**Washington Journal of Law, Technology & Arts**

Volume 7 | Issue 2 Article 4

10-1-2011

# End User Liability for Sofware Developed with Trade Secrets

Jeff Patterson

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 7, ISSUE 2 FALL 2011

# END USER LIABILITY FOR SOFTWARE DEVELOPED WITH TRADE SECRETS

*Jeff Patterson* [*]


Cite as: 7 Wash J.L. Tech. & Arts 105 (2011)
http://digital.law.washington.edu/dspace-law/handle/1773.1/1068

## ABSTRACT

*The National Conference of Commissioners on Uniform State Laws (NCCUSL) developed the Uniform Trade Secrets Act (UTSA) to unify the laws regulating the improper use of secret, economically advantageous information. However, consumers often procure software and other products without knowledge of any trade secrets used in the production of the products. Some companies have sought remedies against end users of products developed using trade secrets. But in* Silvaco Data Systems v. Intel Corp.*, a California appeals court considering this issue in the software context held that execution of compiled object code, which is not easily interpreted by humans, is not an improper use of trade secrets embedded in the underlying, human-readable source code. This ruling implies that end users of software, and perhaps other products, are not liable for misappropriation of trade secrets merely through use of the end products. This Article surveys the application of the UTSA to software and explains why this holding is a proper reading of the Act's scope. In addition, this Article discusses the public policies behind this limitation on liability for end users and possible implications of the Silvaco ruling beyond software.*

---

[*] Jeff Patterson, University of Washington School of Law, Class of 2012; University of Colorado, Ph.D. 2001. Many thanks to Professor Jane Winn of The University of Washington School of Law and James Proctor and Heather Griffith, student editors, for their insightful feedback and invaluable guidance.

TABLE OF CONTENTS



## INTRODUCTION

Liability attaches when one improperly uses the trade secrets of another.[1] However, it is sometimes difficult to determine what actions constitute the use of a trade secret. For instance, can the use of a commercial product, such as software, developed with the stolen trade secrets of another, rise to improper use? Strong statutory construction and public policy arguments exist to limit the liability of such secondary users.

Today, the statutory language governing trade secret law is mostly uniform across the states.[2] However, courts have arrived at conflicting answers regarding the liability of end users of products developed with trade secrets. State common law traditionally governed trade secrets,[3] but since the introduction of the Uniform Trade Secrets Act (UTSA), most states have implemented statutes consistent with either the 1979 or 1985 versions of this uniform law. Even so, courts have varied in their application of the UTSA to determine a party's misappropriation liability when that party

[1] 1-1 ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS, § 1.01 (2010).

[2] 1-1 ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS, § 1.01[2][b] (2010) (most states have adopted trade secret laws consistent with either the UTSA (1979) or the UTSA (1985)).

[3] 1 MELVIN F. JAGER, TRADE SECRET LAW, § 2.3 (2010).

develops a product using trade secret information.

In Silvaco Data Systems v. Intel Corp,[4] a California appellate court applied the UTSA to limit the liability of a party that used commercial software developed with stolen trade secrets. The court held, "One does not, by executing machine-readable software, 'use' the underlying source code; nor does one acquire the requisite knowledge of any trade secrets embodied in that code."[5] This holding is in direct conflict with ClearOne Communications Inc., v. Chiang,[6] a prior opinion by a Federal District Court interpreting the UTSA in Utah.[7]

The question of improper use is critical to users of software and other commercial products. Many products are developed by employing various technologies, some of which are protected by patents, copyrights, and trade secrets. Users often obtain products in the stream of commerce without knowledge of any underlying intellectual property. Even the most diligent users cannot readily discover if all the required intellectual property assignments and licenses are properly in place to avoid infringement or misappropriation.

This Article discusses the UTSA and the unique complexities of its application to software. In addition, this Article explains why the holding in Silvaco—that the UTSA does not attach liability to the use of a product that was developed with trade secrets—is the proper reading of the model code's scope. Finally, this Article discusses the public policy reasons behind this limitation and possible implications beyond the software industry.

