IN THE SUPREME COURT OF THE STATE OF CALIFORNIA

DVD COPY CONTROL ASSOCIATION, INC., Plaintiff/Respondent, v. **ANDREW BUNNER,** Defendant/Appellant.	S102588

Sixth Appellate District, No. H021153
Santa Clara County Superior Court No. CV 786804
The Honorable William J. Elfving, Judge

BRIEF OF ATTORNEY GENERAL BILL LOCKYER AS AMICUS CURIAE IN SUPPORT OF RESPONDENT

BILL LOCKYER
Attorney General of the State of California

MANUEL M. MEDEIROS
State Solicitor

RICHARD M. FRANK
Chief Assistant Attorney General

LOUIS VERDUGO, JR.
Senior Assistant Attorney General

CATHERINE Z. YSRAEL
Supervising Deputy Attorney General

REGINA J. BROWN
EMILIO E. VARANINI IV
Deputy Attorneys General

300 South Spring Street
Los Angeles, CA 90013
Telephone: (213) 897-6505
Fax: (213) 897-2801

TABLE OF AUTHORITIES

Cases

	Page
A&M v. Napster (9th Cir. 2002) 284 F.3d 1091	2, 35
Ashcroft v. ACLU (May 13, 2002) 535 U.S. ____ [122 S.Ct. 1700]	2, 6, 28
Bartnicki v. Vopper (2001) 532 U.S. 514	20
Brookfield Communications, Inc. v. West Coast Entertainment Corp. (9th Cir. 1999) 174 F.3d 1036	24
Brooktree Corp. v. Advanced Micro Devices (Fed. Cir. 1992) 977 F.2d 1555	17
Comedy III Publications v. Saderup (2001) 25 Cal.4th 387	28
DVDCCA v. McLaughlin (Cal. Superior Ct. Jan. 21, 2000) [2000 WL 48512]	6, 36, 37
Gabrielli v. Knickerbocker (1938) 12 Cal.2d 85	30
Gerawan Farming, Inc. v. Lyons (2000) 24 Cal.4th 468	30
Horwich v. Superior Court (1999) 21 Cal.4th 272	14, 16
Integral Development Corp. v. Weissenbach (2002) 99 Cal.App.4th 576, [122 Cal.Rptr.2d 24]	19, 33

TABLE OF AUTHORITIES (continued)

TABLE OF AUTHORITIES (continued)

	Page
Rockwell Graphic Systems, Inc. v. DEV Industries, Inc. (7th Cir. 1991) 925 F.2d 174	8
Sable v. FCC (1989) 492 U.S. 115	20
Sega Enterprises, Ltd. v. Accolade, Inc. (9th Cir. 1992) 977 F.2d 1510	11, 17
Softman Products Company, LLC v. Adobe Systems, Inc. (C.D. Cal. 2001) 171 F.Supp.2d 1075	10, 12
Sony Computer Entertainment, Inc. v. Connectix Corp. (9th Cir. 2000) 203 F.3d 596	4, 11, 22, 23
Turner Broadcasting Systems v. FCC (1994) 512 U.S. 622	20, 32
Turner Broadcasting Systems v. FCC (1997) 520 U.S. 180	28
United States v. Elcom (N.D. Cal. 2002) 203 F.Supp.2d 1111	23, 25, 34
United States v. Microsoft Corp. (D.C. Cir. 2001) (*en banc*) 253 F.3d 34	18
United States v. O'Brien (1968) 391 U.S. 367	25
United States v. Playboy Entertainment (2000) 529 U.S. 803	25, 27
Universal City Studios v. Corley (2nd Cir. 2001) 273 F.3d 429	5, 6, 22-25, 29, 37

TABLE OF AUTHORITIES (continued)

Page

Court Rules

California Rules of Court
Rule 29(c) 2

Other Authorities

14 Uniform Laws Ann., Civ. Procedural and Remedial Laws
(1990) Uniform Trade Secrets Act With 1985 Amendments, Prefatory Note 15

Band, *Closing The Interoperability Gap: NCCUSL's Adoption Of A Reverse Engineering Exception In UCITA*
(May 2002) 19 No. 5 Computer & Internet Law 1 9

European Union Council Directive 91/250 on the Legal Protection of Computer Programs, arts. 6(a), 6(2) 1991 O.J. L.122 at 42 17

Expanding Variety of Players And Software Fuel Momentum Of DVD Sales In First Quarter 2002
(Apr. 30, 2002)
<http://www.dvdinformation.com/news/index.html > <as of June 24, 2002>
36

First Quarter DVD Rental Revenue Surpasses Entire Year 2000
(April 24, 2002)
<http://www.medianews.com/issues/2002/april/news0424_7.shtml > <as of June 26, 2002> 36

Good, *Trade Secrets And The New Realities of the Internet Age*
(1998) 2 Marquette Intellectual Prop. L. Rev. 51 7

Goodlate, *Stealing Entertainment: The Fiscal And Ethical Price Of Piracy Online*, The Washington Times
(May 27, 2002, Final Edition) at A21 36

TABLE OF AUTHORITIES (continued)

IN THE SUPREME COURT OF THE STATE OF CALIFORNIA

DVD COPY CONTROL ASSOCIATION, INC.,

Plaintiff/Respondent,

S102588

v.

ANDREW BUNNER,

Defendant/Appellant.

INTEREST OF THE ATTORNEY GENERAL

The Attorney General is charged by the Constitution with the duty to see that the laws of the State are uniformly and adequately enforced (Cal. Const., art. V, § 13), and therefore has a significant interest in participating as amicus curiae in this case. California is the center of the movie and entertainment industry, and the computer industry similarly has an authoritative presence in this State. (See generally *Nam Tai Electronics, Inc. v. Titzer* (2001) 93 Cal.App.4th 1301, 1313-1314.) On behalf of the State of California, the Attorney General seeks to ensure that the movie, entertainment, and computer industries can continue to depend upon the appropriate protection of their trade secrets under the Uniform Trade Secrets Act ("UTSA") when faced with a free speech challenge. (See *Kewanee Oil Company v. Bicron Corp.* (1974) 416 U.S. 470, 481-482 ["The maintenance of standards of commercial ethics and the encouragement of invention are the broadly stated policies behind trade secret law"].)

The Attorney General recognizes that the Internet "provides relatively unlimited, low-cost capacity for communication of all kinds." (*Reno v. ACLU* (1997) 521 U.S. 844, 870.) Because of "the dramatic expansion of this new marketplace of ideas" for California's citizens (*id.* at 885), the Attorney General has a keen interest in ensuring that the use of this cybermedium to promote First Amendment and Liberty of Speech values not be unduly chilled. Nevertheless, that free-speech claim cannot be used to facilitate the wholesale piracy of DVDs via the Internet, in defiance of federal and state intellectual property law. (Compare, e.g., *A&M v. Napster* (9th Cir. 2002) 284 F.3d 1091 [discussing the wholesale piracy of music from compact discs in defiance of federal copyright law via use of the Internet].) In this vein, the Internet cannot serve as a safe harbor where people can escape criminal or civil liability for conduct which would violate federal or state law in the physical world. (See *Ashcroft v. ACLU* (May 13, 2002) 535 U.S. ____, ___ [122 S.Ct. 1700, 1712].)

In the hope of assisting the Court to find the proper balance, the Attorney General respectfully offers this brief amicus curiae under Rule 29(c) of the California Rules of Court.

INTRODUCTION AND SUMMARY OF ARGUMENT

There is perhaps no more cherished principle in American jurisprudence than the right of persons to speak freely, without fear of censorship. This principle has been reaffirmed countless times since the founding of our Nation. However, the First Amendment should not be a shield for the blatant piracy and theft of trade secrets and digital content.

This Court has been asked to apply the free speech principles embodied in the California and United States Constitutions to a new medium, one which the Framers never contemplated. This medium is computer code, containing both functional and expressive elements. Within the code itself are trade secrets, obtained through improper means by a third party and disseminated by Defendant Andrew Bunner ("Bunner") on the Internet, with full knowledge that the trade secrets were improperly obtained.

Bunner and the Court of Appeal below characterize this medium as "pure speech," subject to the strictest scrutiny. As a result, the Court of Appeal deemed the lower court's injunction prohibiting Bunner from posting this computer code on his website to be an impermissible prior restraint on speech.

This characterization, however, ignores the "non-speech" elements of the code. It further ignores the fact that the statute authorizing the injunction is content-neutral, and involves the protection of Plaintiff DVD Copy Control Association's ("DVDCCA") property rights in its trade secrets.

The Attorney General presents four arguments in this brief as amicus. First, the Attorney General will argue that Bunner's posting of the computer code at issue on the Internet violated the UTSA. Bunner's wrongful acts in publishing the code on the Internet did not strip the code of its trade secret status. In this regard, the Attorney General will argue that, whereas reverse engineering towards a legitimate end, such as achieving software interoperability or creating a new product, is lawful and protected under the UTSA, reverse engineering towards an illegitimate end, such as the creation of a de-encryption program to facilitate content piracy, is not.[1/]

[1] Generally speaking, reverse engineering is the process by which one starts with a known product, and uses applied scientific or industrial know-how to work backwards in order to divine the process by which that product was developed or manufactured. (See *Kewanee Oil, supra*, 416 U.S. at p. 476; Samuelson & Scotchner, *The Law and Economics of Reverse Engineering* (May 2002) 111 Yale L.J. 1575, 1577, fn. 1.) Reverse engineering of a software program to capture or recreate its functional components occurs in one of several ways: (1) by reading about the programs in manuals; (2) by externally observing the visual expression of the program as it operates on a computer; and (3) by performing examinations of the computer instructions contained in a

Second, the Attorney General will argue that this Court should apply an intermediate-scrutiny standard in analyzing the injunction at issue under the First Amendment and California's Liberty-of-Speech Clause. Under this standard, the injunction issued below survives constitutional muster because it burdens "no more speech than necessary to serve a significant government interest." (*Madsen v. Women's Health Center, Inc.* (1994) 512 U.S. 753, 765-766.)

