THE JOHN MARSHALL
REVIEW OF INTELLECTUAL PROPERTY LAW

THE UNCERTAIN PROTECTION OF "DERIVATIVE" TRADE SECRETS

BENJAMIN J. BRADFORD AND REMI JAFFRÉ

ABSTRACT

This article discusses when a trade secret misappropriation claim can be premised on the acquisition, disclosure, or use of a product or method derived from a trade secret, rather than the acquisition, disclosure, or use of a trade secret itself. Although this question is likely to take on increasing importance as digital products that were made through the use of trade secrets and that can easily be copied become a larger part of everyday life, courts have rarely focused on it and have not come to any consensus. In this article, we survey the existing, inconsistent case law and analyze it in light of the applicable statutory text and relevant public policy considerations. The article provides some conclusions and takeaways for practitioners.

Cite as Benjamin J. Bradford and Remi Jaffré, *The Uncertain Protection of "Derivative" Trade Secrets*, 18 J. MARSHALL REV. INTELL. PROP. L. 241 (2019).

THE UNCERTAIN PROTECTION OF "DERIVATIVE" TRADE SECRETS

BENJAMIN J. BRADFORD AND REMI JAFFRÉ

THE UNCERTAIN PROTECTION OF "DERIVATIVE" TRADE SECRETS

BENJAMIN J. BRADFORD AND REMI JAFFRÉ*

I. INTRODUCTION

The purpose of the Uniform Law Commission's Uniform Trade Secrets Act ("UTSA"), which has been almost universally adopted throughout the United States, was to promote the development of a nationally uniform body of trade secrets law. One question, however, is not squarely addressed by the UTSA's text, and the case law remains mired in uncertainty: under what circumstances can a trade secrets claim be premised on the acquisition, disclosure, or use of a product or method derived from a trade secret, rather than the acquisition, disclosure, or use of the trade secret, itself. This article refers to such claims as "derivative trade secrets claims," and to products or methods derived from trade secrets as "derivatives."

These claims have conceptual analogs in other areas of intellectual property law. One of the exclusive rights granted to the owner of a copyright, for example, is the right "to prepare derivative works based upon the copyrighted work."[1] The separate copyright in a derivative work "extends only to the material contributed by the author of such work, as distinguished from the preexisting material employed in the work, and does not imply any exclusive right in the preexisting material."[2] Thus, absent contractual provisions to the contrary, the copyright owner of the underlying work has the ability to control the use and distribution of the derivative work, by virtue of his ownership of the preexisting material incorporated into the derivative work. No such statutory right exists for trade secrets.

Patent law provides some recognition to "derivative" claims, although not on a statutory basis as in copyright law. To infringe a patent, the defendant need not possess or understand the patented invention: it is sufficient that the defendant "put[s] the invention into service, *i.e.*, control[s] the system as a whole and obtain[s] benefit from it."[3] In some situations, this means that one can commit patent infringement by using an unpatented product, if that product derives from a process or product that is itself patented. For example, the Federal Circuit has held that a farmer who planted a seed containing the plaintiff's patented gene sequence had "used" the patent, reasoning that "[t]he gene itself is being used in the planting."[4] But in the patent context this principle is not limitless. One court, for example, dismissed a direct infringement claim against film studios that contracted with a third party to provide motion capture services using the plaintiff's patented

* Benjamin Bradford earned his J.D. from the University of Chicago Law School. He is a litigation partner at Jenner & Block concentrating on intellectual property/technology litigation with a focus on computer and internet technologies. Remi Jaffré earned his J.D. from New York University School of Law. He is a litigator in Jenner & Block's Content, Media, and Entertainment Practice Group.

[1] 17 U.S.C. § 106(2) (2016).

[2] 17 U.S.C. § 103(b) (2016).

[3] Centillion Data Sys., LLC v. Qwest Comm'ns Int'l, Inc., 631 F.3d 1279, 1284 (Fed. Cir. 2011).

[4] Monsanto Co. v. David, 516 F.3d 1009, 1014 (Fed. Cir. 2008).

technology, holding that the studios had not “used” the technology by incorporating its output into their films.[5]

However, even where the standard for patent “use” quoted above is not met, the patent laws render liable a person who imports or sells in the United States products made outside the United States that use a patented process, even if the person never used the process (directly or indirectly).[6] This exception reflects the reality that, due to the territorial limitations of American patent law, the owner of a patented technology has no means to prevent or discourage its unauthorized use abroad other than to control the distribution in the United States of products derived from that technology.

A derivative trade secret can arise in many circumstances. Perhaps most straightforwardly, a derivative trade secret can be a good—a soft drink, for example—produced using a trade secret formula, but not actually containing the underlying trade secret itself (*e.g.*, the secret formula). Another example of a derivative trade secret is software that is produced using a data model, where the data model is the original trade secret. In this example, software for use in a self-driving car could be based upon trade secret data about the car’s breaking speed, ability to handle curves on wet roads, and so on. Or, algorithmic stock trading software might be built in view of a proprietary market model. As a final example, a derivative trade secret may consume the original trade secret where, for example, a chemical compound is manufactured using a substance, such as a catalyst, that is a trade secret.

The ability to control the use or distribution of derivatives is particularly important in the trade secrets context. Absent such protection, the value of the trade secret could be usurped without any recourse for the trade secret owner. For example, someone could abscond with the secret formula for Coca-Cola to a jurisdiction without sufficient trade secret protection and start producing a Coca-Cola knock-off for importation into the United States. In such a situation, if the knock-off manufacturer took sufficient precautions to avoid being subject to U.S. jurisdiction (*e.g.*, only selling to foreign distributors) Coca-Cola would not have recourse against the knock-off manufacturer. And, absent derivative trade secret protection, Coca-Cola also may not have recourse against the importers of the knock-off product, who had no access and did not use the original trade secret – the secret formula.