---

[4] Silvaco Data Systems v. Intel Corp., 184 Cal. App. 4th 210, 109 Cal. Rptr. 3d. 27 (Cal. Ct. App. 2010).

[5] Silvaco, 184 Cal. App. 4th at 216.

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

[7] The ClearOne case was recently affirmed by the Tenth Circuit (ClearOne Communications, Inc. v. Bowers, 643 F. 3d 735 (10th. Cir. 2011)). However, the issues considered on appeal were unrelated to the issues that are in conflict with the holdings of the Silvaco case. Thus, the Tenth Circuit's opinion does not address the conflict between the holdings of Silvaco and ClearOne.

## I. TRADE SECRET LAW AND THE UTSA

Like copyright law, trade secret law does not extend protection to ideas.[8] Trade secret protection instead covers information or facts.[9] As opposed to patent and copyright law, which require public disclosure, trade secret law protects information and requires the trade secret owner to undergo steps to keep the information secret.

Another way in which trade secrets are distinct from other areas of intellectual property is that federal law does not apply. Trade secret protection is under the governance of the states. During the twentieth century, as the importance of trade secrets to the national economy increased, the states' case law diverged.

In an effort to unify trade secret law across the states, the National Conference of Commissioners on Uniform State Law (NCCUSL) drafted the Uniform Trade Secrets Act (UTSA) and promulgated the model code in 1979. The NCCUSL amended the UTSA in 1985. By 2009, 46 states had adopted the UTSA.[10] In

---

[8] Silvaco, 184 Cal. App. 4th at 220.

[9] "Trade secret law does not protect ideas as such. Indeed a trade secret may consist of something we would not ordinarily consider an idea (a conceptual datum) at all, but more a fact (an empirical datum)." *Id.* (emphasis omitted).

[10] ALA. CODE §§ 8-27-1 to 8-27-6 (2011); ALASKA STAT. §§ 45.50.910 to 45.50.945 (2011); ARIZ. REV. STAT. §§ 44-401 to 44-407 (2011); ARK. CODE ANN. §§ 4-75-601 to 4-75-607 (2011); CAL. CIV. CODE §§ 3426 to 3426.11 (2011); COLO. REV. STAT. §§ 7-74-101 to 7-74-110 (2011); CONN. GEN. STAT. §§ 35-50 to 35-58 (2011); D.C. CODE, §§ 36-401 to 36-410 (1981); DEL. CODE ANN. tit. 6, §§2001 to 2009 (2011); FLA. STAT. §§ 688.001 TO 688.009 (2011); GA. CODE ANN. §§ 10-1-760 to 10-1-767 (2011); HAW. REV. STAT. §§ 484B-1 to 482B-9 (2011); IDAHO CODE ANN. §§ 48-801 to 48-807 (2011); 765 ILL. COMP. STAT. §§ 1065/1 to 1065/9 (2011); IND. CODE §§ 24-2-3-1 to 24-2-3-8 (2011); IOWA CODE §§ 550.1 to 550.8 (2011); KAN. STAT. ANN. §§ 60-3330 to 60-3330 (2011); KY. REV. STAT. ANN. §§ 365.880 to 365.900 (2011); LA. REV. STAT. ANN. §§ 51:1431 to 51.1439 (2011); ME. REV. STAT. tit. 10, §§ 1541 to 1548 (2011); MD. CODE ANN., COM. LAW §§ 11-1201 to 11-1209; MICH. COMP. LAWS §§ 445.1901 to 445.1910; MINN. STAT. §§ 325C.01 to 325C.08 (2011); MISS. CODE ANN. §§ 75-26-1 to 75-26-19; V.A.M.S. §§ 417.450–417.467 (1995); MONT. CODE ANN. §§ 30-14-401 to 30-14-409 (2011); NEB. REV. STAT. §§ 87-501 to 87-507 (2011); NEV. REV. STAT. §§ 600A.010 to 600A.100 (2011); N.H. REV. STAT. ANN. §§ 350-B:1 to 350-B:9; N.M. STAT. ANN. §§ 57-3A-1 to 57-3A-7 (2011); N.C. GEN. STAT. §§ 66-152 to 66-158 (2011); N.D. CENT.