Third, the Attorney General will argue that, in applying *Madsen*'s call for a "precision of regulation" in evaluating content-neutral injunctions, this Court should first carefully consider whether the injunction impacts the expressive features of the computer code at issue any more than is necessary to serve the interests asserted. As each computer program has differing expressive and functional features, and as the instantaneous, worldwide dissemination of that program by means of the Internet amplifies the impact of those expressive and functional features, the courts should carefully assess the fit between the proposed injunction and the interests it serves in each case involving computer code. Similarly, in applying *Madsen*'s "precision of regulation" standard, the Court should also look to whether reasonable practical technological alternatives exist that would protect the trade secret at issue, without requiring an injunction against speech elements of the code. However, in doing so, it should place the burden of demonstrating that such alternatives exist on the defendant, not on the plaintiff.

Finally, the Attorney General will argue that, when this intermediate-

program. This latter alternative involves copying the program in question into a computer and then decompiling or transforming the program's object code back into source code. (See, e.g., *Sony Computer Entertainment, Inc. v. Connectix Corp.* (9th Cir. 2000) 203 F.3d 596, 599-600 (*Connectix*); *The Law and Economics of Reverse Engineering, supra,* 111 Yale L.J. at pp. 1608-1609.)

scrutiny standard is applied, the injunction at issue here burdens "no more speech than necessary to serve a significant government interest." That injunction was narrowly tailored to prevent only the destruction (via dissemination) of the trade secrets contained in the computer code to serve the significant, if not compelling, governmental interest in protecting trade secrets and combating piracy. The trial court did *not* prohibit Bunner from voicing his thoughts regarding the computer code, writing and posting articles about the code, or even posting weblinks on his website that might lead readers to sites where the computer code is posted. [2]

ARGUMENT
I.
THE TRIAL COURT PROPERLY ENJOINED BUNNER'S DISSEMINATION OF DVDCCA'S TRADE SECRETS

In order to establish a violation of the UTSA, one must demonstrate (1) the existence of a trade secret, that (2) was "misappropriated" and (3) disseminated with actual or constructive knowledge of this misappropriation. (Civ. Code, §§ 3426.1, 3426.2.)

DeCSS, the decryption program at issue here, contains within it CSS source code and object code owned by DVDCCA, including a proprietary CSS encryption algorithm and master key. (See, e.g., DVDCCA's Opening Brief, pp. 6-7; Bunner's Answer Brief, pp. 5-6; DVDCCA's Reply Brief, pp. 12-13; AA 00479-00481; see also *Universal City Studios v. Reimerdes* (S.D.N.Y. 2000) 111 F.Supp.2d 294, 309-311, affd. *sub. nom. Universal City Studios v. Corley*

[2] Although he does not brief this issue, the Attorney General concurs with DVDCCA's argument that the injunction did not constitute a prior restraint on pure speech. As is discussed below, the computer code at issue is not pure speech, and both the statute and injunction at issue are content-neutral.

(2nd Cir. 2001) 273 F.3d 429.[3])

Bunner contends that the trade secrets contained in DeCSS, the CSS encryption algorithm and master key, no longer retain their trade status because DeCSS has been disseminated over the Internet. (Bunner's Answer Brief, pp. 38-41.) Bunner further contends that, because the original misappropriation of those trade secrets occurred by means of reverse engineering, those trade secrets were not acquired by improper means as required for violation of the UTSA. (Bunner's Answer Brief, pp. 31, 38, 41-42.) Each of these arguments fails.

A. Notwithstanding The Dissemination Of DeCSS On The Internet, The CSS Computer Code Contained In DeCSS Was And Remains A Trade Secret.

The superior court properly held in this case that trade-secret status should not be "deemed destroyed at this stage merely by the posting of the trade secret to the Internet," or else those who misappropriate trade secrets would be encouraged to "post the fruits of their wrongdoing on the Internet as quickly as possible thereby destroying a trade secret forever." (AA 00715; *DVDCCA v. McLaughlin* (Cal. Superior Ct. Jan. 21, 2000) [2000 WL 48512, *3].[4]) Indeed, the United States Supreme Court recently noted that one who seeks to post obscene speech on the Internet should not escape liability merely because he deliberately chose a medium which allowed for the instantaneous, nationwide dissemination of that speech. (See *Ashcroft, supra*, 535 U.S. at p. ____ [122 S.Ct. at p. 1712] (lead opn. of Thomas, J.).)

If posting a trade secret on the Internet automatically defeated the trade secret itself and automatically nullified any hope of an injunction, then trade

[3] This brief will extensively cite both of these Second Circuit opinions. The district court opinion will be referred to as *Reimerdes* and the Court of Appeal's opinion will be referred to as *Corley*.

[4] This citation is to the unpublished lower court opinion in this case.

secrets law, which is at least 150 years old in the United States, see, e.g., *Kewanee Oil, supra*, 416 U.S. at p. 493, would be in jeopardy in the multitude of state and national jurisdictions which have such laws. Along these lines, one court proclaimed itself "troubled by the notion that any Internet user, including those using 'anonymous remailers' [footnote omitted] to protect their identity, can destroy valuable intellectual property rights by posting them over the Internet, especially given the fact that there is little opportunity to screen such postings before they are made." (*Religious Technology Center v. Netcom Online Communication Services, Inc.* (N.D. Cal. 1995) 923 F.Supp. 1231, 1255 (*Netcom*); accord, *Reimerdes, supra*, 111 F.Supp.2d at p. 344.) That same court further noted that one who posts misappropriated trade secrets on the Internet should not, in equity, be permitted to rely on his *own* posting of the trade secret, or on the posting of the trade secret by the misappropriator or his privies, to argue that the trade secret had been destroyed. (*Netcom, supra,* at pp. 1256-1257; accord, *Reimerdes, supra*, 111 F.Supp.2d at pp. 345-346.)

The Attorney General agrees. For reasons including the need to avoid unduly chilling use of the Internet to access information, the *Netcom* court also concluded that a subsequent publisher of misappropriated trade secrets could rely on the *independent* postings of some of those trade secrets by *third parties* on the Internet as a basis for arguing that their trade-secret status had been destroyed. (*Netcom, supra*, 923 F.Supp. at p. 1256.)

But the Attorney General would caution that a trade secret's status is not destroyed merely because it has made an appearance on the Internet due to the posting efforts of independent third parties. Rather, courts should apply a multi-factor test to determine whether the dissemination of a trade secret on the Internet by independent third parties has fairly destroyed its status. Such factors include consideration of the means by which the trade secret was disseminated over the Internet, the nature of the trade secret itself, the time during which the secret has been exposed, and the nature and scope of the efforts made by the owner of the trade secret to remove it from the public domain. (See, e.g., Good, *Trade Secrets And The New Realities of the Internet Age* (1998) 2 Marquette Intellectual Prop. L. Rev. 51, 99-103 & fn. 264 [citing and discussing cases].)[5]

In this case, the record appears to contain (1) evidence of DVDCCA's widespread efforts to contact web sites nationwide and request they cease posting DeCSS (See, e.g., AA 00344-00347); (2) evidence that there was widespread awareness on the Internet in November of 1999 that the posting of DeCSS had become illegal, and that plaintiffs were now contacting web sites to request that they remove DeCSS (AA00348-00354); (3) testimony from Bunner's own expert that CSS' encryption algorithm or master key could not be discovered by independent efforts aside from a review of DeCSS code (AA00484-00486); and (4) the absence of any indication that the actual trade secrets contained in DeCSS, the proprietary CSS encryption algorithm or master key, had been widely disseminated or become widely known among the public. (See DVDCCA's Reply Brief, pp. 12-13 & fn. 7.) If that is the case, then it is the Attorney General's view that CSS' trade-secret status was not destroyed by Bunner's publication of DeCSS on the Internet.

B. CSS' Code Was Acquired Through Improper Means Because The Reverse Engineering at Issue Fell Outside The Scope Of The UTSA's Reverse Engineering Exemption.

It is not enough under the UTSA to prove that the misappropriated code

[5] See also *Reimerdes, supra*, 111 F.Supp.2d at pp. 344-345; cf. *Rockwell Graphic Systems, Inc. v. DEV Industries, Inc.* (7th Cir. 1991) 925 F.2d 174, 179 (Posner, J.) [finding applicable in the trade-secrets context the notion that a trademark is protectable where its holder has made reasonable efforts to police infringement of the mark]; *Netcom, supra*, 923 F.Supp. at p. 1255 [brief public disclosure of trade secrets does not destroy their status in absence of evidence that they have become generally known].)

constituted a trade secret. It must also be shown that the trade secret was misappropriated or acquired through improper means. The Attorney General believes that this showing has been made here.

As is discussed more fully elsewhere,[6] DeCSS was created by a Norwegian hacker who reverse engineered CSS' encryption algorithm and master key from a licensed version provided by DVDCCA to Xing. (See, e.g., AA00349-00350, 00354-00364, 00479-00480, 00484-00485.) Xing's end-user agreement ("EULA") is a "click-on license" agreement[7] which appears while installing Xing's DVD player, and states "[t]he Product in source code form is confidential, and Xing's protected trade secret, and you may not attempt to reverse engineer, decompile, disassemble, or otherwise decipher any portion of the Product."[8] (AA00339-00343.) By reverse engineering CSS, the Norwegian hacker therefore violated the EULA.

Under the UTSA, "[m]isappropriation" is defined in pertinent part as "the 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." (Civ. Code, § 3426.1, subd. (b)(1).) In turn, the term "improper means" is defined as

[6] For a discussion regarding the creation of DeCSS, see, e.g., DVDCCA's Opening Brief, pp. 5 - 6; *Reimerdes, supra*, 111 F.Supp.2d at pp. 311-312.

