Filed 2/27/04 subsequent opinion following remand

**CERTIFIED FOR PUBLICATION**

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA

SIXTH APPELLATE DISTRICT

| | |
|---|---|
| DVD COPY CONTROL ASSOCIATION INC.,<br><br>Plaintiff and Respondent,<br><br>v.<br><br>ANDREW BUNNER,<br><br>Defendant and Appellant. | H021153<br>(Santa Clara County<br>Super. Ct. No. CV786804) |

Plaintiff DVD Copy Control Association, Inc. (DVD CCA) sued defendant Andrew Bunner (Bunner) and others under California's Uniform Trade Secrets Act (UTSA) (Civ. Code, § 3426 et seq.),[1] seeking an injunction to prevent defendants from using or publishing "DeCSS," a computer program allegedly containing DVD CCA's trade secrets.

The trial court granted DVD CCA's request for a preliminary injunction and entered an order prohibiting defendants from posting, disclosing, or distributing DeCSS or related proprietary material. Bunner appealed. His primary argument on appeal was that the injunction infringed his free speech rights under the state and federal constitutions. This court concluded that the injunction was an unconstitutional prior restraint and reversed.

The California Supreme Court granted review and held that the preliminary injunction did not violate the free speech clauses of the United States and California

[1] Hereafter, all undesignated statutory references are to the Civil Code.

Constitutions "*assuming* the trial court properly issued the injunction under California's trade secret law." (*DVD Copy Control Assn., Inc. v. Bunner* (2003) 31 Cal.4th 864, 889 (*DVD*).) The Supreme Court remanded the matter to this court to determine whether the evidence in the record supports the factual findings necessary to establish that the preliminary injunction was warranted under the UTSA. (*Id.* at p. 890.) We now conclude that it was not.[2]

## I. FACTUAL AND PROCEDURAL BACKGROUND

### *A. Introduction*

Digital versatile disks (DVDs) are five-inch discs used to store large amounts of data in digital form. A single DVD may contain a full-length motion picture. Unlike motion pictures on videocassettes, motion pictures contained on DVDs may be copied without perceptible loss of video or audio quality. This aspect of the DVD format makes it particularly susceptible to piracy. For this reason, motion pictures stored on DVDs have been protected from unauthorized use by a content scrambling system referred to as CSS. Simply put, CSS scrambles the data on the disk and then unscrambles it when the disk is played on a compliant DVD player or computer. CSS does not allow the content on the DVD to be copied. (*DVD*, *supra*, 31 Cal.4th at p. 871.)[3]

For obvious reasons, the motion picture industry desired to keep the CSS technology a secret. But to make DVD players and computer DVD drives that can unscramble and play a CSS-protected DVD, the manufacturers had to have the CSS

---

[2] After the parties had completed the briefing on remand, DVD CCA filed a voluntary dismissal without prejudice in the court below and moved this court to dismiss the appeal as moot. Bunner opposed. Concluding that the appeal presents important issues that could arise again and yet evade review, we denied the motion. (See *NBC Subsidiary* (*KNBC-TV*), *Inc. v. Superior Court* (1999) 20 Cal.4th 1178, 1190, fn. 6.)

[3] For a more detailed explanation of the CSS technology see *DVD*, *supra*, 31 Cal.4th at pages 870-872 and *Universal City Studios, Inc. v. Reimerdes* (S.D.N.Y. 2000) 111 F.Supp.2d 294, 305-311 (*Reimerdes*).

"master keys" and an understanding of how the technology works. In an attempt to keep CSS from becoming generally known, the industries agreed upon a restrictive licensing scheme and formed DVD CCA to be the sole licensing entity for CSS. Under the CSS licensing scheme, each licensee receives a different master key to incorporate into its equipment and sufficient technical know how to permit the manufacture of a DVD-compliant device. All licensees must agree to maintain the confidentiality of CSS.