2010, the Massachusetts and New Jersey legislatures introduced the act for adoption.[11] The only states that have not expressed intent to adopt the UTSA are New York and Texas.[12]

Section 1(4) of the UTSA defines a trade secret as "information, including a formula, pattern, compilation, program, device, method, technique, or process."[13] This definition places limitations on what is protectable, namely that a trade secret must be information. Section 1(4)(i) and 1(4)(ii) place further limitations on the definition of a trade secret: the information must have "economic value," must "not be generally known," must not be "readily ascertainable by proper means," and must be "the subject of reasonable efforts to maintain its secrecy."[14]

Section 1(2) of the UTSA attaches misappropriation liability to one who "improperly acquires, discloses, or uses another's trade secrets."[15] The Act "does not define these terms, but leaves their delineation to be adjudicated in the light of the purposes and provisions of the act."[16] The Act does list five actionable varieties of use, four of which clearly require the user to have "knowledge of the trade secret" while "[t]he fifth is arguably ambiguous on this point."[17]

---

CODE §§ 47-25.1-01 to 47-25.1-08 (2011); OHIO REV. CODE ANN. §§ 1333.61–69 (2011); OKLA. STAT. TIT. 78, §§ 85 to 95 (2011); OR. REV. STAT. §§ 646.461 to 646.475 (2011); 12 PA. CONS. STAT. ANN. §§ 5301–5308 (2011); R.I. GEN. LAWS §§ 6-41-1 to 6-41-11 (2011); S.C. CODE ANN. §§ 39-8-1 to 39-8-9 (2011); S.D. CODIFIED LAWS §§ 37-29-1 to 37-29-11 (2011); TENN. CODE ANN. §§ 47–25–1701 to 47–25–1709 (2011); UTAH CODE ANN. §§ 13-24-1 to 13-24-9 (2011); VT. STAT. ANN. TIT. 9, §§ 4601 to 4609, and TIT. § 523; VA. CODE ANN. §§ 59.1-336 to 59.1-343 (2011); WASH. REV. CODE ANN. §§ 19.108.010 to 19.108.940 (2011); W. VA. CODE §§ 47-22-1 to 47-22-10 (2011); WIS. STAT. ANN. § 134.90 (2011); and WYO. STAT. ANN. §§ 40-24-101 to 40-24-11 (2011). The varying effective dates of these laws are set forth in Uniform Trade Secrets Act, 14 UNIFORM LAWS ANNOTATED 537.

[11] Trade Secrets Act, THE NATIONAL CONFERENCE OF COMMISSIONERS ON UNIFORM STATE LAWS, http://www.nccusl.org (last visited Apr. 29, 2011).

[12] Id.

[13] UNIFORM TRADE SECRETS ACT § 1(4) (1985).

[14] U.T.S.A. § 1(4) (1985).

[15] U.T.S.A. § 1(2) (1985).

[16] Silvaco, 184 Cal. App. 4th at 222.

[17] Id. at 224.

## II. THE UTSA AS APPLIED TO SOFTWARE PRIOR TO SILVACO

Legal analysis of trade secret problems in the software context draws a critical distinction between two types of computer code: "source code" and "object code." When developing software, programmers often describe the underlying logic in a high-level language such as C or FORTRAN. This set of human-readable instructions is referred to as "source code." Many of these high-level languages are not directly executable by computer hardware, but must first be transformed into a machine language—also known as object code, executable code, or binary code. Specialized software tools perform this translation and optimize the resulting object code via a process known as "compiling." The resulting object code is in a binary format and not readable by humans. The reverse process, decompiling, or translating object code into human readable source code, is difficult and imperfect in practice. As the complexity of a software design increases, the difficulty of successfully decompiling the source code increases dramatically. Thus, distributing software in an object code format does not typically disclose the underlying design to the end user.