[7] "A click-on license appears when a user is installing a program on his or her computer. The user must click on an 'I agree' icon in order to complete the installation sequence." (Band, *Closing The Interoperability Gap: NCCUSL's Adoption Of A Reverse Engineering Exception In UCITA* (May 2002) 19 No. 5 Computer & Internet Law 1, 2, fn. 22.)

[8] Licensees such as Xing also executed license agreements with DVDCCA, agreeing that they "shall under no circumstances reverse engineer, decompile, disassemble or otherwise determine the operation of CSS Specifications, including without limitation, any encryption/decryption or scrambling/descrambling algorithm." (AA00490.)

including:

> 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.*

(Civ. Code, § 3426.1, subd. (a) (italics added).)

From the face of the statute, it may appear that the Norwegian hacker's conduct is exempted from the UTSA's prohibition. However, as will be seen, the Attorney General will argue that, under applicable canons of statutory construction, the UTSA's reverse engineering exemption should not be read to shield reverse engineering that is directed towards an unlawful purpose or end. Here, the Norwegian hacker reversed engineered DVDCCA's trade secrets, its proprietary encryption algorithm and master key, in order to create a decryption program whose sole use is to bypass the encryption program on DVDs and pirate their digital content. This is reverse engineering directed towards an unlawful purpose and should not be protected under the UTSA.[9]

Finally, Bunner's attempt to invoke Norwegian law, rather than the UTSA, fails because California law applies in determining whether a trade secret was misappropriated.

[9] The question whether an EULA may be enforceable for all purposes, or against "lawful" or traditional uses of reverse engineering of the types discussed *post*, is not presented by this case, and should be decided, if at all, in the appropriate factual context in a future case. A click license agreement would raise serious legal concerns if, for example, it were argued that it allows businesses to avoid general consumer laws, alters existing state standards for finding a contract to be unconscionable, or narrows the duties of businesses on implied and express warranties. Similarly, the Attorney General does not adopt the position that click-license agreements should be treated as licenses rather than as contracts for the sale of a good. (See, e.g., *Softman Products Company, LLC v. Adobe Systems, Inc.* (C.D. Cal. 2001) 171 F.Supp.2d 1075, 1085.)

1. *The Reverse Engineering In This Case Did Not Serve The Legitimate Or Pro-Competitive Ends Typical Of Reverse Engineering.*

Reverse engineering of a software program is conducted legitimately within the software industry for three reasons. First, a program may be reverse engineered by a user or competitor so that it may "interoperate" with other software. Second, a program may be reverse engineered by a competitor so that it may devise its own viable program in order to compete directly or to compete in a different, overlooked market. Finally, a program may be reverse engineered by a user to avoid or fix problems, pitfalls, and defects in it as explanations in manuals and other documentation may be inadequate.[10]

By its very nature, it is apparent that DeCSS was not the product of the type of legitimate reverse engineering discussed above. Although Bunner claims that DeCSS was designed by the Norwegian hacker (and later posted by

[10] See, e.g., *Connectix*, *supra*, 203 F.3d at p. 599 ["[s]oftware engineers designing a product that must be compatible with a copyrighted product frequently must 'reverse engineer' the copyrighted product to gain access to the functional elements of the copyrighted product."]; *id.* at 601-608 [Connectix lawfully reverse engineered Sony's Playstation so that it could develop emulation software to allow Playstation games to be played on a personal computer ("PC")]; *Sega Enterprises, Ltd. v. Accolade, Inc.* (9th Cir. 1992) 977 F.2d 1510, 1527-1528 [reverse engineering lawful notwithstanding copyright law to achieve interoperability between Accolade games and the Sega game console]; *Reimerdes*, *supra*, 111 F.Supp.2d at pp. 319-320 [Digital Millennium Copyright Act exception allows reverse engineering, including the circumvention of access control technologies, in order to achieve interoperability of an independently created program with other programs]; *The Law And Economics Of Reverse Engineering, supra,* 111 Yale L.J. at pp. 1582, 1614-1615, 1642 & fns. 23, 24, 182; *Closing The Interoperability Gap, supra*, at 3-5; Hsia, *Intellectual Property And Technology Law In The Internet Age* (Nov. 2001) 5 NOV Hawaii B.J. 4, 6 [personal computer revolution occurred because of the legality of reverse engineering]; Johnson-Laird, *Software Reverse Engineering In The Real World* (1994) 19 U. Dayton L. Rev. 843, 848-854.

him) so that users of computers with a Linux operating system could watch DVDs, in fact DeCSS was originally designed to play only on the more widespread and popular Windows operating system. And, currently, DeCSS allows a user to decrypt, copy, and save DVD movies on a computer with either a Windows or a Linux operating environment. (See e.g., *Reimerdes, supra*, 111 F.Supp.2d at pp. 311, 315, 318-320; AA00157, AA00225, AA00480.)[11]

Plainly, DeCSS is not an encryption system for DVDs that allows users to play DVDs solely on computers with a Linux operating system while denying those users the ability to freely copy and disseminate the DVD's digital files. This is an important point in assessing Bunner's contention that DeCSS represents a use of reverse engineering to achieve interoperability: DeCSS was not needed for a computer with a Windows operating environment since CSS could *already* function within a Windows operating environment. (See, e.g., *Reimerdes, supra*, 111 F.Supp.2d at pp. 308-310, AA0067-0072, 00263, 00488.)

Nor is DeCSS the end product of other types of reverse engineering discussed above. It is not a "patch" designed to fix a problem, pitfall, or defect in CSS' encryption algorithm or master key. Nor is it a newer, stronger encryption algorithm and master key for DVDs designed to replace CSS. (Compare, e.g., *The Law And Economics Of Reverse Engineering, supra,* 111 Yale L.J. at pp. 1582, 1614-1615, 1642 & fns. 23, 24, 182; *Software Reverse Engineering In The Real World*, *supra,* 19 U. Dayton L. Rev. at pp. 848-854 with *Reimerdes, supra*, 111 F.Supp.2d at pp. 311, 315, 318-320; AA00157, AA00225, AA00480.)

Indeed, the conduct surrounding DeCSS and its dissemination supports the conclusion that DeCSS was not an act of lawful or legitimate reverse

[11] For a helpful discussion on the nature of the Microsoft Windows, and the open source Linux, operating systems, see *Reimerdes*, *supra*, 111 F.Supp.2d at p. 305.

engineering. First, DeCSS was posted on the Internet and freely disseminated to the public. (See, e.g., *Reimerdes, supra,* 111 F.Supp.2d at pp. 311, 320.) Furthermore, it was posted in a form which made it fully executable by any member of the public; if the creator of DeCSS (or subsequent disseminators of DeCSS such as Bunner) were interested in only notifying the public, or the cryptographer community, of his ability to reverse engineer DeCSS, he could have published some abbreviated, non-executable summary of the DeCSS code. Or, DeCSS' creator could have, but did not, simply publish academic findings in lieu of posting DeCSS itself, i.e., in a reputed scientific journal on cryptography, discussing those defects he was able to observe in CSS as a consequence of his reverse engineering efforts so that DVDCCA could correct such defects in the future. In fact, DeCSS' creator, prior to its public dissemination, neither informed DVDCCA of its creation nor otherwise sought a license allowing him (or others) to use CSS in a Linux operating environment so that he (or others) could view DVDs. (See, e.g., *Reimerdes, supra*, 111 F.Supp.2d at p. 311; AA00488.) Alternatively, DeCSS' creator (or subsequent disseminators, such as Bunner) could have, but did not, ask DVDCCA to find a company willing to design and release a DVD player playable on a Linux operating system with CSS.[12]

The Attorney General submits that such reverse engineering for an improper purpose falls outside the UTSA's exemption.

[12] Two companies now plan to release DVD players for computers with a Linux operating system. (*Reimerdes, supra*, at p. 310 & fn. 64.) Moreover, DVDCCA has presented evidence that a request for such a license would have been granted. (See AA00488.)

2. *Neither An Examination Of The Plain Language Nor The Legislative History Of The UTSA Conclusively Resolve The Scope Of The UTSA's Reverse Engineering Exemption.*

The UTSA itself does not provide a statutory definition of the term "reverse engineering." (See Civ. Code, § 3426.1, subd. (a).) The term "reverse engineering" does have a literal or technical construction, namely the process by which one starts with a known product, and uses applied scientific or industrial know-how to work backwards in order to divine the process by which that product was developed or manufactured. (See, e.g., *Kewanee Oil, supra*, 416 U.S. 470, 476.)

But relying on this literal and technical construction of the term "reverse engineering" to the UTSA would disserve the legislative purpose behind the UTSA. Indeed, the literal or technical definition of "reverse engineering" would arguably include "hacking," given that "hacking" has been defined generally as the penetration of computer systems to gain knowledge about those systems, about how they work, and about how to stretch their capabilities. (See, e.g., Reilly, *Cyber-Crimes: A Practical Approach To The Application Of Federal Computer Crime Laws* (May 2000) 16 Santa Clara Computer & High Tech. L.J. 177, 181-183, 185 & Appendix A ("*Cyber-Crimes*"); see also *The Law And Economics of Reverse Engineering, supra*, 111 Yale L.J. at p. 1577 & fn.1 [although *Kewanee Oil* provides the standard definition of reverse engineering, even broader formulations of this term have been used by various scholars and authorities].)

Where the statutory language is less than pellucid, this Court will look beyond this language to legislative intent or to the statutory scheme as a whole in divining the meaning of this term. (See, e.g., *Wilcox v. Birtwhistle* (1999) 21 Cal.4th 973, 977-978; *Horwich v. Superior Court* (1999) 21 Cal.4th 272, 276.)

Here, however, neither the legislative history surrounding the adoption of the UTSA by the California Legislature in 1984, nor the original drafting history of the UTSA itself, sheds any light on this subject. Equally, no decisions apparently exist anywhere in the 44 states governed by the UTSA which speak to this issue.