In spite of these efforts to maintain the secrecy of CSS, DeCSS appeared on the Internet sometime in October 1999 and rapidly spread to other Web sites, including those of the defendants. According to DVD CCA, DeCSS incorporates trade secret information that was obtained by reverse engineering[4] CSS in breach of a license agreement. DVD CCA alleges that DeCSS allows users to illegally pirate the copyrighted motion pictures contained on DVDs, "activity which is fatal to the DVD video format and the hundreds of computer and consumer electronics companies whose businesses rely on the viability of this digital format."

DVD CCA filed the instant complaint for injunctive relief on December 27, 1999, alleging that Bunner and the other defendants had misappropriated trade secrets by posting DeCSS or links to DeCSS on their Web sites, knowing that DeCSS had been created by improper means. The requested injunctive relief sought to prevent defendants from using DeCSS, from disclosing DeCSS or other proprietary CSS technology on their Web sites or elsewhere, and from linking their Web sites to other Web sites that disclosed DeCSS or other CSS technology.

After first denying DVD CCA's request for a temporary restraining order, the trial court issued a preliminary injunction on January 21, 2000, enjoining defendants from

[4] Reverse engineering is the process by which one starts with a known product and works backward to determine how it was developed or manufactured. (*Kewanee Oil Co. v. Bicron Corp*. (1974) 416 U.S. 470, 476.) The concept is not limited to computer software but applies to any product or process.

"[p]osting or otherwise disclosing or distributing, on their websites or elsewhere, the DeCSS program, the master keys or algorithms of [CSS], or any other information derived from this proprietary information." The injunction does not prohibit linking to other Web sites and it does not expressly prohibit defendants from "using" DeCSS.

### *B. The Factual Record*

The evidence before the trial court was submitted in the form of written declarations. John Hoy, President of DVD CCA explained that DeCSS first appeared on the Internet on October 6, 1999. That first posting was in machine-readable form referred to as object code.[5] The DeCSS source code was posted about three weeks later, on or around October 25, 1999. Hoy declared that both postings contain CSS technology and the master key that had been assigned to DVD CCA's licensee, Xing Technology Corporation (Xing), a manufacturer of computer DVD drives. The intended inference is that DeCSS was created, at least in part, by reverse engineering the Xing software. Since Xing licensed its software pursuant to an agreement that prohibits reverse engineering, Hoy concludes that the CSS technology contained in DeCSS was "obtained in violation of the specific provision in the Xing end-user license 'click wrap' agreement which prohibits reverse engineering." Hoy stated on information and belief that Jon Johansen, a resident of Norway, was the author of the program.

Well before DeCSS was released on the Internet, a number of people had become interested in unraveling the CSS security system. Users of the Linux computer operating system[6] had organized a forum dedicated to finding a way to override CSS. Apparently DVD CCA had not licensed CSS to anyone making DVD drives for the Linux system, so

---

[5] To oversimplify, object code is a set of instructions comprised of strings of 1's and 0's. The same instructions written in programming language is referred to as source code. To be executable by a computer, source code must be translated into object code. (*Reimerdes*, *supra*, 111 F.Supp.2d at p. 306.)

[6] Linux is an operating system available for free on the Internet. It is popular with computer scientists and programmers. (*Reimerdes*, *supra*, 111 F.Supp.2d at p. 305.)

that computers using Linux were incapable of playing DVDs. CSS was widely analyzed and discussed in the academic cryptography community. Another exchange of information took place on www.slashdot.org (Slashdot), a news Web site popular with computer programmers. As early as July 1999 comments on Slashdot revealed a worldwide interest in cracking CSS. The gist of these communications is contained in the following excerpts of a discussion that took place on July 15, 1999:

"Yes, it is true, we have now all needed parts for software decoding of DVDs, but any software doing so will be illegal and/or non-free. [¶] . . . The information about CSS was obtained by reverse engineering some DVD software decoder."

"This code was released before anyone checked into the legal end of things. . . . Best idea now is to download the code. Get it spread around as widely as possible. It may not be able to be used legally when all is said and done, but at least it will be out there for others to work with."

"Well, it might not be the most ethical thing on earth, but if the appropriate algorithms were to be found just lying on the web, once the coders have seen them, they don't have a 'forget' button for their brains. . . ."