As of now, however, there is no judicial consensus on whether derivative trade secret claims are cognizable. Very few cases have clearly focused on this issue or tried to develop a conceptual framework for addressing it. Instead, courts faced with derivative claims tend to be guided by the policy considerations applicable to the facts of the particular case before them. This case-by-case approach has created an inconsistent body of law from which it is difficult to discern the general viability of derivative claims.

This article begins by analyzing the relevant definitional provisions of the UTSA, which now govern trade secrets claims throughout most of the country, as well as the Restatement (Third) of Unfair Competition, which is widely relied on by courts as an interpretive guide. It then discusses in more detail the policy

[5] Rearden LLC v. Walt Disney Co., 293 F. Supp. 3d 963, 973–74 (N.D. Cal. 2018).

[6] 35 U.S.C. § 271(g) (2016).

considerations relevant to the recognition of derivative trade secret claims, before moving to a survey of the existing case law. The article concludes with a summary of potential takeaways from the case law.

II. Statutory Analysis

Our analysis begins with the applicable statutory text. As of this writing, 47 states and the District of Columbia have enacted a version of the UTSA.[7] Accordingly, misappropriation of trade secrets are typically governed by the UTSA's definition of "misappropriation." The federal Defend Trade Secrets Act ("DTSA") also uses the UTSA's definition of "misappropriation."[8] The UTSA provides:

> "Misappropriation" means:
> (i) 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
> (ii) disclosure or use of a trade secret of another without express or implied consent by a person who
> (A) used improper means to acquire knowledge of a trade secret; or
> (B) at the time of disclosure or use, knew or had reason to know that his 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

[7] Ala. Code §§ 8-27-1 to -6 (2017); Alaska Stat. §§ 45.50.910–.945 (2017); Ariz. Rev. Stat. Ann. §§ 44-401 to -407 (2017); Ark. Code Ann. §§ 4-75-601 to -607 (2017); Cal. Civ. Code §§ 3426–3426.10 (2017); Colo. Rev. Stat. §§ 7-74-101 to -110 (2017); Conn. Gen. Stat. §§ 35-50 to -58 (2017); Del. Code Ann. Tit. 6, §§ 2001–09 (2017); D.C. Code Ann. §§ 36-401 to -410 (2017); Fla. Stat. Ann. §§ 688.001–.009 (2017); Ga. Code Ann. §§ 10-1-760 to -767 (2017); Haw. Rev. Stat. §§ 482B-1 to -9 (2017); Idaho Code §§ 48-801 to -807 (2017); 765 Ill. Comp. Stat. 1065/1 to 1065/9 (2017); Ind. Code §§ 24-2-3-1 to -2-3-8 (2017); Iowa Code §§ 550.1–.8 (2017); Kan. Stat. Ann. §§ 60-3320 to -3330 (2017); Ky. Rev. Stat. Ann. §§ 365.880–.900 (2017); La. Stat. Ann. §§ 51:1431–:1439 (2017); Me. Rev. Stat. Ann. tit. 10, §§ 1541–48 (2017); Md. Code Ann., Com. Law §§ 11-1201 to -1209 (2017); Mich. Comp. Laws Ann. §§ 445.1901–.1910 (2017); Minn. Stat. Ann. §§ 325C.01–.08 (2017); Miss. Code Ann. §§ 75-26-1 to -19 (2017); Mo. Rev. Stat. §§ 417.450–.467 (2017); Mont. Code Ann. §§ 30-14-401 to -409 (2017); Neb. Rev. Stat. Ann. §§ 87-501 to -507 (2017); Nev. Rev. Stat. Ann. §§ 600A.010–.100 (2016); N.H. Rev. Stat. Ann. §§ 350-B:1 to :9 (2017); N.M. Stat. Ann. §§ 57-3A-1 to -7 (2017); N.C. Gen. Stat. Ann. §§ 66-152 to -157 (2017); N.D. Cent. Code Ann. §§ 47-25.1-01 to -08 (2017); Ohio Rev. Code Ann. §§ 1333.61–.69 (2017); Okla. Stat. tit. 78, §§ 85–94 (2017); Or. Rev. Stat. Ann. §§ 646.461–.475 (2016); 12 Pa. Cons. Stat. Ann. §§ 5301–08 (2017); R.I. Gen. Laws Ann. §§ 6-41-1 to -11 (2017); S.C. Code Ann. §§ 39-8-10 to -130 (2017); S.D. Codified Laws §§ 37-29-1 to -11 (2017); Tenn. Code Ann. §§ 47-25-1701 to -1709 (2017); Tex. Civ. Prac. & Rem. Code Ann. §§ 134A.001–.008 (2017); Utah Code Ann. §§ 13-24-1 to -9 (2017); Vt. Stat. Ann. tit. 9, §§ 4601–09 (2017); Va. Code Ann. §§ 59.1-336 to -343 (2017); Wash. Rev. Code Ann. §§ 19.108.010–.930 (2017); W.V. Code Ann. §§ 47-22-1 to -10 (2017); Wis. Stat. Ann. § 134.90 (2017); Wyo. Stat. Ann. §§ 40-24-101 to -110 (2017).

[8] 18 U.S.C. § 1839(5) (2016).

> (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.[9]

The UTSA definition thus encompasses two types of misappropriation—by "acquisition" or by "disclosure or use"—which courts analyze separately. While the statute sets out in detail the *mens rea* and other requirements for each type of misappropriation, it does not define the central terms "acquisition" or "use."

Another notable aspect of the UTSA definition is that it appears to require that a misappropriator must have *knowledge* of the trade secrets at issue. This is especially true for misappropriation by "disclosure or use." Clauses (A), (B), and (C) under "disclosure or use" all refer to the defendant's acquisition or derivation of "knowledge" of the trade secret. The definition of misappropriation by "acquisition" does not refer to "knowledge" of the trade secret, but at least one court has questioned whether it is possible to "acquire" a trade secret without acquiring knowledge of it.[10] As explained below, some courts have ignored the apparent knowledge requirement in the UTSA's "disclosure or use" definition entirely, while those that have addressed it have disagreed on its meaning.