This is not surprising. When the UTSA was drafted in 1979,[13] it was not known that reverse engineering could be used to accomplish unlawful or market-destructive ends on a mass scale. Only with the subsequent rise of the computer and software industries after the UTSA was drafted did this development become evident. (See, e.g., *The Law And Economics of Reverse Engineering, supra,* 111 Yale L.J. at pp. 1598-1601 [the Semiconductor Chip Protection Act, which protects against unlawful reverse engineering of computer chips, was enacted by Congress in 1984 because of the development of chip piracy in the early 1980s]; *id.* at pp. 1634-1635 [developments in the mid-1990s led to the first proposals to restrict the dissemination of circumvention or decryption technology designed to pirate content]; see also *Cyber-Crimes, supra,*16 Santa Clara Computer & High Tech. L.J. at p. 185 [hacking on the rise in the late 1990s because of the increased availability of hacking tools].)[14]

[13] See 14 Uniform Laws Ann., Civ. Procedural and Remedial Laws (1990) Uniform Trade Secrets Act With 1985 Amendments, Prefatory Note at pp. 434-436.

[14] The California Senate Legislative Committee Comment to the Uniform Trade Secrets Act quotes *Kewanee Oil* for the proposition that "[o]ne of the broadly stated propositions behind trade secret law is "'the maintenance of standards of commercial ethics.'" (Senate Leg. Committee Comment (1984).) This reveals that the California Legislature was aware of *Kewanee Oil* at the time it enacted the UTSA. This is an important point as *Kewanee Oil,* which antedates the emergence of the software and computer industries in California, contains a discussion as to the beneficial or legitimate ends of reverse engineering. (See *Kewanee Oil, supra*, 416 U.S. at pp. 476, 490-492.)

Accordingly, the Court will have to look elsewhere for guidance in discerning the Legislature's intent.

3. *This Court May Look To Other Statutory Canons In Interpreting The UTSA's Reverse Engineering Exemption To Exclude Reverse Engineering For Unlawful Purposes Such As The Creation And Dissemination Of Decryption Software.*

First and foremost, this Court should consider "the object to be achieved [by the UTSA] and the evil to be prevented [by the reverse engineering exception]." (*Wilcox, supra*, 21 Cal.4th at p. 977; *Horwich, supra*, 21 Cal.4th at p. 276.) It should also consider the public policy to be served by the exemption. (*Wilcox*, *supra*, 21 Cal.4th at p. 977.)

As noted earlier, to give the term "reverse engineering" its technical or literal construction would effectively exempt reverse-engineering efforts intended to foster unlawful or illegitimate ends such as content piracy, and would thwart the very purpose behind the UTSA, namely the protection of intellectual property. (See Part III(A)(1), (2) *post.*) Statutory constructions which lead to absurd or anomalous results are to be avoided. (Cf. *People v. Cochran* (2002) 28 Cal.4th 396, ____ [121 Cal.Rptr.2d 595, 597, 601-602] [court looked to cases involving other statutes in eschewing the adoption of a literal or technical construction of the term "for commercial purposes" as used in Penal Code section 311.4, subdivision (b)].)

It is significant that, reflecting the 20-20 hindsight lacking among drafters of the UTSA, other federal and foreign statutes have carefully defined the circumstances under which a reverse engineering exception may be invoked so as to exclude reverse engineering efforts which are directed towards unlawful or market-destructive ends. For example, the Digital Copyright Millennium Act ("DMCA") allows reverse engineering only in order to achieve interoperability of an independently created program with other programs. (See, e.g., *Reimerdes, supra*, 111 F.Supp.2d at pp. 319-320; 17 U.S.C. § 1201, subd. (f).) The Semiconductor Chip Protection Act ("SPCA") allows the reverse engineering of a chip only to understand it or, following such reverse engineering, to develop a second "original" chip with a different design layout. (See, e.g., *Brooktree Corp. v. Advanced Micro Devices* (Fed. Cir. 1992) 977 F.2d 1555, 1565; 17 U.S.C. § 906; see also *The Law and Economics of Reverse Engineering, supra,* 111 Yale L.J. at pp. 1595-1602 [noting that witnesses distinguished between illegitimate and legitimate reverse engineering in discussing the SPCA at Congressional hearings].)

The Vessel Hull Protection Act (for a limited period of time) bars the reverse engineering of original boat design configurations in order to sell identical copies, apparently because of the perceived market-destructive effects arising from this type of reverse engineering. (See, e.g., *id.* at pp. 1593-1594 & fn. 84; 17 U.S.C. §§ 1302, 1303.) The European Union enacted a software directive creating a reverse engineering exemption only for the creation of interoperable programs; this exemption has been likened to the one fashioned by the Ninth Circuit in *Sega, supra*, 977 F.2d at pp. 1527-1528. (See, e.g., *The Law and Economics of Reverse Engineering, supra,* 111 Yale L.J. at p. 1612, fn. 178; *European Union Council Directive 91/250 on the Legal Protection of Computer Programs*, arts. 6(a), 6(2) 1991 O.J. L.122 at pp. 42, 45; *Report from the European Commission to the Council on the Implementation and Effects of Directive 91/250/EEC on the Legal Protection of Computer Programs* (April 10, 2000) at 6-8, 13-15, <http://www.europa.edu> <as of July 3, 2002>.)

Certain of these statutes, such as the DMCA and the SPCA, explicitly distinguish between lawful and unlawful reverse engineering. Significantly, however, none provides that the dissemination of circumvention software or technology should be protected if it results from the reverse engineering of encryption software and technology. Indeed, the DMCA specifically provides that circumvention technology that is based on the reverse engineering of encryption software may not be disseminated at all. (See, e.g., *Reimerdes*, *supra*, 111 F.Supp.2d at pp. 319-320.)

Furthermore, it is also significant that scholars operating with the benefit of 20-20 hindsight have also forcefully advocated that a distinction be drawn between legitimate and illegitimate reverse engineering. The authors of *The Law and Economics of Reverse Engineering* conclude that the dissemination of circumvention software should be prohibited, even if the software in question were the product of reverse engineering. (See *The Law And Economics Of Reverse Engineering, supra*, 111 Yale L.J. at p. 1641.)

Construing "reverse engineering" under the UTSA in accordance with the distinction drawn by other statutes and commentators, this Court should interpret the exemption to exclude reverse engineering directed towards an illegitimate end, such as the reverse engineering of encryption software to create decryption software. As noted, that interpretation would further California's strong public policy interests in protecting trade secrets and combating piracy insofar as it exempts encryption software from the UTSA's reverse engineering exception. (See Part III (A)(1), (2), *post.*)

Finally, it truly would lead to an anomalous or absurd result if, by the incorporation of a literal interpretation of the term "reverse engineering," the UTSA now stood alone among intellectual property laws worldwide in granting an absolute and unfettered right to individuals to reverse engineer encryption software and then disseminate decryption software. "That is no more correct than the proposition that use of one's personal property, such as a baseball bat, cannot give rise to tort liability." (*United States v. Microsoft Corp.* (D.C. Cir. 2001) (*en banc*) 253 F.3d 34, 63 [discussing Microsoft's claim that it has an absolute and unfettered right to use intellectual property as it wishes].)

As UTSA's reverse engineering exception does not operate here to shield the creation and dissemination of DeCSS (which includes CSS code safeguarded by DVDCCA as trade secrets), the Xing click-license agreement barring the reverse engineering and disclosure of CSS' computer code in this case creates an enforceable duty for trade secret purposes. The Norwegian hacker's violation of that duty was a misappropriation of trade secrets by improper means.

4. *California Law Ultimately Controls Here In Determining Whether A Trade Secret Has Been Misappropriated.*

As noted, Bunner alleges there is insufficient evidence that the reverse engineering in question violated Norwegian law. (See Bunner's Answer Brief, pp. 41-42.) However, California's UTSA, not foreign law, ultimately governs in determining whether there has been a misappropriation of trade secrets. (*Magnecomp v. Athene Co., Ltd.* (1989) 209 Cal.App.3d 526, 539-540 [contrasting California's strong interest in prosecuting the misappropriation of trade secrets with the lack of any strong interest on the part of the Japanese government in protecting the theft of those secrets]; see also *Integral Development Corp. v. Weissenbach* (2002) 99 Cal.App.4th 576, ___ [122 Cal.Rptr.2d 24, 36-37] [noting California's strong interest in enforcing the UTSA even where the misappropriation in question occurred in Germany and involved a German citizen].) Accordingly, California law (i.e., the UTSA), and not Norwegian law, is dispositive in determining whether trade secrets were obtained through improper means.

II.

THE INJUNCTION SHOULD BE REVIEWED PURSUANT TO AN INTERMEDIATE-SCRUTINY STANDARD

The Court of Appeal reversed the trial court's order, on the grounds that the injunction was a prior restraint on pure speech and thus violated the First Amendment of the United States Constitution. The Attorney General respectfully disagrees. In his view, the injunction prohibiting only the dissemination of computer code (specifically CSS and DeCSS), need be reviewed only under, and readily satisfies, an intermediate-scrutiny standard. As will be further explained, the intermediate-scrutiny standard is warranted because (1) the injunction and statute pursuant to which it issued are content-neutral, and (2) contrary to the views of the appellate court, the "speech" at is issue in computer code is not "pure speech."

On its face, the UTSA is "content-neutral," i.e., the statute draws no distinction between misappropriations of trade secrets, based on ideas or views expressed in the misappropriation. (See Civ. Code, §§ 3426.1, subds. (a), (b), 3426.2, subd. (a).) Content-neutral regulations that may implicate speech, such as the UTSA, are subject only to "intermediate scrutiny." (See *Turner Broadcasting Systems v. FCC* (1994) 512 U.S. 622, 662 (*Turner I*); *Ward v. Rock Against Racism* (1989) 491 U.S. 781, 789.) This is to be contrasted with "*content-based*" statutes, *i.e.,* statutes that facially distinguish between favored speech and disfavored speech, *Bartnicki v. Vopper* (2001) 532 U.S. 514, 526, which are permissible only if they serve a compelling state interest and be the least restrictive means of serving that interest. (See, e.g., *Sable v. FCC* (1989) 492 U.S. 115, 126.)