Courts have long held that software, in the form of source code, can contain information protected by trade secret law.[18] Courts have also recognized the disclosure distinctions inherent in the distribution[19] of software as source code versus as object code.[20] The distribution of object code might not disclose any trade secrets that are embedded in the source code from which it was compiled because object code does not disclose the details of the

[18] See Telex Corp. v. International Business Machines Corp., 367 F. Supp. 258 (N.D. Okl. 1978); Q-Co Industries, Inc. v. Hoffman, 625 F. Supp. 608 (S.D. N.Y. 1985); and Data Gen. Corp. v. Grumman Sys. Support Corp., 825 F. Supp. 340 (D. Mass. 1993).

[19] It is common practice in the software industry to distribute software in compiled, executable form only. One advantage to this practice is that the user has no access to the source code and thus, any embedded trade secrets remain secret.

[20] 2 MELVIN F. JAGER, TRADE SECRET LAW, 9. Secret Protection for Computer Technology, III. Computer Source Codes Versus Object Codes, § 9:11 (October 2010).

underlying design. Even if the source code contains information subject to trade secrecy protection, this embedded information remains secret.

Software, like many commercial products, often involves the integration of various independent technologies. These technologies are potentially protectable by various forms of intellectual property law and owned by disparate parties. Because end users often lack specific knowledge of the intellectual property used in application development, most software distributed through commercial channels is essentially a "black box."

Parties whose trade secrets are incorporated into source code that is later compiled and released as object code constituting software may desire remedies against third-party users of the software. However, whether the law extends trade secret protection to object code compiled from protected source code remained unsettled prior to the *Silvaco* decision. In the words of one pre-Silvaco commentator:

> If an object code represents secret novel and valuable information, its misappropriation in breach of confidence should be actionable. Cases involving the theft of object codes are rare, so that extension of trade secrets protection to object codes is supported more by logic and reason than by common law precedent.[21]

Two post-UTSA cases considered this issue. ClearOne Communications, Inc. v. Chiang,[22] discussed infra Section III(B), relied heavily on case law from non-UTSA jurisdictions. In McCormack Dodge Corp. v. ABC Management Systems Inc., a Washington state court took an expansive view of which assets are considered information eligible for protection. The court held that the software at issue included "(1) the source code . . . ; (2) the object code derived from the source code; (3) any flow charts and/or underlying algorithms derivable from the source code; and

---

[21] See JAGER, supra note 21, at 4.

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

(4) user manual, operations manual and installation manual."[23] In applying the UTSA, the court ruled that all the above components are protectable under trade secret law.[24]

In a pre-UTSA case, Computer Print Systems, Inc. v. Lewis, a court held an act of stealing object code to be a misappropriation of trade secrets.[25] There is an important factual distinction between this case and both Silvaco and ClearOne. The defendant in Computer Print breached a duty of confidence and stole the object code from the plaintiff. In both Silvaco and ClearOne, the defendant obtained the object code from a third party.

## III. THE SILVACO DECISION AND ITS REASONING

In April 2010, the California Court of Appeals in *Silvaco* considered the whether an unknowing end user of software is liable for misappropriation of trade secrets.[26] The defendant-appellee, Intel, obtained circuit simulation software in the form of object code from a third-party vendor, CSI.[27] Aided by two former Silvaco employees, CSI had stolen trade secrets in the form of source code from the plaintiff-appellant, Silvaco.[28] CSI then developed the compiled software product and delivered it to Intel.[29] In a prior proceeding, Silvaco had obtained a misappropriation judgment against CSI.[30]

Silvaco asserted that, under the California Uniform Trade Secret Act (CUTSA), Intel had also misappropriated its trade secrets.[31] Silvaco argued that: (1) "executable code incorporates the same 'information' as the source code from which it is

---

[23] McCormack Dodge Corp. v. ABC Management Systems, Inc. 222 U.S.P.Q. (BNA) 432, 433 (Wash. Super. Ct. 1983).

[24] Id. at 444.

