that exemplary damages and attorneys’ fees need to be proved by clear and convincing evidence.”); *Vacco Indus., Inc. v. Van Den Berg*, 5 Cal. App. 4th 34, 54 (1992) (affirming fees award given “jury’s determination, upon clear and convincing evidence, that defendants’ acts of misappropriation were done with malice”).

184. *AgroFresh Inc. v. Essentive LLC*, No. 16-662 (MN), 2020 U.S. Dist. LEXIS 222898, at \*23 (D. Del. Nov. 30, 2020) (quoting 12 Pa. Con. Stat. Ann. § 5302).

185. *See API Americas Inc. v. Miller*, 380 F. Supp. 3d 1141, 1151 (D. Kan. 2019) (noting that the state legislature and the courts had not yet defined the term under the Kansas UTSA); *Kassa Ins. Servs., Inc. v. Pugh*, 2014 Wash. App. LEXIS 1036, at \*14–15 (“Because neither ‘willful’ nor ‘malicious’ is defined by statute, we resort to dictionary definitions for clarification.”).

186. *See Steves and Sons, Inc. v. Jeld-Wen, Inc.*, 988 F.3d 690, 726 (4th Cir. 2021) (affirming trial court’s challenged trade secret jury instructions).

187. *See id.* (also noting the appealing party’s “perfunctory and undeveloped argument” on the point).

188. 53 F.4th 368 (6th Cir. 2022).

something that took six months of research—when he was only one month into his job—and where there was evidence that both planned to use deceit.<sup>189</sup> The court noted that “willful and malicious misappropriation” under the UTSA cannot mean simply intentional misappropriation, as the basic claim already requires intentional conduct. It thus affirmed a jury instruction referring to “behavior motivated by spite or ill will and a disregard for the rights of another with knowledge of probable injury.”<sup>190</sup>

In a 2021 Ohio case granting a motion to dismiss claims for exemplary damages under the DTSA and Ohio UTSA, the court found that the plaintiff had failed to plead allegations to support a claim for “willful and malicious” misappropriation.<sup>191</sup> The plaintiff alleged that the defendant had engaged in misappropriation, but its conclusory recitation of the words “willful” and “malicious” was insufficient to plead sufficient facts to support that theory of recovery. The court held that under Ohio law, a sufficient pleading would require alleging a “state of mind under which a person intentionally does a wrongful act without a reasonable[,] lawful excuse and with the intent to inflict injury or under circumstances from which the law will infer an evil intent.”<sup>192</sup> In the alternative, the court also noted that one might plead “conscious disregard for the rights of others,” which is a “high bar” requiring “a mental state so callous in its disregard for the rights and safety of others that society deems it intolerable.”<sup>193</sup>

Other cases have offered similar formulations. Under the Virginia UTSA, for example, willful and malicious means “acting consciously in disregard of another person’s rights or acting with reckless indifference to the consequences, with the defendant aware, from his knowledge of existing circumstances and conditions, that his conduct probably would cause injury to another.”<sup>194</sup> A Washington court affirmed a finding of willful and malicious misappropriation where the defendant took a customer list. It used a legal dictionary to define willful as “voluntary” or “intentional,” and malicious as

---

189. *Id.* at 376–77, 395.

190. *Id.* at 394–95.

191. *Trent P. Fishers Ent., LLC v. SAS Automation, LLC*, No. 3:20-cv-216, 2021 U.S. Dist. LEXIS 62914, at \*17–19 (S.D. Ohio Mar. 31, 2021).

192. *Id.* at 16 (citing an Ohio case and BLACK’S LAW DICTIONARY).

193. *Id.* at 17. It should be noted that the case refers to “punitive” damages, which is not the same thing as “exemplary” damages, and thus its recitation of the legal standard may not be entirely correct.

194. *See Smart Team Global, LLC v. Humbletech, LLC*, No. 19-CV-4873 (AJN) (BCM), 2022 U.S. Dist. LEXIS 30281, at \*28–29 (S.D.N.Y. Feb. 18, 2022) (applying the DTSA and the Virginia UTSA; ruling on a motion for default and noting that, because the DTSA does not define “willful and malicious,” courts look to the relevant state UTSA for guidance).