To be sure, the injunction at issue here was issued against a particular kind of expression. But, the enforcement of a content-neutral statute is not rendered "content-based," for purposes of free-speech analysis, merely because it happens that the statute is being enforced against a form of protected speech. To accept such reasoning "would be to classify virtually every injunction as content or viewpoint based." (*Madsen, supra*, 512 U.S. at p. 762 [ruling that an injunction issued pursuant to a content-neutral statute is not rendered content-based because it is enforced against abortion protestors].) Nevertheless, the high court has cautioned that, because injunctions "carry greater risks of censorship and discriminatory application than do general ordinances" (*id* at p. 765), an injunction regulating speech should be held to a "somewhat more stringent application of First Amendment principles" (*id.*) even if the injunction were issued pursuant to a content-neutral statute, although the injunction need not be subject to a strict scrutiny test. (*Id.* at pp. 766-767.) In *Madsen*, the Court upheld those portions of the injunction that "burden no more speech than necessary to eliminate the unlawful conduct targeted by the state court's injunction" (*id.*. at p. 777), because the injunction protected significant governmental interests (*id.* at pp. 767-768).

Here, the injunction restrained nothing more than Bunner's dissemination of DeCSS and CSS on the Internet. The injunction thus burdened no more of Bunner's speech than is necessary to eliminate the continued dissemination of a trade secret, thereby furthering the substantial governmental activity of fostering creativity and invention by protecting intellectual property against misappropriation.

But, the Attorney General submits that the *Madsen* intermediate-scrutiny standard is appropriate in this case, not only because the statute and injunction at issue are content-neutral, but also because the expression contained in the DeCSS computer code is incidental to its functional purpose of directly executing computer processes. As will be explained, computer code such as DeCSS is language that is both communicative, when read by a trained human being, and directly effective, when "read" by a computer, in executing certain functions. Any free-speech analysis of Bunner's claim of right to utter the "speech" aspect of DeCSS must also take into consideration the public interest in interdicting the *functional* aspect of DeCSS as a set of commands effecting the destruction of a trade secret.

"Computers . . . operate with a series of on and off switches, using two digits in the binary (base 2) number system -- 0 (for off) and 1 (for on). All data and instructions input to or contained in computers therefore must be reduced [to] the numbers 1 and 0." (*Reimerdes, supra,* 111 F.Supp.2d at pp. 305-306 & fns. 10, 11.) The strings of 0s and 1s which embody data or instructions, known as object code, can command computers to perform complex or simple tasks. (*Id.* at pp. 305-306 & fn. 16; accord, *Corley, supra*, 273 F.3d at pp. 438-439.) While some people can read and program in object code, it is "inconvenient, inefficient, and, for most people, probably impossible to do so." (*Reimerdes, supra*, 111 F.Supp.2d at p. 306; accord, *Corley, supra*, 273 F.3d at p. 439.)

As a result, computer programmers have developed programming languages. "These languages, like other written languages, employ symbols and syntax to convey meaning. The text of programs written in these languages is referred to as source code." *(Reimerdes, supra*, 111 F.Supp.2d at p. 306; accord, e.g., *Connectix, supra,* 203 F.3d at p. 600, fns. 3, 4; Johnson-Laird, *Software Reverse Engineering In The Real World* (1994) 19 U. Dayton L. Rev. 843, 856-857.) [15]

[15] However, "the distinction between source and object code is not as crystal clear as [it] first appears. Depending upon the programming language, source code may contain many 1's and 0's and look a lot like object code or may contain many instructions derived from spoken human language. Programming languages the source code for which approaches object code are referred to as low level source code while those that are more similar to spoken language are

Either directly or, more commonly through the medium of another program most often referred to as a compiler, computer instructions written in source code are translated into the machine readable strings of 1's and 0's known as object code. Object code is typically executable by the computer on a direct basis. (*Reimerdes, supra*, 111 F.Supp.2d at p. 306 & fn. 18; *Software Reverse Engineering In The Real World*, *supra,* 19 U. Dayton L. Rev. at pp. 858-860.)

Federal courts have consistently treated source and object code as having both expressive (nonfunctional) as well as functional features. (See, e.g., *Junger v. Daly* (6th Cir. 2000) 209 F.3d 481, 484-485.)[16] "Mathematical formulae and musical scores are written in 'code,' i.e., symbolic notations not comprehensible to the uninitiated, and yet both are covered by the First Amendment." *Corley, supra*, 273 F.3d at p. 445.) And, "programmers use snippets of code to convey their ideas for new programs; economists and other creators of computer models publish the code of their models in order to demonstrate the models' vigor." (*Id.* at p. 448, fn. 22.) But, "[i]n the digital age, more and more conduct occurs through the use of computers and over the Internet. Accordingly, more and more conduct occurs through 'speech' by way of messages typed onto a keyboard or implemented through the use of computer code when the object

---

referred to as high level source code." (*Reimerdes, supra*, 111 F.Supp.2d at p. 306; accord, *Corley, supra*, 273 F.3d at 439.) Source code can also contain commentaries or specifications consisting of "marginal annotations" by the programmer or software engineer designed to aid other programmers and software engineers to interpret, understand, and read the code. (See, e.g., *Connectix, supra,* 203 F.3d at p. 600; *Software Reverse Engineering In The Real World*, *supra,* 19 U. Dayton L. Rev. at p. 857.)

[16] See also *Connectix, supra,* 203 F.3d at pp. 599-600, 602; *Reimerdes, supra*, 111 F.Supp.2d at pp. 326-329; *United States v. Elcom* (N.D. Cal. 2002) 203 F.Supp.2d 1111, 1126. "[C]omputer code, whether source or object — is a means of expressing ideas, ..." (*Reimerdes, supra*, 111 F.Supp.2d at p. 327; accord, e.g., *Corley, supra*, 273 F.3d at pp. 445-448 & fns. 21, 22; *Elcom, supra*, 203 F.Supp.2d at pp. 1126-1127.

code commands computers to perform certain functions." (*United States v. Elcom* (N.D. Cal. 2002) 203 F.Supp.2d 1111, 1128; see *Corley, supra*, 273 F.3d at p. 451.)

Furthermore, and apropos the instant litigation, the potential impact of computer-code functionality is infinitely multiplied by virtue of the Internet.[17] "Using a Web browser, such as Netscape's Navigator or Microsoft's Internet Explorer, a cyber 'surfer' may navigate the Web - searching for, communicating with, and retrieving information from various web sites. [Citation.]" (*Brookfield, supra*, 174 F.3d at p. 1044.) As the Second Circuit Court of Appeals persuasively observed:

> Unlike a blueprint or a recipe, which cannot yield any functional result without human comprehension of its content, human decision-making, and human action, computer code can instantly cause a computer to accomplish tasks and instantly render the results of those tasks available throughout the world via the Internet. The only human action required to achieve these results can be as limited and instantaneous as the click of a mouse. These realities of what code is and what its normal functions are require a First Amendment analysis that treats code as combining nonspeech and speech elements.

(*Corley, supra,* 273 F.3d at p. 451, citing *Red Lion Broadcasting Co. v. FCC*

[17] "The Internet is a global network of interconnected computers which allows individuals and organizations around the world to communicate and share information with one another. The Web, a collection of information resources contained in documents located on individual computers around the world, is the most widely used and fastest-growing part of the Internet except perhaps for electronic mail ("e-mail"). [Citation.] With the Web becoming an important mechanism for commerce, [citation], companies are racing to stake out their place in cyberspace. Prevalent on the Web are multimedia "web pages" — computer data files written in Hypertext Markup Language ("HTML") — which contain information such as text, pictures, sounds, audio and video recordings, and links to other web pages. [Citation.]" (*Brookfield Communications, Inc. v. West Coast Entertainment Corp.* (9th Cir. 1999) 174 F.3d 1036, 1044.)

(1969) 395 U.S. 367, 386.) Consideration of the expressive aspects of computer code, therefore, should not eclipse recognition of the impact of the code's simple functionality. (See, e.g., *Junger*, *supra*, 209 F.3d at p. 485 ["The functional capabilities of source code, and particularly those of encryption source code, should be considered while analyzing the government interest in regulating the exchange of this form of speech."].)

Inasmuch as computer code is hybrid mix of speech and non-speech qualities, a free-speech analysis of a restraint on dissemination of computer code bears a certain resemblance to analyses used in respect to restraints on hybrid mixtures of speech and conduct. *United States v. O'Brien* (1968) 391 U.S. 367, is such a case. There, the United States Supreme Court analyzed an asserted First Amendment defense to a prosecution for expressive burning of a draft card. *Madsen v. Women's Health Center, supra*, is another such case. There, the Court considered a free-speech objection to an injunction against picketing, an activity that affected both an expression of views and a deliberate obstruction of abortion-clinic patronage. In such "mixed" cases, the Court has applied a intermediate-scrutiny test to evaluate the free-speech implications of the restriction at issue.

Applying this precept, the Second Circuit Court of Appeals applied intermediate scrutiny to an injunction obtained under the DMCA prohibiting the dissemination of DeCSS by a website entitled 2600 Quarterly. (*Corley, supra*, 273 F.3d at pp. 450-455.)[18] In doing so, that court relied on First Amendment jurisprudence that the development of new media can present "unique problems, which inform our assessment of the interests at stake, and which may justify

[18] See also *Elcom, supra*, 203 F.Supp.2d at pp. 1128-1129 [intermediate scrutiny applies to an injunction prohibiting the dissemination of a computer program enabling the removal of use restrictions on Adobe Acrobat PDF files and on files formatted for the Adobe eBook Reader].

restrictions that would be unacceptable in other contexts." (See *United States v. Playboy Entertainment* (2000) 529 U.S. 803, 813; *Red Lion Broadcasting, supra*, 395 U.S. at p. 386.)