[25] Computer Print Systems, Inc. v. Lewis, 821 Pa. Super. 240, 422 A.2d 148, 212 U.S.P.Q. (BNA) 626 (1980).

[26] Silvaco Data Systems v. Intel Corp., 184 Cal. App. 4th 210, 109 Cal. Rptr. 3d. 27 (Cal. Ct. App. 2010).

[27] Id. at 216.

[28] Id.

[29] Id.

[30] Id.

[31] Id.

compiled, so that executing it on a computer constitutes 'use' of any trade secrets reflected in the source code";[32] (2) "apart from the informational content of the source code, the secrets claimed by it include certain 'methods, techniques, and algorithms' that were 'contain[ed]' and 'use[d]' in the executable code"[33]; and (3) that liability under CUTSA does not require comprehension of the trade secret.[34]

In response, Intel claimed that: (1) "it never possessed the source code identified by Silvaco as constituting and containing its trade secrets, but only executable code supplied by CSI";[35] and (2) "the possession and use of [the software] in the form of executable object code or binary code could not impart knowledge of any trade secrets embodied in the source code."[36]

The trial court recognized a difference between the source code and object code versions of the software. Because source code is merely the information that communicates or enables the functionality and design of the software,

> [B]y acquiring the CSI software that 'embodies' Silvaco's source code, Intel did not acquire, or gain knowledge of, the information that constitutes Silvaco's alleged trade secret . . . . It is not the functionality of the CSI software that constitutes Silvaco's alleged trade secret, but Silvaco's means of creating that functionality through the source code.[37]

The appellate court affirmed on summary judgment, stating that a defendant cannot "be liable for misappropriation of a trade secret which is admittedly embodied in *source* code, based upon the act of executing, on his own computer, *executable* code allegedly tainted by the incorporation of design features

---

[32] Id. at 218.
[33] *Id.* (emphasis omitted).
[34] Id.
[35] Id. at 217 (emphasis omitted).
[36] Id. at 218.
[37] Id. at 219.

wrongfully derived from the plaintiff's source code."[38]

The appellate court's analysis relied primarily on two legal determinations: (1) that one does not ordinarily use source code by executing the object code compiled from the source code; and (2) that one does not acquire the requisite knowledge of any trade secrets embedded in the underlying source code by executing the object code.[39]

### *A. What Information is a Trade Secret as it Pertains to Software*

The first key issue decided by the appellate court was which of Silvaco's assets are protectable under the UTSA. It is undisputed that the defendant only ever had access to compiled object code, which is unreadable by humans. Therefore, the plaintiff, in order to establish grounds for misappropriation liability, attempted to define its trade secrets as "various features, functions, and characteristics of the design and operation of . . . software,"[40] as well as a method for carrying out the functionality of its software.

Designs are not subject to trade secrecy protections. The *Silvaco* court stated that a "design may constitute the basis for a trade secret, such that information concerning it could be actionably misappropriated; but it is the information—not the design itself—that must form the basis for the cause of action."[41] The court found that "the only trade secrets at issue are found in Silvaco's source code."[42] While "the finished (compiled) product might have distinctive characteristics resulting from the design—such as improved performance—they cannot constitute trade secrets because they are not secret, but are evident to anyone running the finished program."[43] Thus, to establish improper use of a trade secret embedded in software in California, a plaintiff must establish *use* of the underlying source code.

---

[38] Id. at 220.
[39] Id. at 216.
[40] Silvaco, 184 Cal. App. 4th at 221.
[41] Id. at 221-22 (emphasis omitted).
[42] Id. at 222.
[43] Id.

### *B. What Constitutes Use of a Trade Secret When Executing Software*

The court in Silvaco looked to the UTSA drafters' intention and determined that their choice of the noun "use" was meant in the ordinary sense.[44] The term commonly implies "if not direct physical possession, at least a certain proximity or immediacy to the thing used."[45]

For misappropriation by use, the UTSA requires that "at the time of disclosure or use, [the defendant] knew or had reason to know that his knowledge of the trade secret was acquired under circumstances giving rise to a duty to maintain its secrecy."[46] In order to improperly use a trade secret, one must have knowledge of the trade secret.