“substantially certain to cause injury” and “without just cause or excuse.”<sup>195</sup> It affirmed the trial court’s finding of willful and malicious misappropriation in a case where a defendant took a secret customer list because the taking was voluntary, it was substantially certain that his acts would injure the plaintiff, and he had no just cause or excuse.<sup>196</sup>

Relying on common law definitions, an Ohio court defined the terms as “willful, i.e., done with actual or constructive knowledge of its probable consequences” and “malicious, i.e., done with an intent to cause injury.”<sup>197</sup> The Ninth Circuit affirmed a case finding that under California law, “‘malice’ means conduct which is intended by the defendant to cause injury to the plaintiff or despicable conduct which is carried on by the defendant with a willful and conscious disregard of the rights and safety of others.”<sup>198</sup> And a Florida case construing the DTSA and the state UTSA-found that “[i]n the civil context, statutes that require ‘willful’ behavior are generally interpreted to permit a finding of liability when the complained of behavior is ‘knowing or reckless.’”<sup>199</sup>

Federal district courts have also considered “the duration of misappropriative conduct, the defendant’s consciousness of resulting injury and any efforts to cover up malfeasance,”<sup>200</sup> “the need to deter similar misconduct in the future,”<sup>201</sup> “the amount of compensatory damages awarded,” and “the wealth of the particular defendant[.]”<sup>202</sup> Cases frequently

---

195. *Kassa Ins. Serv., Inc. v. Pugh*, 2014 Wash. App. LEXIS 1036, at \*14–15.

196. *Id.*

197. *Trent P. Fisher Enterprises, LLC v. SAS Automation, LLC*, No. 3:20-CV-216, 2021 U.S. Dist. LEXIS 62914, at \*16–17 (S.D. Ohio Mar. 31, 2021) (citing 4 MILGRIM ON TRADE SECRETS § 15.02 (2020)).

198. *Citcon USA, LLC v. RiverPay, Inc.*, No. 18-cv-2585-NC, 2020 U.S. Dist. LEXIS 163600, at \*14 (N.D. Cal. Sept. 8, 2020) (citing California jury instruction CACI 4411), *aff’d* in relevant part, No. 20-16929, 2022 U.S. App. LEXIS 2717, at \*5 (9th Cir. Jan. 31, 2022).

199. *Behav. Analyst Certification Bd., Inc. v. Rodriguez*, No. 1:21-cv-22834-SCOLA/GOODMAN, 2022 U.S. Dist. LEXIS 135221, at \*30 (S.D. Fla. July 29, 2022), report and recommendation adopted as modified, No. 21-22834-Civ-Scola, 2022 U.S. Dist. LEXIS 174109, at \*30–39 (S.D. Fla. Sept. 26, 2022).

200. *See AgroFresh Inc. v. Essentiv LLC*, 2020 U.S. Dist. LEXIS 222898, at \*73 (quoting *Advanced Fluid Sys., Inc. v. Huber*, 295 F. Supp. 3d 467, 493 (M.D. Pa. 2018), *aff’d* 958 F.3d 168 (3rd Cir. 2020)).

201. *See DiscoverOrg Data, LLC v. Bitnine Global, Inc.*, No. 19-CV-08098-LHK, 2020 U.S. Dist. LEXIS 210494, at \*27–8 (N.D. Cal. Nov. 9, 2020).

202. *See Citcon USA*, 2020 U.S. Dist. LEXIS at \*5; *Proofpoint, Inc. v. Vade Secure, Inc.*, No. 19-cv-04238-MMC, 2021 U.S. Dist. LEXIS 223204, at \*11 (N.D. Cal. Nov. 18, 2021) (similar factors as to amount of damages and wealth of defendant).

offer slightly different standards and wording. We thus lack a nationwide consensus.<sup>203</sup>

At the same time, courts find that merely acting for competitive business motives is insufficient for exemplary damages.<sup>204</sup> For example, in a Pennsylvania case, the plaintiff satisfied the “willful and malicious” standard as to one key defendant who “siphoned [plaintiff’s] trade secrets to [corporate defendant] for almost an entire year,” and “worked tirelessly to divert” contracts from his current employer to a competitor.<sup>205</sup> That defendant also altered “title blocks” on documents, showing his consciousness of wrongdoing, wrongfully downloaded files, and engaged in “wholesale destruction of evidence” after receiving a subpoena.<sup>206</sup> As the court put it, “[w]e struggle to conceive a pattern of conduct more emblematic of willfulness and malice.”<sup>207</sup> However, the court declined to find enhanced damages against other defendants, because their acts were wrongful, but “their motives were purely competitive.”<sup>208</sup>

Echoing that theme, some courts underscore that simply engaging in trade secret misappropriation is insufficient for enhanced damages. Under Texas law, for example, “the intent to commit the tort” of trade secret