Bunner first became aware of DeCSS on or about October 26, 1999 as a result of reading and participating in discussions on Slashdot. Bunner explained that he is a part-time user of Linux and supports its acceptance as a viable alternative to established computer operating systems such as Microsoft Windows. Bunner thought DeCSS would be useful to other Linux users. He claimed that at the time he posted the information on his Web site he had no information to suggest that the program contained any trade secrets or that it involved the misappropriation of trade secrets. There is no evidence as to the date Bunner first posted the program on his Web site.

Counsel representing the motion picture industry had become aware of the DeCSS posting on October 25, 1999. Beginning November 4, 1999, counsel sent letters to Web site operators and Internet service providers hosting Web pages that contained DeCSS or

links to DeCSS and demanded the information be taken down. Sixty-six such letters were sent between November 4 and November 23, 1999. None of the letters listed in counsel's declaration were addressed to Bunner or to his Web site address. About 25 of the 66 sites were taken down. DeCSS was also removed from Johansen's Web site on or around November 8, 1999, but a link to DeCSS reappeared on the same site on or around December 11, 1999.

Meanwhile, the news that the CSS encryption system had been penetrated made headlines in Internet news magazines. *Wired News* ran several articles in the first days of November 1999 announcing the development of DeCSS. An article on November 4, 1999 said: "It shouldn't be surprising that an awful lot of people are upset at this week's Wired News reports about a utility to remove DVD security. But it's out there and people are using it." An article on *eMedia* around the same time explained that DeCSS was "available for free download from several sites on the World Wide Web."

DVD CCA filed suit on December 27, 1999, naming as defendants the operators of every infringing Web site it could identify. A hearing for a temporary restraining order was to be held the following day. In support of that application, DVD CCA informed the court that since October 25, 1999, DeCSS had been displayed on or linked to at least 118 Web pages in 11 states and 11 countries throughout the world and that approximately 93 Web pages continued to publish infringing information.

The lawsuit outraged many people in the computer programming community. A campaign of civil disobedience arose by which its proponents tried to spread the DeCSS code as widely as possible before trial. Some of the defendants simply refused to take their postings down. Some people appeared at the courthouse on December 28, 1999 to pass out diskettes and written fliers that supposedly contained the DeCSS code. They made and distributed tee shirts with parts of the code printed on the back. There were even contests encouraging people to submit ideas about how to disseminate the information as widely as possible.

### *C. The Trial Court's Findings*

The trial court issued the preliminary injunction based upon the following findings: First, CSS is DVD CCA's trade secret and for nearly three years prior to the posting of DeCSS on defendants' Web sites, DVD CCA had exerted reasonable efforts to maintain the secrecy of CSS. The court stated that trade secret status should not be deemed destroyed merely because the information was posted on the Internet, because, "[t]o hold otherwise would do nothing less than encourage misappropriaters [*sic*] of trade secrets to post the fruits of their wrongdoing on the Internet as quickly as possible and as widely as possible thereby destroying a trade secret forever."

Second, the trial court found that the evidence was "fairly clear" that the trade secret had been obtained through a reverse engineering procedure that violated the terms of a license agreement and, based upon some defendants' boasting about their disrespect for the law, it could be inferred that all defendants knew that the trade secret had been obtained through improper means.

Third, the balancing of equities favored DVD CCA. The court determined that while the harm to defendants in being compelled to remove trade secret information from their Web sites was "truly minimal," the current and prospective harm to DVD CCA was irreparable in that DVD CCA would lose the right to protect CSS as a trade secret and to control unauthorized copying of DVD content. The court pointed out: "once this information gets into the hands of an innocent party, the Plaintiff loses their [*sic*] ability to enjoin the use of their [*sic*] trade secret. If the court does not immediately enjoin the posting of this proprietary information, the Plaintiff's right to protect this information as secret will surely be lost, given the current power of the Internet to disseminate information and the Defendants' stated determination to do so." The trial court did not expressly consider the harm to defendants' First Amendment rights.