In addition to this statutory language, courts have also looked to the Restatement (Third) of Unfair Competition ("Restatement"), which contains several sections on trade secrets law.[11] The Restatement's definition of actionable "appropriation" also includes an "acquisition" prong and a "disclosure or use" prong, and mirrors the UTSA's definition in most other respects.[12] The Restatement's discussion of acquisition is not noteworthy for purposes of this article, but on the issue of use, the Restatement says the following:

> There are no technical limitations on the nature of the conduct that constitutes "use" of a trade secret . . . . As a general matter, *any exploitation of the trade secret* that is likely to result in injury to the trade secret owner or enrichment to the defendant is a "use" under this Section. Thus, *marketing goods that embody the trade secret*, employing the trade secret in manufacturing or production, relying on the trade secret to assist or accelerate research or development, or soliciting customers through the use of information that is a trade secret . . . all constitute "use."[13]

The Restatement thus intends that "use" should be interpreted broadly, and specifically states that "marketing goods that embody the trade secret" should constitute actionable use. Indeed, several cases have relied on the Restatement for

[9] UNIF. TRADE SECRETS ACT § 1(2) (1985).

[10] *See infra* notes 64–65 and accompanying text.

[11] RESTATEMENT (THIRD) OF UNFAIR COMPEITITION, ch. 4, Topic 2 (1995).

[12] *Id.* § 40. The Restatement further notes that the definition is "intended to be consistent with and applicable to actions under the Uniform Trade Secrets Act;" *Id.* § 40 cmt. a.

[13] *Id.* § 40 cmt. c (emphasis added).

precisely that proposition.[14] Arguably, this language supports the view that "derivative" trade secrets claims are actionable when they are based on the defendant's marketing and sale of goods that "embody" the underlying trade secrets (a term the Restatement does not define or elaborate on), even if the defendant has not had direct access to the trade secrets themselves.

Courts thus have little statutory or other authoritative guidance to help them determine whether to recognize "derivative" claims. Further, what little guidance there is in the text of the UTSA and the Restatement arguably sends contradictory signals on this particular question.

III. Case Law on Derivative Trade Secret Claims

As noted above, courts have reached very different conclusions about the propriety of derivative trade secret claims, while usually failing to recognize the nature of the issue confronting them. As the cases bear out, the public policy implications of derivative trade secret claims tend to influence court decisions. Accordingly, below, this section begins by investigating the policy considerations that likely form the implicit background of these courts' decisions. We then survey cases in which courts have implicitly recognized a derivative claim and cases where courts have declined to recognize them, bringing to light the focus of these courts' reasoning.

A. Public Policy Considerations

A principal reason for recognizing derivative trade secret claims is simply that they further one of the central goals of trade secret law: "the maintenance of standards of commercial ethics."[15] As one treatise puts it, "[t]he legal protection of trade secrets stabilizes the relationship of people in commercial transactions by providing rules of fair play which govern even in the absence of an express contract."[16]

Suppose, for example, that the company DataCo develops a proprietary data model and contracts with software developer SoftCo (perhaps overseas) to use the trade secret data model to develop a piece of software, NewSoft. DataCo and SoftCo enter into an agreement with ironclad protections for DataCo's trade secret model, but as can happen, a third-party BadApple somehow obtains a copy of NewSoft—either by using wrongful means itself, or simply by chance (*e.g.*, because a copy falls off the back of a truck) but under circumstances making it clear that NewSoft is derived from DataCo's proprietary model.[17] In either situation, if BadApple makes copies of NewSoft and starts distributing them, it does so in full awareness that it is

[14] *See, e.g.*, Penalty Kick Mgmt. Ltd. v. Coca Cola Co., 318 F.3d 1284, 1292 (11th Cir. 2003) (applying Georgia law); Cognis Corp. v. ChemCentral Corp., 430 F. Supp. 2d 806, 812 (N.D. Ill. 2006); PMC, Inc. v. Kadisha, 93 Cal. Rptr. 2d 663, 673 (Cal. Ct. App. 2000).

[15] UNIF. TRADE SECRETS ACT § 1 (1985) (quoting Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470 (1974)).

[16] MELVIN F. JAGER, TRADE SECRETS LAW § 1.3 (1st ed. 1991).

[17] *See* UNIF. TRADE SECRETS ACT § 1(2)(i), (ii). As noted above, the UTSA definition of "misappropriation" requires some wrongful conduct or a *mens rea* on the defendant's part.

usurping the fruits of DataCo's investment in developing its trade secret model. It is no less guilty of breaching commercial ethics than if it had somehow acquired the trade secret process, rather than its resulting product.

But absent a derivative trade secret claim, the trade secret holder, DataCo, may not succeed in a claim against the misappropriator, BadApple, either for breach of contract (because they are not in privity) or for trade secret misappropriation because BadApple, in theory, does not possess DataCo's actual trade secret. If SoftCo had somehow given substantial assistance to BadApple, DataCo might theoretically have a claim against SoftCo for aiding and abetting BadApple's misappropriation, but courts have, by and large, been skeptical that a claim for aiding and abetting trade secret misappropriation exists.[18]

A second reason for derivative trade secret recognition is that derivative trade secret claims may, in some circumstances, be the only way to adequately protect a trade secret itself. In the hypothetical above, DataCo's contract with SoftCo contains protections for DataCo's trade secret model, which would presumably extend to SoftCo's customers. BadApple's customers, however, are not bound by those protections when they buy NewSoft from BadApple, and are thus under no obligation to refrain from reverse engineering the trade secret model—to the extent that would be feasible—which would destroy the value of the trade secret itself.

Such a scenario may seem far-fetched, but it is not as unlikely as it seems. The cases in the next two sections describe similar scenarios. These types of scenarios are, in fact, more likely in today's computer age because digital products like software that was manufactured with using a trade secret can easily be copied without authorization. Thus, for both reasons, there are public policy reasons counseling in favor of recognizing a derivative trade secret claim.