The Attorney General submits that the *Madsen* intermediate-scrutiny standard is appropriate for purposes of assessing the impact of the subject injunction against Bunner's asserted First Amendment right to disseminate DeCSS. However, as will be explained, the Attorney General believes that two important refinements of the *Madsen* standard are appropriate for use in cases involving a proposed injunction on the dissemination of computer code.

In admonishing that review of an injunction should be "somewhat more stringent" than is the case with content-neutral statutes, the *Madsen* Court noted that a "precision of regulation" was required in ensuring that no more speech was burdened than necessary." (*Madsen, supra*, 512 U.S. at p. 767 & fn. 4.) On one hand, in applying this standard, the *Madsen* Court found that a 36-foot buffer zone around an abortion clinic's entrances and driveway burdened no more speech than was necessary, especially given that "few other options" existed. (*Id.* at pp. 769-770.) And, the *Madsen* Court further found that the ban on shouting, yelling, the use of bullhorns, or the use of other sound amplification equipment between the hours of 7:30 a.m. and noon on Mondays through Fridays was appropriate as "noise control is particularly important around hospitals and medical facilities during surgery and recovery periods." (*Id.* at pp. 772-773.)

On the other hand, in applying this standard, the *Madsen* Court found that the inclusion of private property on the back and side of the clinic within the 36-foot buffer zone "burdened more speech than was necessary" as it failed to serve the significant government interests relied on by the state supreme court. (*Madsen, supra*, 512 U.S. at p. 771.) Further, the *Madsen* Court struck down that part of the injunction banning defendants from physically approaching, within 300 feet of the clinic, any person seeking its services "'unless such a person indicates a desire to communicate.'" (*Id.* at p. 774.) The Court found that, given its prior holdings regarding the need of our citizens to "tolerate insulting, and even outrageous speech" in public debate, this provision burdened more speech than was necessary "to prevent intimidation and to ensure access to the clinic." (*Id.* at pp. 773-774.) Finally, the *Madsen* Court struck down a prohibition against picketing, demonstrating, or using sound amplification equipment within 300 feet of the residences of clinic staff, noting, based on its prior case law, "that a limitation on the time, duration of picketing, and number of pickets outside of a smaller zone could have accomplished the desired result." (*Id.* at p. 775.)

The precision-of-regulation standard applied by *Madsen* suggests that, where a proposed injunction involves computer code, courts should carefully consider whether the injunction burdens the expressive features of the computer code at issue any more than is necessary to serve the interests asserted. If a program's expressive features are more than incidental to its functional features, *Madsen* instructs that a court must carefully assess not just whether the proposed injunction addresses the functional features of the computer code at issue but also whether the proposed injunction burdens the expressive features of that code more than is necessary. (See *Madsen, supra,* 512 U.S. at pp. 771, 773-774.) And in assessing the expressive and functional features of computer code for this purpose, the Court should also take account of the existence of the Internet as a medium which amplifies both the expressive and functional features of computer code by allowing for its instantaneous, worldwide transmission. (See *Playboy, supra*, 529 U.S. at p. 813; *Red Lion Broadcasting, supra*, 395 U.S. at p. 386.) By applying *Madsen*'s precision-of-regulation standard in this manner, courts can carefully balance the heightened First Amendment interests involved in cases where a program's expressive content is not merely incidental to its functional features against the substantial state interest of preventing the dissemination of a trade secret, which would justify an injunction against the dissemination of code.[19] (Cf. *Comedy III Publications v. Saderup* (2001) 25 Cal.4th 387, 401-407 [Court crafted test designed to carefully balance the state law interest in safeguarding intellectual property against the First Amendment interest in freedom of expression in determining whether celebrities and their heirs may assert their state-created publicity rights].)

Moreover, where a proposed injunction involves dissemination of computer code that has more than incidentally expressive features, courts should also consider whether the defendant has advanced any reasonably practical technological alternatives to the injunction. (See *Madsen, supra,* 512 U.S. at p. 775.) Even in the context of a content-neutral time, place, and manner restriction subject to deferential intermediate scrutiny, the availability of reasonable alternatives is not necessarily irrelevant; it is simply not part of the

[19] Some computer programs can have truly minimal expressive content. For example, DeCSS does nothing more than circumvent the access control to DVDs so that digital content on those DVDs can freely be replicated and disseminated without the permission of its creators. (See, e.g., *Reimerdes, supra*, 111 F.Supp.2d at pp. 294, 304-305, 311.) But, not all computer programs have such minimal expressive content. For example, Internet hyperlinks serve as "cross-references within a single document, between documents on the same site, or between documents on different sites." (See *id.* at p. 307.) Via web browsers, a user can "view hypertext documents and follow the hyperlinks that connect them, typically by moving the cursor over a link and depressing the mouse button." (See *ibid.*) Internet hyperlinks correspondingly have a higher expressive content, when viewing them through a First Amendment prism, than DeCSS. (See *id.* at 339; see *also Ashcroft, supra,* 535 U.S. at p. ____ [122 S.Ct. at p. 1703] ["'surfing' the World Wide Web [is] the primary method of remote information retrieval on the Internet today."].) For other (hypothetical) examples of computer programs with more expressive features than DeCSS, see, e.g., *Reimerdes, supra*, 111 F.Supp.2d at p. 333, fn. 217.

plaintiff's burden. (Compare *Turner Broadcasting Systems v. FCC* (1997) 520 U.S. 180, 217-218 (*Turner II*) ["The less-restrictive analysis has never been part of the content-neutral inquiry into the validity of content-neutral regulations on speech."] with *id.* at p. 218 [Court still carefully examined the nature of, and quantum of evidence for, the proffered alternatives to the government's must-carry rules applicable to cable channels before concluding that none of them were "an adequate alternative to must-carry for promoting the Government's legitimate interests."].)

This is not to suggest that "strict scrutiny's" least-restrictive-alternative test should apply whenever wrongful dissemination of a trade secret involves use of more-than-incidentally expressive computer code. Quite to the contrary, the efficacy of using intermediate scrutiny to evaluate injunctions directed to the functional capabilities of computer code would be substantially hindered if the least-restrictive-alternative analysis employed in the review of content-based injunctions applied notwithstanding the content-neutrality of the injunction and the underlying UTSA. (Cf. *Corley, supra,* 273 F.3d at pp. 451-452.) If the "strict scrutiny" burden were placed on an UTSA plaintiff, that plaintiff could find itself unable to disprove or negate the plausible existence of such alternatives even though it suffers demonstrable harm from the publication of the code. Moreover, by the time the plaintiff could amass evidence sufficient to meet its burden of disproving the availability of adequate alternatives, it may be too late to remedy the harm caused by the posting of the code, given that such code can be instantaneously disseminated worldwide due to the Internet.

The Attorney General suggests only that a sufficient showing by the defendant of reasonably practical technological alternatives to the injunction is a reasonable factor for consideration when defendant asserts an expressive value in the wrongful dissemination of a computer code trade secret. (See *Corley,* *supra,* 273 F.3d at p. 455, fn. 29.)[20]

Finally, the Attorney General submits that the same test is appropriate under the free-speech protections of the California Constitution. The Liberty of Speech Clause of the California Constitution provides "[e]very person may freely speak, write and publish his or her sentiments on all subjects, being responsible for the abuse of that right. A law may not restrain or abridge liberty of speech or press." (Cal. Const., art. I, § 2, subd. (a).) The second sentence prohibiting laws restraining, or abridging, the freedom of speech parallels language of the First Amendment. (E.g., *Gerawan Farming, Inc. v. Lyons* (2000) 24 Cal.4th 468, 490.)

However, California's right to free speech is qualified by the imposition of responsibility "for abuse of this right." (Cal. Const., art. I, § 2, subd. (a); *Werner v. Southern Cal. etc. Newspapers* (1950) 35 Cal.2d 121, 124-25 (Traynor, J., writing for the Court).) That imposition of responsibility dates back to 1849. (Compare Cal. Const., art. I, § 2, subd. (a), as amended June 3, 1980, with Cal. Const. of 1849, art. I, § 9.)

This Court has long held that "cogent reasons must exist before a state court in construing a provision of the state Constitution will depart from the construction placed by the Supreme Court of the United States on a similar provision in the Federal Constitution." (E.g., *Gabrielli v. Knickerbocker* (1938) 12 Cal.2d 85, 89.) Applying this principle, this Court has held not only that the test for content-neutrality is the same under both the Liberty of Speech Clause

[20] If the burden were placed on a defendant, the injunction barring the posting or dissemination of computer code could be lifted once the defendant has met its burden of proving the existence of such alternatives. (See *Swan Magnetics v. Superior Court* (1997) 56 Cal.App.4th 1504, 1508.) And, presumably, the harm suffered in the meantime is relatively minimal as the defendant is merely enjoined from publicizing or disseminating the computer code in question.

and the First Amendment, but also that the same intermediate-scrutiny standard obtains in both contexts. (*Los Angeles Alliance For Survival v. City of Los Angeles* (2000) 22 Cal.4th 352, 364-365, 368, 378-379.) Correspondingly, the injunction should be subject to the same intermediate scrutiny under the Liberty of Speech Clause that it is under its federal counterpart.

III.

THE PRELIMINARY INJUNCTION AT ISSUE WITHSTANDS INTERMEDIATE SCRUTINY

Applying the intermediate-scrutiny test set forth above, along with the additional factors accounting for the medium at issue, the Attorney General respectfully submits that the preliminary injunction barring the dissemination of DeCSS "burdens no more speech than necessary to serve a significant government interest." (See *Madsen, supra,* 512 U.S. at pp. 765-766; *Los Angeles Alliance for Survival, supra,* 22 Cal.4th at pp. 367, 373-374, 378.)

A. The Injunction Furthers Significant Government Interests.

1. *The Injunction Serves A Significant Legitimate Interest In Preventing The Unlawful Dissemination Of Trade Secrets.*

The Uniform Trade Secrets Act defines a trade secret as:

> . . . information, including a formula, pattern, compilation, program, device, method, technique, or process, that (1) [d]erives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and (2) [i]s the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

(Civ. Code, § 3426.1, subd. (d).)