## II. DISCUSSION

### *A. Standard of Review*

A preliminary injunction is appropriate to maintain the status quo pending trial of the merits. (*Paradise Hills Associates v. Procel* (1991) 235 Cal.App.3d 1528, 1537.) The UTSA expressly provides for an injunction preventing the disclosure of a trade secret. (§ 3426.2.) "Injunctions in the area of trade secrets are governed by the principles applicable to injunctions in general. (*Hilb*, *Rogal & Hamilton Ins. Services v. Robb* (1995) 33 Cal.App.4th 1812, 1820, fn. 4.) 'In deciding whether to issue a preliminary injunction, a trial court weighs two interrelated factors: the likelihood the moving party ultimately will prevail on the merits, and the relative interim harm to the parties from the issuance or nonissuance of the injunction.' (*Hunt v. Superior Court* (1999) 21 Cal.4th 984, 999.)" (*Whyte v. Schlage Lock Co*. (2002) 101 Cal.App.4th 1443, 1449-1450.)

Citing *California Assn. of Dispensing Opticians v. Pearle Vision Center, Inc.* (1983) 143 Cal.App.3d 419, 433-434 (*Pearle Vision*), DVD CCA argues that where, as here, injunctive relief is authorized by statute, the moving party need not show irreparable injury. *Pearle Vision* affirmed an injunction sought by the State Board of Optometry, among others, stating " 'where an injunction is authorized by statute, a violation thereof is good and sufficient cause for its issuance.' " (*Id.* at p. 433.) However, the same district court of appeal has since declared "this assertion is, as a blanket statement of law, incorrect." (*Leach v. City of San Marcos* (1989) 213 Cal.App.3d 648, 661.) "When the plaintiff is not a governmental entity and the statute does not expressly provide otherwise, a finding of interim harm is necessary." (*Id.* at pp. 661-662.) Thus, even if *Pearle Vision* were a correct statement of the law, it would not apply here. The UTSA does not authorize an injunction in the absence of a showing of harm and DVD CCA is not a public entity. DVD CCA must have demonstrated both that it had a

likelihood of success on the merits and that the balance of harms weighed in favor of granting the injunction.

The conclusions of the trial court on these points are typically subject to a deferential standard of review. (*Whyte v. Schlage Lock Co*., *supra*, 101 Cal.App.4th at p. 1450.) However, "where a [F]ederal right has been denied as the result of a [factual] finding . . . or where a conclusion of law as to a Federal right and a finding of fact are so intermingled as to make it necessary, in order to pass upon the Federal question, to analyze the facts," appellate review is not so deferential. (*Fiske v. Kansas* (1927) 274 U.S. 380, 385-386.) The reviewing court must independently review the record to determine whether it supports the requisite factual findings with convincing clarity. (*Bose Corp. v. Consumers Union of U.S., Inc*. (1984) 466 U.S. 485, 514.)

This constitutional standard of review applies here. The Supreme Court's conclusion that the preliminary injunction did not offend Bunner's constitutional rights was premised upon the assumption that the injunction was proper under the UTSA. (*DVD*, *supra*, 31 Cal.4th at pp. 889-890.) It follows that we must now exercise our independent judgment to determine whether the record is adequate to establish, with convincing clarity, that the assumption is correct.

*B. The Existence of a Trade Secret.*

In order to obtain an injunction prohibiting disclosure of an alleged trade secret, the plaintiff's first hurdle is to show that the information it seeks to protect is indeed a trade secret. The UTSA defines a trade secret as "information . . . that: [¶] (1) Derives independent economic value, actual or potential, from not being generally known . . . ; and [¶] (2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy." (§ 3426.1, subd. (d).) In short, the test for a trade secret is whether the matter sought to be protected is information (1) that is valuable because it is unknown to others and (2) that the owner has attempted to keep secret. (*ABBA Rubber Co. v. Seaquist* (1991) 235 Cal.App.3d 1, 18.) The first element is the crucial one here: in

order to qualify as a trade secret, the information "must be secret, and must not be of public knowledge or of a general knowledge in the trade or business." (*Kewanee Oil Co. v. Bicron Corp.*, *supra*, 416 U.S. at p. 475.)