Knowledge of information requires possession of the information. The court stated that "[t]o say that one 'knows' a fact is also to say that one possesses information of that fact."[47] If the disputed trade secret is source code, then in order to use the information, one must possess the source code. Knowledge of the trade secret does not require comprehension of the information to claim misappropriation;[48] however, a proximity or immediacy to the information is required.

### *C. Contrasting Silvaco with ClearOne*

Although the facts of ClearOne Communications, Inc. v. Chiang[49] are strikingly similar to those of *Silvaco*, the federal court in Utah interpreted the UTSA to reach an opposite result. Applying Utah's enactment of the UTSA, the district court held that one may be liable for misappropriation by executing object code.[50] In *ClearOne*, a third party, WideBand, stole the plaintiff's source

---

[44] Id. at 223.
[45] Id. at 223.
[46] U.T.S.A. § 1(2)(B) (1985).
[47] Silvaco, 184 Cal. App. 4th at 226 (emphasis omitted).
[48] ClearOne, 2007 WL 4376125 at *2.
[49] Id.
[50] Id.

code with the aid of an ex-employee of ClearOne. WideBand compiled the source code and licensed the resulting object code to the defendant, Biamp. The plaintiff, ClearOne, obtained a misappropriation judgment against WideBand and also claimed that Biamp, by executing the object code, improperly used its trade secrets.

In a brief footnote, the court declared ClearOne's "proprietary software" to be a trade secret.[51] The court deemed ClearOne's "computer code, computer code architecture . . . and algorithms" to be trade secrets under the UTSA.[52] Under this analysis, the court appears not to distinguish between information that communicates a design and the design itself.

The court acknowledges the mental state requirement of the defendant (knowledge of the trade secret).[53] However, in another footnote, the court states that the statutory language is "generally understood to reflect knowledge that the trade secret was derived through improper means,"[54] as opposed to actual knowledge of the information. The court cites a treatise to justify this understanding, stating that liability will only attach "after having actual knowledge or reason to know that the information was improperly obtained."[55]

As a rebuttal to the plaintiff's citing of ClearOne, the Silvaco court states that "[t]he statute specifies required mental states with respect to both the trade secret *and* the means by which it became available to the defendant. To equate one of these requirements with the other offends basic principles of statutory construction."[56] In addition, the Silvaco court points out that the cited treatise has been superseded and was likely quoted out of context.[57]

The ClearOne court did not analyze the distinction between source code and object code as information. From the language of the opinion, one can infer the court's view: if the source code is

---

[51] *Id* at 2 n.2.
[52] Id.
[53] Id. at 2.
[54] Id. at 2 n.3.
[55] Id. at 2 n.3 (citing JAGER, Trade Secrets Law § 2:03) (emphasis omitted).
[56] Silvaco, 184 Cal. App. 4th at 228 (citing ClearOne, 2007 WL 4376125).
[57] Id. at 227.

eligible for protection, then the compiled object code is also a de facto trade secret. In order to establish that object code is eligible for protection, the court cites Data General Corp. v. Grumman Systems. Support Corp.[58] In that case, a defendant was liable for misappropriation when it loaded and ran the plaintiff's object code. Both the ClearOne and Data General courts relied on an older, pre-UTSA opinion involving a plaintiff's object code, Trandes Corp. v. Guy F. Atkinson Co.[59] The Trandes Corp. court stated, "An infringer may be liable for misappropriating trade secrets when it loads and runs a computer program in its object code form, even if the infringer never understands exactly how the program works."[60] These cases hold that trade secret law protects object code compiled from source code containing trade secrets. Because both Data General and Trandes are pre-UTSA holdings these opinions may not have been persuasive to the Silvaco court.