---

203. Other such cases include *Brightview Grp., LP v. Teeters*, No. SAG-19-2774, 2021 U.S. Dist. LEXIS 64487, \*69–70 (D. Md. Mar. 29, 2021) (where plaintiff sought recovery of attorneys’ fees under the Maryland UTSA and the DTSA, the court denied a defense motion for summary judgment; the court followed the Maryland standard that “willful and malicious” means “an act does for an improper motive and without legal justification’ and ‘to deliberately cause harm or injury’”) (citation omitted); *Ajaxo Inc. v. E\*Trade Group, Inc.*, 135 Cal. App. 4th 21, 45 (2005) (affirming finding of “willful and malicious misappropriation” where trial court instructed jury that “willful” means “a purpose or willingness to commit the at or engage in the conduct in question, and the conduct was not reasonable under the circumstances then present and was not undertaken in good faith,” and that “malice” means “conduct which is intended by the defendant to cause injury to the plaintiff or despicable conduct which is carried on by the defendant with a willful and conscious disregard for the rights of others when the defendant is aware [of] the probable consequences of its conduct and willfully and deliberately fails to avoid those consequences. Despicable conduct is conduct which is so vile and wretched that it would be looked down upon and despised by ordinary decent people.”).

204. See *Arnold’s Office Furniture, LLC v. Borden*, No. 5:20-cv-05470-JMG, 2022 U.S. Dist. LEXIS 150824, at \*4–7 (E.D. Pa. Aug. 23, 2022) (reciting standard and declining to award additional damages where defendant was motivated by greed but factors were not clearly met); *Proofpoint*, 2021 U.S. Dist. LEXIS 223024, at \*10–11 (same; there was no finding of actual loss and the jury’s unjust enrichment award was unclear).

205. *Huber*, 295 F. Supp. 3d at 493.

206. *Id.*

207. *Id.* at 494.

208. *Id.*

misappropriation “alone cannot justify an award of exemplary damages.”<sup>209</sup> Rather, the defendant’s conduct “must have been outrageous, malicious, or otherwise reprehensible.”<sup>210</sup> Thus, even a defendant’s act of concealing who was acquiring certain mineral leases in the course of misappropriation did not suffice for exemplary damages, because this was insufficient to show malice, and there was no evidence that the defendants caused the plaintiff “an injury independent of and qualitatively different than the misappropriation itself.”<sup>211</sup>

Similarly, in a 2020 District of Delaware case, a jury found willful and malicious misappropriation despite a fair amount of evidence showing that the defendant depended on the representations of a third party who brought the technology to the company. In *AgroFresh Inc. v. Essentiv LLC*, an individual who was well-known as an inventor in the relevant field offered technology to the defendant in an agreement where he made customary representations that he was the “sole owner” of the technology and had the right to disclose it.<sup>212</sup> The defendant sought assurances that the inventor could convey the technology “free and clear” of encumbrances.<sup>213</sup> At the same time, the defendant was aware that the inventor had previously worked with another company in the same field but did not make efforts to learn its intellectual property assignment terms. Perhaps most significantly, the defendant also concealed its relationship with the inventor.<sup>214</sup> Admitting these mixed facts, the court affirmed the jury’s verdict. However, it declined to award enhanced UTSA damages, because these facts did not show any effort to engage in continuing misconduct, as the defendant had changed course when it learned the facts.<sup>215</sup>

### C. SEPARATING EMPLOYEE MALICE FROM MANAGEMENT INTENT

There is a remarkable absence of analysis in the case law to distinguish the malicious intent of a corporate defendant from the intent of the wayward

---

209. *See Eagle Oil & Gas Co. v. Shale Expl., LLC*, 549 S.W.3d 256, 283 (Tex. Ct. App. 2018).

210. *See id.* (noting that exemplary damages are available only in the most exceptional instances).

211. The court applied a clear and convincing evidence standard in its finding. *See id.* at 285 (“[Defendant’s] intentional misappropriation of [plaintiff’s] trade secrets is not legally sufficient evidence of malice. If it were, exemplary damages would be recoverable as a matter of course in every misappropriation case, rather than the exceptional case involving egregious misconduct and injury.”; “Because the record lacks clear and convincing evidence of an intent on [defendant’s] part to inflict substantial injury, independent and qualitatively different than the compensable harms associated with misappropriation of [plaintiff’s] trade secrets, we hold that the evidence is legally insufficient to support the jury’s finding of malice.”).

212. *AgroFresh*, 2020 U.S. Dist. LEXIS 222898, at \*23–24.

213. *See id.*

214. *See id.* at \*25.

215. *See id.* at \*72–83.

employee who engaged in misappropriation. Where malice (however defined) must be shown, the differences in a corporate defendant's intent and the intent of an employee may be significant. As in our discussion of vicarious liability, this difference would be apparent in cases where a new hire downloads files from the prior employer and the new employer is unaware of that conduct. It would be difficult to attribute malice to the new employer where it is difficult to attribute vicarious liability in the first place.