The secrecy requirement is generally treated as a relative concept and requires a fact-intensive analysis. (1 Milgrim on Trade Secrets (2003) § 1.07[2], pp. 1-343, 1-352.) Widespread, anonymous publication of the information over the Internet may destroy its status as a trade secret. (*Religious Technology Center v. Netcom On-Line Com*. (N.D.Cal. 1995) 923 F.Supp. 1231, 1256; see also *Religious Tech. Center v. NetCom On-Line Comm*. (N.D.Cal. 1995) 907 F.Supp. 1361.) The concern is whether the information has retained its value to the creator in spite of the publication. (See Rest.3d Unfair Competition, § 39, com. f, p. 431.) Publication on the Internet does not necessarily destroy the secret if the publication is sufficiently obscure or transient or otherwise limited so that it does not become generally known to the relevant people, i.e., potential competitors or other persons to whom the information would have some economic value.

In the instant matter, the secrecy element becomes important at two points. First, if the allegedly proprietary information contained in DeCSS was already public knowledge when Bunner posted the program to his Web site, Bunner could not be liable for misappropriation by republishing it because he would not have been disclosing a trade secret.[7] Second, even if the information was not generally known when Bunner posted it,

[7] "Misappropriation" of a trade secret includes: "(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: [¶] . . . [¶] (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; . . ." (§ 3426.1, subd. (b).) "Improper means," in turn, is defined to include "theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means. Reverse engineering or independent derivation alone shall not be considered improper means." (*Id*. at subd. (a).)

if it had become public knowledge by the time the trial court granted the preliminary injunction, the injunction (which only prohibits *disclosure*) would have been improper because DVD CCA could not have demonstrated interim harm.

1. The Likelihood of Prevailing on the Merits

The trial court did not make an express finding that the proprietary information contained in DeCSS was not generally known at the time Bunner posted it. Indeed, there is no evidence to support such a finding. Bunner first became aware of DeCSS on or around October 26, 1999. But there is no evidence as to when he actually posted it. Indeed, neither Bunner's name nor his Web site address appears among the 66 cease and desist letters counsel sent in November. We do know, however, that by the first week in November Internet news magazines were publicizing the creation of DeCSS and informing readers that the program was available to be downloaded for free on the Internet. As early as July 1999 people in the computer programming community were openly discussing the fact that the CSS code had been reverse engineered and were brainstorming ways to be able to use it legally. That means that when DeCSS appeared in October 1999 there was a worldwide audience ready and waiting to download and re-post it.

DVD CCA urges us, in effect, to ignore the fact that the allegedly proprietary information may have been distributed to a worldwide audience of millions prior to Bunner's first posting. According to DVD CCA, so long as Bunner knew or should have known that the information he was republishing was obtained by improper means, he cannot rely upon the general availability of the information to the rest of the world to avoid application of the injunction to him. In support of this position, DVD CCA contends that the denial of an injunction would offend the public policies underlying trade secret law, which are to enforce a standard of commercial ethics, to encourage research and invention, and to protect the owner's moral entitlement to the fruits of his or her labors. (See *DVD*, *supra*, 31 Cal.4th at pp. 880-882.) DVD CCA points out that

these policies are advanced by making sure that those who misappropriate trade secrets do not avoid "judicial sanction" by making the secret widely available.

The first problem with this argument is that by denying a preliminary injunction the court does not per se protect a wrongdoer from judicial sanction, which in most cases would come following trial on the merits.

Second, the evidence in this case is very sparse with respect to whether the offending program was actually created by improper means. Reverse engineering alone is not improper means. (See footnote 7 *ante*.) Here the creator is believed to be a Norwegian resident who probably had to breach a Xing license in order to access the information he needed. We have only very thin circumstantial evidence of when, where, or how this actually happened or whether an enforceable contract prohibiting reverse engineering was ever formed.