## IV. POSSIBLE IMPLICATIONS BEYOND SOFTWARE

Although Silvaco is a software case, its holding may be significant for parties using other technologies that incorporate trade secrets. The *Silvaco* opinion limits the liability of end users at the expense of the rights and privileges of trade secret holders. The ClearOne court espoused the opposite tradeoff. However, because ClearOne's analysis relied on pre-UTSA case law and did not distinguish between information and designs, the Silvaco decision is more consistent with the scope of the UTSA and its underlying public policy rationales.

The Silvaco court limited the liability of those that use products developed with another's trade secrets. " '[U]se' in the ordinary sense is not present when the conduct consists entirely of possessing, and taking advantage of, something that was made

[58] Data General Corp. v. Grumman Sys. Support Corp., 825 F. Supp. 340 (D. Mass. 1993).

[59] Trandes Corp. v. Guy F. Atkinson Co., 798 F. Supp. 284 (D. Md. 1992).

[60] See ClearOne, 2007 WL 4376125 at *3. See also Data General, 825 F. Supp. at 359; Trandes Corp. v. Guy F. Atkinson Co., 798 F. Supp. 284 (D. Md. 1992).

using the secret."[61] The Silvaco court also stated, "[U]sing a product does not constitute a 'use' of trade secrets employed in its manufacture."[62] These statements are not specific to software technologies.

Public policy also justifies the application of Silvaco to other industries. Many products in the stream of commerce involve multiple layers of intellectual property and do not provide the end user proper notice of the underlying rights. Even if producers had incentives to disclose intellectual property used in the manufacture of a product, consumers would experience an undue burden when attempting to draw lines between proper and improper use.

This burden and potential liability would distort the supply and demand curves for products. Even though Silvaco states this principle in terms of software, the result is applicable to many industries. If the act of running completed 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 latter alleged that the software was based in part upon purloined source code. This risk could be expected to inhibit . . . sales and discourage innovation."[63]

The Silvaco court's use of a familiar analogy demonstrates the potential application of its holding to products beyond software.[64] In this analogy, a pie recipe represents the trade secret (which, in Silvaco, was the source code) and the baked pie represents the finished product (object code). A person "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 an ordinary sense, and this is true even if the baker is accused of stealing the recipe from a competitor, and the diners know this acquisition."[65] In the same fashion, a person who uses an end product that incorporates trade secrets should not be subject to liability for that use alone.

---

[61] Silvaco, 184 Cal. App. 4th at 224 (emphasis omitted).
[62] Id.
[63] Id. (emphasis omitted)
[64] *See* id.
[65] Id.

## CONCLUSION

The California Court of Appeals in Silvaco expressly held that the execution of binary object code is not an improper use of any trade secrets embedded in the underlying source code. This holding releases end users of compiled software obtained in good faith from claims of misappropriation.

Although Silvaco directly contradicts ClearOne, another UTSA case, the holding in Silvaco is more consistent with the UTSA. By extending protection to the execution of object code, the ClearOne court appears to extend trade secret status to designs and functionality, which are not within the scope of the UTSA. In addition, the ClearOne court seems to rely on pre-UTSA case law to arrive at this holding.

The Silvaco holding is not limited to the software industry. Because of the public policies at stake, an unknowing end user of a product is not liable for the improper use of the trade secrets used to produce a product.

## PRACTICE POINTERS

- Educate clients about the risks associated with acquiring technology that might have third party intellectual property embedded in the technology. Advise clients that one strategy to minimize such risks is to require the vendor to provide IP infringement indemnities.
- Advise clients that any executable software the client procures from another party may contain the trade secrets of other parties. Depending upon the relevant state, executing that software may give rise to liability for the misappropriation of trade secrets.
- If a client suspects a piece of executable software to contain the trade secrets of someone other than the party from whom it obtained the software, the client may wish to run the software on servers physically located in the state of California.
- If a client suspects its source code was embedded in another party's object code and is attempting to enforce its

rights under the UTSA, the client may wish to attempt to bring suit in the state of Utah.

- If a client embeds trade secrets in its source code, the client should treat both the source code and the compiled object code as trade secrets. Any licensing of these assets should include non-disclosure agreements to maintain secrecy.