The reasons against recognizing derivative trade secrets claims mirror policy reasons for restricting the scope of intellectual property rights in general, namely that such claims could be exploited to create an unwarranted monopoly or could subject an innocent party to liability that is deemed unjust. Consistent with those policy reasons, the argument can be made that the owner of a trade secret should lose his or her ownership rights after a sufficient distance has been reached along the supply chain from the trade secret itself. Granting trade secret owners the rights to control the use and distribution of all goods derived from those secrets, no matter how remote, potentially extends the specter of liability to millions of buyers of those goods. While, as explained above, actionable misappropriation under the UTSA cannot occur without wrongful conduct or some degree of *mens rea*, the risk of embroiling millions of innocent end-users of goods in trade secrets litigation counsels against excessive broadening of a trade secret owner's rights. As one court has remarked, potentially exposing innocent end-users to the costs of litigation would depress consumer demand in certain markets, hindering the development of those markets and discouraging innovation.[19]

[18] *See, e.g.*, Legacy Separators LLC v. Halliburton Energy Servs. Inc., No. 4:14-CV-2081, 2016 WL 4386130, at *3 (S.D. Tex. Aug. 16, 2016); *But cf.* Stoneeagle Servs., Inc. v. Davis, 2013 WL 12143946, at *9 (N.D. Tex. Aug. 14, 2013) (declining to dismiss secondary liability claims based on the defendants' aiding and abetting the misappropriation of a trade secret).

[19] Silvaco Data Sys. v. Intel Corp., 109 Cal. Rptr. 3d 27, 41 (Ct. App. 2010).

This dichotomy between bad actors who knowingly exploit a product derived from a trade secret and innocent actors who unknowingly obtain an unauthorized derivative is also reflected in the cases that address derivative trade secret claims, as discussed in the next two sections. Courts tend to want to hold the bad actors liable, while not punishing the innocent actors.

B. Cases Recognizing Derivative Trade Secrets Claims

1. Misappropriation by Acquisition

We have identified only two cases arguably involving derivative trade secrets claims for misappropriation by acquisition. Those cases provide some support for the view that such claims can exist if the trade secret at issue is susceptible to reverse engineering from the derivative. In *ATS Products, Inc. v. Champion Fiberglass, Inc.*,[20] the plaintiff, ATS, alleged that it owned "trade secrets relating to: (1) formulas for making fire-safe plastics by combining phenol-resorcinol resins with catalysts and/or fillers, and (2) information regarding the best methods and practices for using resins, hardeners and fillers to manufacture plastic products."[21] ATS's predecessor worked with the defendant, Champion, to develop products using ATS's resins. One of Champion's employees then formed his own company, Thermalguard, and began building resins using ATS's trade secrets without authorization. ATS prevailed in a separate lawsuit against Thermalguard and the former employee.[22]

In this subsequent lawsuit against Champion, ATS alleged that Champion had bought misappropriated resins from Thermalguard, and used them to produce the "Flame Shield" product that Champion then sold to the Bay Area Rapid Transit.[23] Although it was not alleged that Champion ever possessed the trade secrets themselves, the court held that the complaint stated a claim against Champion for misappropriation by acquisition, relying on the allegation that "the resins are susceptible to reverse engineering which would, in turn, yield the trade secrets to anyone who possessed the resins."[24] The rule suggested by *ATS Products* is that one "acquires" a trade secret when one acquires a product from which the trade secret can be reverse engineered or otherwise learned.

However, an earlier case suggests that no actionable "acquisition" takes place until the defendant has *actually* reverse engineered the trade secret. In *Minnesota Mining & Manufacturing Co. v. Johnson & Johnson Orthopaedics, Inc.*,[25] the defendant, JJO, received samples of a new slippery resin under development by the plaintiff, 3M, under circumstances that JJO's president concluded were suspicious,

[20] ATS Prod., Inc. v. Champion Fiberglass, Inc., No. C 13-02403 SI, 2013 WL 6086924 (N.D. Cal. Nov. 19, 2013).

[21] *Id.* at *1 (internal quotation marks omitted).

[22] *Id.*

[23] *Id.*

[24] *Id.* at *3.

[25] Minnesota Mining & Mfg. Co. v. Johnson & Johson Orthopaedics, Inc., Civ. No. 4-86-359, 1991 WL 441901 (D. Minn. Apr. 30, 1991).

according to his own testimony.[26] The court found that JJO nevertheless chemically analyzed the samples to determine the key novel ingredient, and that [b]y reason of its receipt and use of the…samples, JJO was able to bring its [own] product to market three months earlier than it otherwise would have.[27] The court held that JJO had misappropriated 3M's trade secret stating: "JJO acquired 3M's trade secret as a result of its chemical analysis of the [resin] samples, identifying the slip agents. JJO then used this trade secret to make its own slippery resin product."[28] However, addressing a statute of limitations argument, the court further stated:

> Actionable acquisition of 3M's trade secret did not occur until JJO analyzed the samples and successfully discovered the slippery resin formula. Had JJO merely locked the samples in a cabinet, or analyzed them and failed to discover the formula, 3M would have been hard pressed to sue for misappropriation. The statute defines "trade secret" as "information." Mere possession of the rolls did not allow JJO to acquire the "information" about the roll's slippery resin. Only the analysis allowed that acquisition.[29]

Arguably, then, the claim recognized by the *Minnesota Mining* case was not a derivative claim at all, because it required the defendant to come into direct contact with the trade secrets themselves. But *Minnesota Mining* can also be read to support the existence of derivative claims if it is interpreted as holding that a derivative claim for misappropriation by acquisition requires only that the defendant *exploit* the trade secret derivative in some manner—in this case, by using it to reverse engineer the trade secret. This reading of *Minnesota Mining* makes it consistent with *ATS Products*, in which Champion exploited the derivative resin by making and selling its "Flame Shield" product.

2. Misappropriation by Use

The case law on derivative claims for misappropriation by use is more developed, and the weight of authority generally recognizes such claims. Several cases have held that a defendant can be liable for selling goods that were made by using a trade secret, even if the goods were made by a third party and the defendant never possessed the trade secrets themselves.