Finally, assuming the information was originally acquired by improper means, it does not necessarily follow that once the information became *publicly* available that everyone else would be liable under the trade secret laws for re-publishing it simply because they knew about its unethical origins. In a case that receives widespread publicity, just about anyone who becomes aware of the contested information would also know that it was allegedly created by improper means. Under DVD CCA's construction of the law, in such a case the general public could theoretically be liable for misappropriation simply by disclosing it to someone else. This is not what trade secret law is designed to do.

It is important to point out that we do not assume that the alleged trade secrets contained in DeCSS became part of the public domain simply by having been published on the Internet. Rather, the evidence demonstrates that in this case, the initial publication was quickly and widely republished to an eager audience so that DeCSS and the trade secrets it contained rapidly became available to anyone interested in obtaining them. Further, the record contains no evidence as to when in the course of the initial distribution

of the offending program Bunner posted it. Thus, DVD CCA has not shown a likelihood that it will prevail on the merits of its claim of misappropriation against Bunner.

2. Interim Harm

The element of secrecy also bears upon the question of interim harm. The Restatement explains the relationship this way: "Injunctive relief is often appropriate in trade secret cases to insure against additional harm from further unauthorized use of the trade secret and to deprive the defendant of additional benefits from the appropriation. If the information has not become generally known, an injunction may also be appropriate to preserve the plaintiff's rights in the trade secret by preventing a public disclosure. If the trade secret has already entered the public domain, an injunction may be appropriate to remedy any head start or other unfair advantage acquired by the defendant as a result of the appropriation. However, if the defendant retains no unfair advantage from the appropriation, an injunction against the use of information that is no longer secret can be justified only on a rationale of punishment and deterrence. Because of the public interest in promoting competition, such punitive injunctions are ordinarily inappropriate in trade secret actions." (Rest.3d Unfair Competition, § 44, com. c, p. 500.)

As the trial court clearly explained, the preliminary injunction prohibiting disclosure was intended to protect the trade secret. Therefore, even if Bunner was liable for misappropriation, if the information had since become generally known, a preliminary injunction prohibiting disclosure would have done nothing to protect the secret because the secret would have ceased to exist. Further, assuming that an injunction against the *use* of information could be justified, we can conceive of no possible justification for an injunction against the *disclosure* of information if the information were already public knowledge.

This case is distinguishable from *Underwater Storage*, *Inc. v. United States Rubber Co*. (D.C. Cir. 1966) 371 F.2d 950, 955 (*Underwater Storage*), which DVD CCA cites for the proposition that "a misappropriator or his privies can[not] 'baptize' their

wrongful actions by general publication of the secret." In *Underwater Storage* the defendant had misappropriated trade secrets and used them to develop a storage system for the United States Navy. After completing its work for the Navy, the defendant later published the alleged trade secrets, presumably representing them as its own technical know-how. (*Id*. at p. 952.) In resolving a statue of limitations question, the appellate court rejected the contention that the subsequent publication of the secret prevented the plaintiff from seeking compensation from the original misappropriator. The court stated: "Once the secret is out, the rest of the world may well have a right to copy it at will; but this should not protect the misappropriator or his privies." (*Id*. at p. 955.) *Underwater Storage* was not concerned with the issuance of a preliminary injunction. The information was concededly public when the case was filed. The court's holding was that under the circumstances the defendant could still be liable in damages for his previous misappropriation. That holding does not alter the conclusion that a preliminary injunction cannot be used to protect a secret if there is no secret left to protect.

One of the analytical difficulties with this case is that it does not fit neatly into classic business or commercial law concepts. The typical defendant in a trade secret case is a competitor who has misappropriated the plaintiff's business secret for profit in a business venture. In that scenario, the defendant has as much interest as the plaintiff has in keeping the secret away from good faith competitors and out of the public domain. But here, according to DVD CCA it has no good faith competitors. And the alleged misappropriators not only wanted the information for themselves, they also wanted the whole world to have it.