Forty-four states and the District of Columbia have adopted variations of the UTSA, all permitting the enjoining of unlawful dissemination of trade secrets.[21] These trade-secrets laws serve substantial (perhaps even compelling) interests of those respective states and of the business community at large.[22]

As the United States Supreme Court declared in the seminal case of *Kewanee Oil*: "The maintenance of standards of commercial ethics and the encouragement of invention are the broadly stated policies behind trade secret law." (*Kewanee Oil, supra*, 416 U.S. at pp. 481-482 [finding that state trade secrets laws are not generally preempted by federal patent law].) In elaborating on this observation, it cited with approval an earlier observation made by the Pennsylvania Supreme Court that state trade-secret protection is important "to the subsidization of research and development and to increased economic efficiency within large companies through the dispersion of responsibilities for creative developments." (*Id.*, citing *Wexler v. Greenberg* (Penn. 1960) 160 A.2d 430, 434-435.)

The Court further observed that trade-secrets laws encourage the dissemination of knowledge by encouraging the licensing of secret processes to others who can be placed under binding legal obligations to protect the trade secret. (*Kewanee* Oil, *supra*, 416 U.S. at pp. 486-487.) And, it gives the States a means by which they can aid companies in combating industrial espionage.

[21] See, e.g., <http://execpc.com/~mhallign/42state.html> ; <http://law.wustl.edu/WULQ/78-3/millikin.pdf>

[22] Bunner suggests an interest cannot be recognized as substantial or compelling in First Amendment jurisprudence unless it is "a coequal provision of the [Federal] Constitution." (See Bunner's Answer Brief, pp. 37, 46-48 & fn. 34.) The Attorney General disagrees. The United States Supreme Court has recognized as important or compelling various non-constitutionally based interests such as the promotion of fair competition, see *Turner II, supra*, 520 U.S. at pp. 197-208, or ensuring public safety and order while safeguarding the medical privacy of our citizens, see *Madsen*, *supra*, 512 U.S. at p. 768, or the protection of our children's well-being, see, e.g., *Reno, supra*, 521 U.S. at pp. 869-870.

(*Id.* at pp. 487-488.)

In discussing how trade secrets law and patent law in fact complement one another, the *Kewanee Oil* Court highlighted the importance of trade secrets law:

> Trade secrets law and patent law have co-existed in this country for over one hundred years.... Trade secret law encourages the development and exploitation of those items of lesser or different invention [that] might be accorded protection under the patent laws, but which items still have an important part to play in the technological and scientific advancement of the Nation. Trade secret law promotes the sharing of knowledge, and the efficient operation of industry; it permits the individual inventor to reap the rewards of his labor by contracting with a company large enough to develop and exploit it. Congress, by its silence over these many years, has seen the wisdom of allowing the States to enforce trade secret protection.

(*Kewanee Oil, supra*, 416 U.S. at p. 493.)

Moreover, from 1974 (when *Kewanee Oil* was decided) until the present, the business community has repeatedly resorted to state trade secrets laws as an important means of protecting their intellectual assets. (See, e.g., *The Law and Economics of Reverse Engineering, supra,* 111 Yale L.J. at pp. 1597-1598 [trade secrets laws are more important to the computer chip industry in protecting their intellectual assets than are patents]; *id.* at 1615-1620 [discussing the economic incentives present in the computer industry for software companies to keep their source code a closely guarded trade secret]; *id.* at pp. 1615-1616, 1620 & fn. 212 [application programming interfaces, which govern how an operating system sends and receives information from other software programs, are often maintained as closely held trade secrets].)

Consequently, California's UTSA — including its injunctive relief provisions, see Civil Code, section 3426.2, subdivision. (a) — serve the important, perhaps even compelling, end of protecting trade secrets. (Cf.

Integral Development, supra, 99 Cal.App.4th at pp. ___ [122 Cal.Rptr.2d at pp. 36-37] [finding same in jurisdictional context]; *Magnecomp, supra,* 209 Cal.App.3d at p. 540 [same].)

2. *The Injunction Furthers The Equally Significant Governmental Interest In Combating Piracy.*

Aside from this significant interest in protecting trade secrets, the injunction serves a significant, perhaps even compelling, interest in protecting DVDs against wholesale digital piracy by prohibiting the posting of DeCSS on the Internet. The Attorney General respectfully urges this Court to recognize this interest here.

As the *Reimerdes* district court observed:

> The anti-trafficking provision of the DMCA [barring the dissemination of circumvention technology such as DeCSS] furthers an important governmental interest — the protection of copyrighted works stored on digital media from the vastly expanded risk of piracy in this electronic age.

(*Reimerdes*, *supra*, 111 F.Supp.2d at p. 330.)[23]

In *Elcom, supra,* 203 F.Supp.2d at pp. 1129-1130, the district court endorsed the importance of this governmental interest in preventing piracy. At issue in that case was a pending criminal prosecution of a company under the DMCA for selling a circumvention program, which allowed a purchaser of an Adobe Acrobat e-book to freely make and disseminate copies. In finding that the DMCA's criminal provisions survived First Amendment scrutiny, the court quoted at length from House and Senate Reports on the DMCA, reasoning that "a plentiful supply of intellectual property — whether in the form of software,

[23] The Second Circuit agreed, noting that "the Government's interest in preventing unauthorized access to encrypted copyrighted material is *unquestionably* substantial, ..." (*Corley*, *supra*, 273 F.3d at p. 454 (italics added).)

music, movies, literature, or other works — drives the demand for a more flexible and efficient electronic marketplace." (203 F.Supp.2d at p. 1129, quoting H.R. Rep. No. 105-551, pt. 2, at p. 23 (1998) and S. Rep. No. 105-190, at p. 8 (1998).) The court further explained:

> Due to the ease with which digital works can be copied and distributed worldwide virtually instantaneously, copyright owners will hesitate to make their works readily available on the Internet without reasonable assurance that they will be protected against massive piracy.

(*Ibid.*) In fact, one state court has found California's interest in combating piracy to be significant for First Amendment purposes. (See *People v. Anderson* (1992) 235 Cal.App.3d 586, 590-591, affd. (9th Cir. 1994) 26 F.3d 100.)

The need perceived by Congress and the courts to combat piracy on the Internet is far from academic. The *Napster* case illustrates just how a service which unlawfully facilitated the Internet transmission of digital music files "ripped" from music compact discs onto computers reduced music compact disc sales, and made it more difficult for music companies to offer fee-based services for copyrighted digital music. (See, e.g., *A&M v. Napster* (9th Cir. 2001) 239 F.3d 1004, 1011-1012, 1016-1018, 1020.)

According to a recent article, online services encouraged such widespread unauthorized copying of music compositions that over 500 million music files from 3 million users were available in May of 2002 alone. (Mariano, *Music Industry Sounds Off On CD Burning* (CNET June 11, 2002) <http://story.news.yahoo.com/news?tmpl=story&u=/cn/20020611/tc_cn/935120> <as of June 12, 2002>.) That same article states that the music industry lost an estimated $4.3 billion worldwide due to piracy, both offline and online. (See *id.*) Another article states:

> There are billions of unauthorized music downloads per month. Last year, record sales in the United States were down 10 percent. The Motion Picture Association of America estimates that it already loses

> more than $3 billion annually to the sale of illegally copied videotapes. By some estimates, more than 350,000 movies are downloaded every day.

(Goodlate, *Stealing Entertainment: The Fiscal And Ethical Price Of Piracy Online*, The Washington Times (May 27, 2002, Final Edition) at A21.) [24]

Accordingly, the need to protect trade secrets and combat piracy constitute significant interests justifying the injunction at issue.

B. The Injunction Burdens No More Speech Than Is Necessary To Further These Interests.

The only positive duty created by the injunction is the requirement that DeCSS itself (or the CSS encryption algorithm and master keys if they are separated from DeCSS) not be posted on a web site. (AA 00711; *McLaughlin, supra* [2000 WL 48512 at *1].) "They may still continue to discuss and debate

[24] The increasing importance of DVDs to the entertainment industry and to consumers only highlights the need to combat piracy. (E.g., *First Quarter DVD Rental Revenue Surpasses Entire Year 2000* (Apr. 24, 2002) <http://www.medianews.com/issues/2002/april/news0424_7.shtml > <as of June 26, 2002> [consumers spent $633.7 million to rent DVDs in the first quarter of 2002]; *Expanding Variety of Players And Software Fuel Momentum Of DVD Sales In First Quarter 2002* (Apr. 30, 2002) <http://www.dvdinformation.com/news/index.html > <as of June 24, 2002> [According to figures compiled by Ernst & Young on behalf of the DVD Entertainment Group, more than 120 million DVD movies and music shipped in the first three months of 2002, a 74 percent increase over the same quarter last year]; *ibid.* [". . . DVD players sold through to U.S. consumers have reached nearly 35 million units and the current installed base is approximately 27.4 million homes (adjusting for homes owning two or more DVD players)"]; Natale, *Press Play to Access The Future: The DVD Has Opened Up New Ways To Access The Future — Some Intended And Some Quite Definitely Not*, Los Angeles Times, Sunday Calendar (April 7, 2002, Home Edition) at 4 *et. seq.* [DVD gives consumers the ability to interact with the storytelling and filmmaking process of movies, to create or enjoy alternate versions of movies, and to understand how movies are made]; *ibid.* [sales of DVDs last year reached $4.6 billion, 2 ½ times their 2000 revenue].)

the subject [of DeCSS or copying DVDs] as they have in the past in both [*sic*] educational, scientific, philosophical, and political context [*sic*]." (AA00714; *id.* [2000 WL 48512 at *2].)