In *ClearOne Communications, Inc. v. Chiang*,[30] the plaintiff, ClearOne, alleged that a former employee breached a non-disclosure agreement by providing ClearOne's "Honeybee Code"—a computer source code and object code used to improve the quality of a speakerphone produced by ClearOne—to the third-party, WideBand.[31] WideBand used the Honeybee Code to derive its own "WideBand Code,"

[26] *Id.* at *46.

[27] *Id.* at *48.

[28] *Id.* at *77.

[29] *Id.* at *78 (citation omitted).

[30] ClearOne Comm'ns, Inc. v. Chiang, No. 2:07-cv-37 TC, 2007 WL 4376125 (D. Utah Dec. 13, 2007)

[31] *See id.* at *2–3.

which it then licensed to defendant Biamp. More importantly, WideBand licensed the WideBand Code in "object code" form—i.e., in the form of zeros and ones legible only by computers and not by humans. Biamp, in turn, incorporated the code into an "echo acoustic cancellation sound card," which was widely distributed.[32] Biamp argued that it "never had knowledge of the allegedly misappropriated trade secret because it could not read the object code."[33] The court denied Biamp's motion to dismiss, holding that "[t]here is no requirement of comprehension of the trade secret to state a claim for misappropriation under the Utah [UTSA]."[34] It also emphasized allegations that Biamp knew that WideBand had derived the WideBand code through improper means.[35] The claim in *ClearOne* can be thought of as a derivative claim, because Biamp never had direct access to the human-legible source code constituting the trade secret, and only had access to the object code derived from it.

Similarly, in *Cognis Corp. v. ChemCentral Corp.*,[36] the plaintiff, Cognis, developed a formula and production method for CAPCURE, "a distinctive curing agent for epoxy resin adhesive."[37] Non-party GabePro, a former manufacturer of CAPCURE for Cognis, began to produce a CAPCURE equivalent using Cognis's technology, and sued Cognis in state court seeking a declaration that this did not violate Cognis's rights. Cognis counterclaimed in the state-court action, for misappropriation of trade secrets. In a separate federal lawsuit, filed a year and a half later, Cognis sued GabePro's distributor ChemCentral, which allegedly continued to solicit customers for and sell GabePro's CAPCURE equivalent despite knowing about the state-court lawsuit.[38]

The court in the federal lawsuit recognized that Cognis never alleged "that [ChemCentral] ever knew the formula or manufacturing process for CAPCURE or [the equivalent]," and that its theory was "that distribution of a product manufactured by another's use of a trade secret constitutes use of that trade secret."[39] The court nevertheless denied ChemCentral's motion to dismiss, holding that "Cognis's allegations show that it is possible, under a broad reading of the word 'use,' that it may be able to show that [ChemCentral] misappropriated its trade secrets" by marketing the CAPCURE equivalent with knowledge of the state-court lawsuit between Cognis and GabePro.[40] In so concluding, the court relied on Illinois precedent and on the Restatement provision quoted above, which the court interpreted as endorsing a "very broad" understanding of "use."[41] The court also highlighted allegations that ChemCentral was aware that Cognis protected its technology and of the lawsuit against GabePro in concluding that ChemCentral satisfied the UTSA's mens rea requirement.[42]

[32] *Id.* at *1.

[33] *Id.* at *2.

[34] *Id.*

[35] *Id.* at *2–3.

[36] Cognis Corp. v. ChemCentral Corp., 430 F. Supp. 2d 806 (N.D. Ill. 2006).

[37] *Id.* at 808.

[38] Complaint at 6, Cognis Corp. v. ChemCentral Corp., 430 F. Supp. 2d 806 (N.D. Ill. 2006) (No. 05-cv-6344), ECF No. 1.

[39] *Cognis*, 430 F. Supp. 2d at 811–12.

[40] *Id.* at 813.

[41] *Id.* at 812.

[42] *Id.* at 812–13.

In a third case, *VIA Technologies, Inc. v. ASUS Computer International*,[43] the plaintiff, VIA, alleged that two Taiwanese corporations acquired its controller chip technology by conducting a "mass raiding" of VIA employees, who breached severance agreements with VIA by providing the technology to the Taiwanese corporations.[44] The Taiwanese corporations then allegedly manufactured chips incorporating VIA's technology. VIA brought suit in California against ACI, an American affiliate of the Taiwanese corporations. Because VIA sought relief only for actions that took place in the United States, its claim against ACI was based only on ACI's marketing and sale of the infringing chips.[45] The complaint did not allege that ACI itself had been directly involved in the use of VIA's trade secrets to manufacture the chips at issue.[46] The court nevertheless held that VIA had sufficiently alleged misappropriation against ACI.[47] In so holding, it relied on the statement that "marketing goods that embody the trade secret constitutes use of the trade secret," and also cited the *Cognis* case.[48] The court also noted the complaint's allegation that ACI sold the chips "with the knowledge that those products were made using the trade secrets."[49]

Finally, in *X6D, Ltd. v. Li-Tek Corps. Co.*,[50] the plaintiffs alleged that they provided proprietary manufacturing and design information for 3D glasses to one of the defendants, Li-Tek, under a manufacturing outsourcing agreement. Li-Tek allegedly retained this information and manufactured its own unauthorized 3D glasses, and another group of defendants allegedly served as the distributors for the unauthorized glasses under the trade name Etoniq.[51] The Etoniq defendants moved to dismiss, arguing that they did not *use* the trade secret information because the glasses were manufactured by Li-Tek, which did not move to dismiss. The court disagreed, holding that the moving defendants' sale of the glasses was a sufficient allegation of use of trade secrets.[52] Once again, the court relied on the Restatement and singled out the Restatement's assertion that "marketing goods that embody the trade secret" constitutes use.[53] The court also held that the complaint sufficiently alleged that the Etoniq defendants had knowledge that the glasses were manufactured using the plaintiffs' trade secrets.[54]

It is notable that in all four of these cases, the defendant was a commercial distributor of the derivative, not merely an end-user. As a comparison with the cases discussed in the next section shows, courts are more inclined to find derivative trade secrets liability where the defendant engaged in the distribution of the derivative goods for profit than where the defendant is a mere end-user of the product. The "maintenance of standards of commercial ethics" quite logically supports liability for

[43] VIA Tech., Inc. v. ASUS Comput. Int'l, No. 14-cv-03586-BLF, 2015 WL 3809382 (N.D. Cal. June 18, 2015).