We concur with the concerns expressed by Judge Whyte in his opinion in *Religious Technology Center v. Netcom On-Line Com*., *supra*, 923 F.Supp at page 1256: "The court is troubled by the notion that any Internet user, . . . can destroy valuable intellectual property rights by posting them over the Internet, especially given the fact that there is little opportunity to screen postings before they are made. [Citation.]

Nonetheless, one of the Internet's virtues, that it gives even the poorest individuals the power to publish to millions of readers, [citation], can also be a detriment to the value of intellectual property rights. The anonymous (or judgment proof) defendant can permanently destroy valuable trade secrets, leaving no one to hold liable for the misappropriation." (Fn. omitted.)

There is little question that such behavior is unethical and that it probably violates other laws. But that which is in the public domain cannot be removed by action of the states under the guise of trade secret protection. (*Kewanee Oil Co. v. Bicron Corp.*, *supra*, 416 U.S. at p. 481.)

The evidence in the present case is undisputed that by the time this lawsuit was filed hundreds of Web sites had posted the program, enabling untold numbers of persons to download it and to use it. The only inference that can be drawn from this evidence is that by December 27, 1999 when DVD CCA first took legal action to stop publication of DeCSS, the technology had become available to those persons most interested in obtaining it. DVD CCA presented no evidence that the disclosure it sought to prohibit would cause more or different harm than that it claims it would have suffered by the general disclosure of the program. Accordingly, the record does not support the trial court's finding that the balance of harms favored DVD CCA.

## III. CONCLUSION

We conclude that evidence in the limited record before us does not justify the issuance of an injunction under the UTSA. DVD CCA presented no evidence as to when Bunner first posted DeCSS and no evidence to support the inference that the CSS technology was still a secret when he did so. Further, there is a great deal of evidence to show that by the time DVD CCA sought the preliminary injunction prohibiting disclosure of the DeCSS program, DeCSS had been so widely distributed that the CSS technology may have lost its trade secret status. There is no evidence at all to the contrary. Thus, DVD CCA has not shown a likelihood of success on the merits; nor has it demonstrated

that it would suffer further harm if the preliminary injunction did not issue.[8] The preliminary injunction, therefore, burdens more speech than necessary to protect DVD CCA's property interest and was an unlawful prior restraint upon Bunner's right to free speech. (*DVD*, *supra*, 31 Cal.4th at p. 881; and see *Madsen v. Women's Health Center, Inc.* (1994) 512 U.S. 753, 765.) It follows that issuance of the injunction was an abuse of the trial court's discretion.

It is important to stress that our conclusion is based upon the appellate record filed in this court. It is *not* a final adjudication on the merits. The ultimate determination of trade secret status and misappropriation would be subject to proof to be presented at trial. (*Whyte v. Schlage Lock Co*., *supra*, 101 Cal.App.4th at p. 1453.)

## IV. DISPOSITION

The order granting a preliminary injunction is reversed. Defendant Andrew Bunner shall recover his appellate costs.

Premo, Acting P.J.

WE CONCUR:

Elia, J.

Mihara, J.

[8] Because we find the injunction insupportable for the reasons stated, we do not reach Bunner's argument that the injunction would violate the intellectual property clause of the United States Constitution. (U.S. Const., art. I, § 8.)

| | |
|---|---|
| Trial Court: | Santa Clara County Superior Court<br>Superior Court No. CV 786804 |
| Trial Judge: | Hon. William J. Elfving |
| Attorneys for Plaintiffs-Respondents: | Weil, Gotshal & Manges, Redwood Shores, Jared B. Bobrow, Christopher J. Cox, Kimberly A. Schmitt, Robert G. Sugarman, Gregory S. Coleman, Beth L. Lemberger, New York |
| Attorneys for Defendant-Appellant: | Richard R. Wiebe, San Francisco;<br><br>Hopkins & Carley, Arthur V. Plank, Allonn E. Levy, San Jose;<br><br>First Amendment Project, Oakland, James R. Wheaton, David A. Greene;<br><br>Tomlinson Zisko Morosoli & Maser, Thomas E. Moore III, Palo Alto;<br><br>Electronic Frontier Foundation, San Francisco, Cindy A. Cohn |