But even in a case where vicarious liability for employee conduct is tenable, imposing exemplary damages for malicious intent is distinct from liability for ordinary remedies. It requires a judgment that the employer-defendant itself harbored an enhanced level of wrongful intent. Thus, courts should distinguish uncoordinated or ad-hoc behavior by employees from top-down directives from company management in assessing these questions. As with paying closer attention to questions of vicarious liability, these distinctions may reduce the exaggerated damages claims that so often plague trade secret lawsuits.

In some instances, courts applying caution might still separate corporate defendants which provide some degree of training or policies to employees on trade secret issues from employee-defendants who ignore such guidance. There is a material difference between a company defendant that trains employees not to use potential trade secrets from former employers and an employee-defendant who chooses to violate such training through ad-hoc decisions. There are caveats. The majority of companies likely do not provide such training, and the mere absence of training should not be construed as evidence in favor of a finding of malice, especially without empirical metrics comparing training at similarly-situated companies.<sup>216</sup> Moreover, the size and maturity of a business (or the department or division at issue) will surely play into the analysis, as less mature companies are even less likely to provide such training or policies. And many of those who do provide training on information-handling may focus more on protecting the company's own information than the information of others. All that said, the intentionality of an employee who violates express training is not the same as the intentionality of the company which provides such training, to whatever degree.

---

216. I have been unable to find statistics on companies providing trade secret training. In this author's experience, a sizable majority of small and mid-sized technology companies do not. Large company training tends to focus on protection of the company's own information and not practical instruction to avoid trade secret problems with other employers. For these reasons, it would not be wise for courts to assess "willful and malicious misappropriation" based on the presence or absence of such training, in a corporate environment where such training is not customary. The question is rather the need to separate the intentionality of companies that opt to provide such training from employee-defendants who violate it.

With the rise in trade secret litigation in recent years, at least some companies provide workforce training sessions on how to avoid trade secret risks. This author has given many such training sessions over the past two decades, often spurred by letters sent by former employers to newly-hired company employees; though few companies seem to have such training or policies in place. And in 2021, as part of its ongoing series of commentaries on trade secret law, the Sedona Conference promulgated guidelines on such training.<sup>217</sup> Those guidelines recommend training new hires, noting that employees “need to understand that they have an obligation to protect the third party’s trade secret information from misappropriation.”<sup>218</sup> They explain that “training on preventing use of former-employer information when an employee is wondering whether he or she is able to use an item of information can include practical guidance on searching the public domain,” as well as telling others “that they might be inappropriately sharing information that might appear to be the trade secrets of others.”<sup>219</sup>

To be sure, a startup or mid-sized company rarely would have the administrative staff or the resources for employee training, especially on a relatively esoteric issue like trade secret risk. Different departments or divisions within a company might treat the issue differently, based on their sophistication and history. Using such training to assess whether a company’s level of intent differs from that of a wayward employee who behaved with malice might thus differ on a sliding scale based on the size and longevity of the company, and its maturity in the circumstances. But even with such variability, it is somewhat surprising that the case law on exemplary damages has not inquired into the distinction between corporate intent and the actions of wayward employee-defendants who disobey training and instructions. In such cases, can a corporate defendant who had provided any degree of policies or training be found to have engaged in “willful and malicious misappropriation,” no matter how egregious the behavior of a lower-level employee-defendant who the direct target of the accusations is?

In such cases, courts should make a principled distinction between the willfulness and malice of one, but not the other. By the same token, if a company were to implement a workforce IP training program, and if it were later sued for trade secret misappropriation for the acts of a non-executive

---

217. See The Sedona Conference, *Commentary on Protecting Trade Secrets Throughout the Employment Life Cycle*, 23 SEDONA CONF. J. 807 (2022), <https://thesedonaconference.org/node/10020>. I provided comments on an early draft but was not otherwise involved in this publication.

218. See *id.* at 872–73.

219. See *id.* at 874.

level employee, the company might use the program as evidence in support of an argument against exemplary damages, making a distinction between itself and a wayward employee-defendant who, for example, maliciously downloaded information from his or her prior employer and used it at the new job.

## VI. CONCLUSION

Trade secret law puts more emphasis on questions of the defendant's intent than other areas of intellectual property law. This Article offers three normative proposals to illuminate the importance of intentionality in the context of secondary liability.

First, courts should rescue the "accident or mistake" safe harbor in the trade secret statutes from inattention and use it when one defendant buys or licenses information from a third party in an ordinary commercial transaction that turns out to contain another's trade secret, and innocently uses the information. Second, courts should pay more attention to exceptions to vicarious liability, especially when a former employer sues a rival based on a departing employee's download of files before leaving the plaintiff's employ. Third, when assessing questions of enhanced damages for willful and malicious misappropriation, courts should pay more attention to the distinction between the intent of a company-defendant and the actions of a wayward employee.