[44] *Id.* at *1.

[45] *Id.* at *5.

[46] *See id.* at *1–2.

[47] *Id.* at *4.

[48] *Id.*

[49] *Id.*

[50] X6D, Lyd. v. Li-Tek Corps. Co., No. CV 10-2327-GHK (PJWx), 2010 WL 11512197 (C.D. Cal. Oct. 26, 2010).

[51] *Id.* at *1.

[52] *Id.* at *3.

[53] *Id.* (quoting RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 cmt. C (1995)).

[54] *Id.*

a defendant who profits from the distribution of a product knowing that the product was created using another's trade secrets without authorization, as was alleged to be the case in all four cases discussed in this section.

While these cases are consistent with general public policy principles, they may not satisfy the statutory requirement that the misappropriator have "knowledge" of the relevant trade secret, as discussed above. *Cognis*, *VIA Technologies*, and *X6D* do not even mention this issue. The *ClearOne* court addresses this issue briefly in a footnote, but its analysis on this point is not persuasive. In considering Biamp's argument that it could not be liable for misappropriation because it did not understand the indecipherable object code that had been licensed to it, the court held that "[t]here is no requirement of comprehension of the trade secret to state a claim" under the UTSA.[55] Then, in a footnote, the court recognized that the UTSA "uses the phrase 'knowledge of the trade secret,'" but held that "this phrase is generally understood to reflect knowledge that the trade secret was derived through improper means."[56]

Although this reading is consistent with the outcomes in *Cognis*, *VIA Technologies*, and *X6D*, it arguably creates some tension with regard to the text of the UTSA. For example, clause (A) of the definition of misappropriation by disclosure or use covers a person who "used improper means to acquire knowledge of a trade secret."[57] Under the *ClearOne* court's interpretation, the definition would cover a person who used improper means to acquire knowledge that the trade secret at issue was derived through improper means, which makes little sense. The argument could be made, however, that the words "knowledge of a trade secret" in the UTSA are more plausibly read to require that the defendant have knowledge of the trade secret itself, and that the defendant's knowledge of the circumstances under which the trade secret was acquired or derived is addressed in the rest of the definition of "misappropriation."

But the *ClearOne* opinion does suggest one way of reconciling derivative claims with the "knowledge of the trade secret" requirement. Other courts have agreed with *ClearOne*'s observation that "knowledge" does not mean "comprehension,"[58] and one court, although taking a dim view of derivative claims generally, has stated that, "at least in some circumstances," the UTSA requirement might be satisfied by "*constructive* knowledge of the secret."[59] The same court further explained: "one who knowingly possesses information constituting a trade secret cannot escape liability merely because he lacks the technical expertise to understand it, or does not speak the language in which it was written."[60] One who possesses a product from which a trade secret can be reverse engineered is arguably in the same position, with reverse engineering taking the place of translation in the court's hypothetical. If so,

[55] *ClearOne*, 2007 WL 4376125, at *2.

[56] *Id.* at *2 n.3.

[57] UNIF. TRADE SECRETS ACT § 1(2)(ii)(A) (1985).

[58] *See* Advanced Recovery Sys., LLC v. Am. Agencies, LLC, No. 2:13CV283DAK, 2017 WL 3912984, at *6 (D. Utah Sept. 6, 2017); *Silvaco*, 109 Cal. Rptr. 3d at 42 ("A requirement of 'knowledge of the trade secret' simply is not a requirement that the defendant 'comprehend' the secret or learn its 'details.'").

[59] *Silvaco*, 109 Cal. Rptr. 3d at 42 n.7. This case is discussed in more detail at pages 19–21.

[60] *Id.*

derivative claims can satisfy the UTSA's "knowledge of the trade secret" requirement through the defendant's constructive knowledge.

That principle may have been at work in *Advanced Recovery Systems, LLC v. American Agencies, LLC*,[61] in which the plaintiff, AA, brought a misappropriation claim against several companies and individual defendants. AA input its trade secrets—customer lists, debt information and collection efforts, data about business transactions, and the like—into debt collection software created by one of the defendant companies, ARS. AA alleged that the defendants misappropriated the trade secrets when ARS sold the software, AA's information included, to one of the other defendants in violation of an agreement with the plaintiff. The individual defendants, apparent officers of the corporate defendants, argued that they "never accessed AA's data and, thus, did not learn the secret."[62] But the court disagreed, stating that the individual defendants "had possession of and access to AA's trade secrets."[63] The court appeared to take the position that the individual defendants' possession of the software was enough, even though they claimed never to have accessed the information contained in the software.

The distinction between "knowledge" in the form of possession, on one hand, and "comprehension," which courts appear to agree is not required under the UTSA, on the other, could be one way to resolve the apparent tension between derivative trade secret claims and the UTSA's "knowledge of the trade secret" requirement. A plaintiff bringing a derivative claim could argue that the defendant's possession of the derivative constitutes constructive knowledge of the secret, which is akin to possessing information that one lacks the technical expertise to understand. That position may be more persuasive the easier it is to reverse engineer the trade secret. The more difficult this process is, the more strained the analogy becomes to possessing technical information one does not understand. Thus, as was the case for misappropriation by acquisition claims, the degree to which that trade secret can be reversed engineered from the derivative is a potentially important factual aspect of a derivative claim for misappropriation by use. When the trade secret can be reversed engineered relatively easily, there is a strong argument that a derivative claim satisfies the "knowledge of the trade secret" requirement.