Moreover, "[n]othing in this Order shall prohibit discussion, comment or criticism, so long as the proprietary information identified above is not disclosed or distributed." (AA00716; *id.* [2000 WL 48512 at *4].) If Bunner and the other Defendants want to compose haiku on DeCSS, discuss the drawbacks of DVDCCA's encryption system, or critique DVDCCA's efforts to safeguard against the pirating of digital content, they are free to do so under the terms of the injunction. (Compare *ibid.* with Bunner's Answer Brief, pp. 3, fn. 4.)

Similarly, if the parties to this suit (or anyone else) wish to lobby for the creation, or licensing, of CSS code which will enable DVDs to be played on Linux operating systems, they are free to do so. (See AA00488 & *Reimerdes, supra*, at pp. 310, 337 & fns. 64, 243 [suggesting that DVDCCA will do, or is doing, as much].) And, in contrast to the injunction at issue in *Corley*, the injunction expressly allows Bunner and other Defendants to link to other web sites which may contain DeCSS. (AA00716; *McLaughlin, supra* [2000 WL 48512 at *4].)

Applying the two refinements of the *Madsen* test does not change this result. The minimal expression contained in the DeCSS computer code is incidental to its functional purpose of directly executing computer processes such that the injunction on its dissemination burdens no more speech than is necessary to achieve the interests asserted. Moreover, Bunner has not suggested, insofar as the Attorney General can determine, that any reasonably practical technological alternatives exist to the injunction. While the existence of such alternatives to enjoining the posting of DeCSS were suggested in *Corley*, the *Corley* court found that the defendant had failed to meet its burden.

(See *Corley, supra*, 273 F.3d at p. 455, fn. 29.)

Accordingly, the injunction burdens no more speech than necessary to combat piracy and protect trade secrets.

CONCLUSION

The Court of Appeal's decision below, if affirmed, dramatically narrows the scope of the UTSA and detrimentally impacts the ability of California businesses to protect their intellectual assets. This impact extends to brick and mortar businesses as well as high technology industries.

Far from ensuring that the marketplace of ideas remain robust, the Court of Appeal's decision could seriously undermine contributions to this marketplace. Absent an appropriate balancing of free speech principles and the substantial governmental interests in preventing theft and piracy of trade secrets, the UTSA is rendered toothless. Stripped of the protections provided their intellectual property rights pursuant to this statute, businesses may well lose the incentive to contribute to this marketplace.

Accordingly, for the reasons set forth above, the Attorney General respectfully submits that this Court should reverse the decision of the Court of Appeal, and affirm the preliminary injunction granted by the superior court. Alternatively, should this Court instead remand this case for further proceedings in accordance with its opinion, this Court should instruct the lower court to apply intermediate scrutiny under the First Amendment and the California Liberty of Speech Clause.

///

///

Dated: August 2, 2002

Respectfully submitted,

BILL LOCKYER
Attorney General of the State of California

MANUEL M. MEDEIROS
State Solicitor

RICHARD M. FRANK
Chief Assistant Attorney General

LOUIS VERDUGO, JR.
Senior Assistant Attorney General

CATHERINE Z. YSRAEL
Supervising Deputy Attorney General

czy fn

Regina Brown

REGINA J. BROWN
Deputy Attorney General

Emilio E. Varanini IV

EMILIO E. VARANINI IV
Deputy Attorney General

On behalf of the Attorney General as amicus curiae

CERTIFICATE OF COMPLIANCE

Pursuant to California Rules of Court Rule 14(c)(1), counsel for amici curiae hereby certify that the foregoing brief submitted in support of the position of the DVD Copy Control Association, Inc. complies with the type-volume limitations of that Rule.

Exclusive of the exempted portions in California Rules of Court Rule 14(c)(3), the brief contains 13,022 words, as calculated by counsel's word processing program.

Respectfully submitted,

BILL LOCKYER
Attorney General of the State of California

MANUEL M. MEDEIROS
State Solicitor

RICHARD M. FRANK
Chief Assistant Attorney General

LOUIS VERDUGO, JR.
Senior Assistant Attorney General

CATHERINE Z. YSRAEL
Supervising Deputy Attorney General

EMILIO E. VARANINI IV
Deputy Attorney General

On behalf of the Attorney General as
amicus curiae

DECLARATION OF SERVICE

Case Name: **DVD COPY CONTROL ASSOCIATION, INC. v. ANDREW BUNNER**
Case No.: **S102588**

I declare:

I am employed in the Office of the Attorney General, which is the office of a member of the California State Bar at which member's direction this service is made. I am 18 years of age or older and not a party to this matter; my business address is 300 South Spring Street, Los Angeles, California 90013. I am familiar with the business practice at the Office of the Attorney General for collection and processing of correspondence for mailing with the United States Postal Service. In accordance with that practice, correspondence placed in the internal mail collection system at the Office of the Attorney General is deposited with the United States Postal Service that same day in the ordinary course of business.

On August 2, 2002, I served the attached **BRIEF OF ATTORNEY GENERAL BILL LOCKYER AS AMICUS CURIAE IN SUPPORT OF RESPONDENT** by placing a true copy thereof enclosed in a sealed envelope with postage thereon fully prepaid, in the internal mail system of the Office of the Attorney General, addressed as follows:

PLEASE SEE ATTACHED SERVICE LIST.

On August 2, 2002, I caused original plus fourteen (14) copies of the **BRIEF OF ATTORNEY GENERAL BILL LOCKYER AS AMICUS CURIAE IN SUPPORT OF RESPONDENT** in this case to be delivered to the California Supreme Court at **300 South Spring Street, North Tower, Second Floor, Los Angeles, California 90013** by **personal service.**

I declare under penalty of perjury under the laws of the State of California the foregoing is true and correct and that this declaration was executed on August 2, 2002, at Los Angeles, California.

C. VILLAREAL	
Declarant	Signature

SERVICE LIST

Supreme Court of the State of California. **[Via U.P.S.]**
Frederick K. Ohlrich, Clerk of the Court
350 McAllister Street
San Francisco, CA 94102-4783

Court of Appeal of the State of California **[Via U.P.S.]**
Sixth Appellate District
Attention: Mr. Willy Magsaysay
333 West Santa Clara Street, Suite 1060
San Jose, CA 95113

Santa Clara County Superior Court **[Via U.P.S.]**
Attention: Hon. William S. Elfving
191 North First Street
San Jose, CA 95113-1090

Attorneys for Petitioner, DVD Copy Control Association, Inc. **[Via U.P.S.]**
Jared Bobrow, Esq.
Christopher J. Cox, Esq.
WEIL, GOTSHAL & MANGES LLP
201 Redwood Shores Parkway
Redwood Shores, CA 94065

Jeffrey L. Kessler, Esq.
Robert G. Sugarman, Esq.
Gregory S. Coleman, Esq.
Edward J. Burke, Esq.
John F. Greenman, Esq.
WEIL, GOTSHAL & MANGES LLP
767 Fifth Avenue
New York, NY 10153

Attorneys for Respondent, Andrew Bunner **[Via U.P.S.]**

James R. Wheaton, Esq.
David Green, Esq.
First Amendment Project
1736 Franklin Avenue, 9th floor
Oakland, CA 94612

Thomas E. Moore, III, Esq.
TOMLINSON, ZISKO, MOROSOLI & MASER LLP
200 Page Mill Road, 2nd floor
Palo Alto, CA 94306

Allonn E. Levy, Esq.
HS Law Group
210 North Fourth Street, Suite 200
San Jose, CA 95112

Cindy Cohn
Robin D. Gross, Esq.
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110

Attorney for Amici Curiae **[Via U.S. Mail]**
American Civil Liberties Union of Northern California
and Silha Center for the Center for the Study of Media Ethics and Law
Ann Brick (SBN 65296)
American Civil Liberties Union Foundation of North California, Inc.
1663 Mission Street, Suite 460
San Francisco, CA 94103

Attorney for Amici Curiae **[Via U.S. Mail]**
Microsoft Corporation, Ford Motor Company, The Boeing Company,
Sears, Roebuck & Co., The Procter & Gamble Company, AOL Time
Warner Inc., Bellsouth Corporation, The BellSouth Corporation,
The Coca-Cola Company, and the National Association of Manufacturers
Richard A. Epstein, Esq.
1111 East 60th Street
Chicago, Illinois 60637

Attorneys for Amicus Curiae **[Via U.S. Mail]**
Computer Professionals for Social Responsibility
Jennifer Granick, Esq.
Computer Professionals for Social Responsibility
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

Attorneys for Amicus Curiae **[Via U.S. Mail]**
The Intellectual Property Owners Association
Milbank, Tweed, Hadley & McCloy, LLP
James Pooley, Esq.
630 Hansen Way, Second Floor
Palo Alto, CA 94304

Attorneys for Amici Curiae **[Via U.S. Mail]**
Intellectual Property Law Professors,
The Computer & Communications Industry Association,
and the United States Public Policy Committee of the Association
for Computing Machinery
Jennifer M. Urban
Samuelson Law, Technology & Public Policy Clinic
UC at Berkeley School of Law
396 Simon Hall
Berkeley, CA 94720-7200

Attorneys for Amici Curiae
Motion Picture Association of America, Inc.; American Federation of Musicians of the United States and Canada; American Federation of Television & Radio Artists; AFMA (Formerly The American Film Marketing Association); American Society of Composers; Authors and Publishers; American Society of Media Photographers, Inc.; Association of American Publishers, Inc.; Broadcast Music, Inc.; Department of Professional Employees; Directors Guild of America; Graphic Artists Guild; Interactive Digital Software Association; National Academy of Recording Arts & Sciences, Inc.; National Association of Theatre Owners; National Cable & Telecommunications Association, Inc.; National Football League; National Hockey League; National Music Publishers' Association; Office of the Commissioner of Baseball; Producers Guild of America; Professional Photographers of America; Recording Industry Association of America; Screen Actors' Guild; and Writers Guild of America, West, Inc.
David E. Kendall
WILLIAMS & CONNOLLY LLP
725 Twelfth Street, N.W.
Washington, D.C. 20005