C. Cases Not Recognizing Derivative Trade Secrets Claims

The opinion in *Silvaco Data Systems v. Intel Corp.*[64] is, perhaps, the most comprehensive judicial analysis of derivative trade secrets claims to date. In that case, the plaintiff, Silvaco, created a piece of software called SmartSpice, which simulated the properties of an electronic circuit before it was physically built. CSI, a competitor, misappropriated the trade secrets used in SmartSpice, aided by two former Silvaco employees, and used them to create its own software, DynaSpice. After obtaining a judgment against CSI, Silvaco brought actions against

[61] *Advanced Recovery Sys.*, 2017 WL 3912984, at *6.
[62] *Id.* at *6 (citing *Silvaco*, 109 Cal. Rptr. 3d).
[63] *Id.*
[64] *Silvaco*, 109 Cal. Rptr. 3d at 41.

several users of DynaSpice, including the defendant in this case, Intel, alleging that their use of the DynaSpice software was a misappropriation of Silvaco's trade secrets, namely, those embedded in the source code of SmartSpice. Intel defended against the claim by noting that it had never possessed or had access to any part of the SmartSpice source code: all it had was the *object* code (i.e. the zeros and ones, which are incomprehensible upon visual inspection) of the CSI software.

In affirming the trial court, the appellate court rejected Silvaco's acquisition claim on the basis that Intel had never come "into possession of the source code constituting the claimed trade secrets."[65] The court continued:

> Indeed, Silvaco does not directly argue that Intel acquired the trade secrets at issue but only that, under the terms of the statute, it *could* have done so without itself having "knowledge" of them. We doubt the soundness of this suggestion, but assuming it is correct, it remains beside the point unless Intel came into possession of the secret.[66]

Thus, the *Silvaco* court strongly implied that the defendant's knowledge of the relevant trade secret—which, as discussed above, is not explicitly part of the UTSA's definition of misappropriation by acquisition—is nonetheless a required element of a misappropriation by acquisition claim.

The *Silvaco* court then went on to reject Silvaco's misappropriation by use claim premised on Intel's use of the DynaSpice software. Its reasoning is worth quoting at length:

> One clearly engages in the "use" of a secret, in the ordinary sense, when one directly exploits it for his own advantage, e.g., by incorporating it into his own manufacturing technique or product. But "use" in the ordinary sense is not present when the conduct consists entirely of possessing, and taking advantage of, *something that was made* using the secret. One who bakes a pie from a recipe certainly engages in the "use" of the latter; but one who eats the pie does not, by virtue of that act alone, make "use" of the recipe in any ordinary sense, and this is true even if the baker is accused of stealing the recipe from a competitor, and the diner knows of that accusation. Yet this is substantially the same situation as when one runs software that was compiled from allegedly stolen source code. The source code is the recipe from which the pie (executable program) is baked (compiled).[67]

Silvaco can be understood to hold that the use of a derivative does not constitute use of the trade secret itself—a holding that appears to foreclose derivative claims for misappropriation by use.

Silvaco, however, differs factually from a typical derivative claim in several respects. First, the defendant in *Silvaco*, Intel, was an "end-user" of the product made using the trade secret, rather than the marketer and seller of the product. Instead, Intel positioned itself as a *customer* of a typical derivative claim defendant,

[65] *Id.* at 40.
[66] *Id.*
[67] *Id.* at 41.

rather than the defendant itself. This expressly factored into the *Silvaco* court's conclusion that Intel had not committed actionable "use" of Silvaco's trade secrets. The court explained:

> If merely running finished software constituted a use of the source code from which it was compiled, then every purchaser of software would be exposed to liability if it were later alleged that the software was based in part upon purloined source code. This risk could be expected to inhibit software sales and discourage innovation to an extent far beyond the intentions and purpose of [the California UTSA].[68]

VIA Technologies, which upheld a derivative misappropriation by use claim, distinguished *Silvaco* on precisely this basis, stating: "*Silvaco*, however, dealt with a . . . claim against an end user of the product, not a party actively marketing and selling the product for use by others."[69]

Relatedly, in *Silvaco* it is unclear whether Intel satisfied the *mens rea* requirements of the UTSA's definition of misappropriation. The *Silvaco* court emphasized that Intel had originally purchased DynaSpice without any knowledge of how it was developed, and that it had learned only later of mere *claims* by Silvaco that CSI had derived DynaSpice from Silvaco's trade secrets without authorization.[70] The court further explained: "Only when CSI entered into a stipulated judgment requiring it to stop using Silvaco code could an outsider rationally conclude that there was substance to Silvaco's claims. But that very judgment authorized CSI to continue marketing and supporting its products provided they were modified to excise Silvaco's trade secrets."[71] Thus, the court stated, "it is far from apparent that Intel's conduct here offended any sound or settled standard of commercial ethics."[72] This distinguishes *Silvaco* from *ClearOne*, *Cognis*, *VIA Technologies*, and *X6D*, in which, as noted above, it was alleged that the defendant knew that the derivative at issue was derived from the plaintiff's trade secrets.

Finally, in *Silvaco* it was "undisputed that the object code executed by Intel could not disclose the underlying source code or permit the exploitation of its features and design."[73] In other words, the parties agreed that the trade secret at issue (the source code) could not be reverse engineered from the derivative (the object code). This distinguishes *Silvaco* from *ATS Products*, in which the court upheld an acquisition claim based on the defendant's possession of a product from which the relevant trade secrets *could* be reverse engineered. And as explained above, the degree to which the relevant trade secrets can be reverse engineered logically has an effect on the persuasiveness on a derivative claim for misappropriation by use as well.

These aspects of the facts underlying *Silvaco*—the concession that the trade secrets could not be reverse engineered, Intel's status as an end user, and Intel's

[68] *Id.* at 41.

[69] *VIA Tech.*, 2015 WL 3809382, at *4.

[70] *Silvaco*, 109 Cal. Rptr. 3d at 46.

[71] *Id.*

[72] *Id.*

[73] *Id.* at 38.

"innocence"—suggest that the *Silvaco* court's sweeping statements about the meaning of "acquisition" and "use" are of more limited reach than they first appear. Perhaps for this reason, *Silvaco* has been relied on much less than might be expected for having such a long and thoroughly reasoned opinion.

The main exception is *ATS Products*, discussed above. Although the court in *ATS Products* held that the defendant's alleged acquisition of a resin from which the plaintiff's trade secrets could be reverse engineered stated an acquisition claim, in reliance on *Silvaco*, it dismissed the plaintiff's derivative misappropriation by use claim arising out of the same facts. It explained that the plaintiff, ATS, "has not alleged that [the defendant] Champion exploited its trade secrets for its own gain, an act that would constitute use. ATS has only alleged that Champion used the resin—not the trade secret formulas—to create the . . . product that it eventually sold to BART."[74] Like *Silvaco*, the court in *ATS Products* took the position that use of a derivative does not constitute actionable use of the underlying trade secrets.

Other courts dismissing what are effectively derivative trade secrets claims have not relied on *Silvaco*, and instead have tended to conceptualize the claims as attempting to impose secondary, or aiding-and-abetting, liability on the defendants. For example, in *Control Module, Inc. v. Data Management, Inc.*,[75] the plaintiff, Control Module, manufactured data-entry and control computer terminals according to the requirements of defendant, Data Management, which created software for use on the terminals. Encouraged by Data Management, two Control Module employees created their own company, Xipher, which produced terminals using Control Module's technology and sold them to Data Management. Control Module sued Data Management for misappropriation, but the court dismissed the claim, stating:

> The Complaint does not allege that Data Management itself acquired or disclosed or used the Trade Secrets, only that Data Management purchased Integrity terminals from Xipher and that Data Management induced, encouraged, aided, or abetted the principals of Xipher to use the Trade Secrets in creating the Integrity terminals. However, [the California UTSA] does not include within its definition of "misappropriation" inducing, encouraging, aiding, or abetting another to misappropriate a trade secret.[76]

Similarly, in a pre-*Silvaco* case, *Sonoma Foods, Inc. v. Sonoma Cheese Factory, LLC*,[77] the plaintiff hired a third party, Rumiano, to make flavored Jack cheese products based on recipes and formulas alleged to be trade secrets.[78] Rumiano terminated its relationship with the plaintiff, but continued to use the secrets to make cheese products, which it sold to defendant Cheese Factory. The court held that the plaintiff had not stated a misappropriation claim against Cheese Factory, which was alleged to be "merely a retail operation [that] does not make cheese

[74] *ATS Prods.*, 2013 WL 6086924, at *3.

[75] Control Module, Inc. v. Data Mgmt., No. 3:07CV00475 (AWT), 2007 WL 4333814 (D. Conn. Dec. 10, 2007).

[76] *Id.* at *4.

[77] Sonoma Foods, Inc. v. Sonoma Cheese Factory, LLC, No. C 07-00554 JSW, 2008 WL 913279 (N.D. Cal. Apr. 3, 2008).

[78] *Id.* at *3.

products."[79] The court explained that the plaintiff had not alleged that Cheese Factory had "used, disclosed, or marketed trade secrets—the recipes for Plaintiff's flavored Jack cheese products," but rather that Rumiano was alleged to have done so.[80] The court thus framed the claim as involving secondary liability, and concluded that "[p]laintiff has not alleged facts to support its theory that Cheese Factory may be vicariously or jointly liable for Rumiano's conduct."[81]

IV. CONCLUSIONS AND TAKEAWAYS

As the foregoing makes clear, whether derivative trade secret claims are cognizable is still an open question in many jurisdictions. The cases on this issue are inconsistent and generally focus on the specific facts before them without addressing the broader conceptual issue of whether such claims should be recognized. This means that it is hard to draw useful generalizations from these cases.

Nevertheless, the optics of a particular derivative claim appear to influence whether it is ultimately successful. A derivative claim is more likely to be upheld where the defendant is distributing the derivative for profit with the full knowledge that it was derived from trade secrets without authorization. As the *Silvaco* case shows, however, courts will understandably be more reluctant to find liability where the defendant is "innocent" and did not know about the trade secret origins of the derivative. Courts are also less likely to extend liability to mere end-users of a product than to those who attempt to profit off the plaintiff's trade secrets. Given the uncertain state of the law, it is incumbent on the plaintiff's litigation counsel to ensure that the defendant does not come across as an unsuspecting innocent party caught up in a trade secret dispute that does not concern it.

Another factor that appears to impact the outcome of a derivative trade secret claim is the degree to which the trade secret can be reverse engineered. For misappropriation by acquisition claims, if the trade secret can be reverse engineered, there is a strong argument that acquiring the derivative effectively means acquiring the trade secret itself. The fact that, in *Silvaco*, it was conceded that the trade secrets could not be reverse engineered may partly account for the difference in outcome between the acquisition claims in that case and in *ATS Products*. As to misappropriation by use claims, a plaintiff will have a stronger argument that the UTSA's "knowledge of the trade secret" requirement is satisfied if he can argue that the defendant's possession of the derivative amounts to constructive knowledge of the trade secret itself.

This is somewhat paradoxical, because the easier a trade secret is to reverse engineer, the greater the danger that it will in fact be reverse engineered and lose its trade secret protection. Accordingly, plaintiffs bringing derivative claims must take the usual precautions of owners of trade secrets that can easily be reverse engineered—namely, they must control the distribution of their derivatives through licenses, confidentiality agreements, contractual restrictions on reverse engineering, and the like.

[79] *Id.*
[80] *Id.*
[81] *Id.*

Litigation over the status of trade secret derivatives is not likely to disappear any time soon, but that status is still unclear. Given the idiosyncratic facts of *Silvaco*, which to date is the only case to squarely discuss the issue of derivative trade secrets claims, this is an area of the law that could benefit from further judicial discussion and development.