No. S102588

IN THE SUPREME COURT OF THE

STATE OF CALIFORNIA

DVD COPY CONTROL ASSOCIATION, INC., *Plaintiff/Appellant,*	) Court of Appeal No. H021153
V.	) Superior Court No. CV 786804
ANDREW BUNNER, *Defendant/Respondent.*	) (Hon. William J. Elfving, Judge Presiding)

BRIEF OF *AMICI CURIAE*
INTELLECTUAL PROPERTY LAW PROFESSORS,
THE COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION, AND THE UNITED STATES PUBLIC POLICY COMMITTEE OF THE ASSOCIATION FOR COMPUTING MACHINERY SUPPORTING AFFIRMANCE

Jennifer M. Urban (Bar No. 209845)
Samuelson Law, Technology and Public Policy Clinic
University of California at Berkeley School of Law (Boalt Hall)
396 Simon Hall
Berkeley, CA 94720-7200
(510) 642-7561

On the Brief:
Pamela Samuelson
Chancellor's Professor of Law and Information Management
University of California at Berkeley School of Law (Boalt Hall)
434 North Addition
Berkeley, CA 94720-7200
(510) 642-6775

ATTORNEYS FOR *AMICI CURIAE*

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

COURT RULES

OTHER AUTHORITIES

BOOKS

ARTICLES

APPLICATION FOR LEAVE TO FILE BRIEF AMICI CURIAE

Pursuant to Rule 29.3(c) of the California Rules of Court, the Computer & Communications Industry Association, the United States Public Policy Committee of the Association for Computing Machinery, and the intellectual property law professors listed on Appendix A respectfully request leave to file the attached Brief Amici Curiae in support of Affirmance. This Application and the accompanying Brief Amici Curiae are filed within the time specified in Rule 29.3(c) of the California Rules of Court.

A. The Amici Curiae.

The law professor Amici teach, write, and speak publicly about intellectual property law and policy. Both individually and as a group, they are concerned with the proper evolution of trade secrecy law, the consistency of this law with federal constitutional interests, and with preservation of legal rules that permit reverse engineering in order to promote innovation and competition in high technology and other industries. Amici law professors have no financial interest in the outcome of this litigation nor any relationship with the parties.

Amicus Computer & Communications Industry Association (CCIA) is a non-profit trade association and as such has no parent corporation nor any issued stock or partnership shares. CCIA's mission is to promote open, barrier-free competition in the offering of computer and communications products and services worldwide. CCIA's members include: AOL Time Warner; Atreus Corporation; Block Financial Corporation; CAI/SISCo; Covad Communications Co.; Datum, Inc.; Eastman Kodak Co.; Entegrity Solutions Corporation; Fujitsu Limited; Haynes Electronics, Inc.; Hitachi Data Systems, Inc.; Intuit, Inc.; Liberate Technologies, Inc.; MRO Software, Inc.; Merant; NetCom Solutions International, Inc.; NOKIA; Nortel Networks; Novak Biddle Venture Partners; NTT America, Inc.; Okidata Americas, Inc.; Oracle Corporation; QuickHire; SABRE Inc./Travelocity; StreamCast Networks, Inc; Sun Microsystems, Inc.; Tantivy Communications, Inc.; Time Domain Corporation; United Parcel Service; Valaran Corporation; Verio, Inc.; Verizon; ViON Corporation; and Yahoo!, Inc. Neither CCIA nor its

members has a direct financial interest in the outcome of this litigation.[1]

The Association for Computing Machinery (ACM) is a leading professional association of computer scientists and other information technology professionals dedicated to advancing the art, science, engineering and application of information technology. Amicus United States Public Policy Committee of the Association for Computing Machinery (USACM) serves as the focal point for ACM's interactions with U.S. government organizations and the science and technology policy community. USACM supports the mission of ACM by utilizing its independent technical expertise to assist policy-makers and the public in understanding the implications of computing and information technology policy issues.[2]

B. Interest of Amici Curiae.

Amici law professors submit this brief out of concern with the proper evolution of state trade secrecy law and with preservation of

[1] For more information regarding CCIA, *see* <http://www.ccianet.org>.
[2] For more information regarding USACM, *see* <http://www.acm.org/usacm/>.

limiting principles of trade secrecy law that are critical to maintaining balance between trade secrecy law and federal intellectual property law and policy. The Superior Court's analysis of the trade secret misappropriation claim is, in their view, deeply flawed and threatens to undermine important public policy purposes of trade secrecy law and federal intellectual property law which strongly support the right to reverse engineer mass marketed products and to republish information that, although once a trade secret, has lost its trade secrecy status by virtue of being widely published on the Internet.

CCIA has long supported interpretations of intellectual property laws to permit reverse engineering performed to develop interoperable products. Although neither CCIA nor its members has a direct financial interest in the outcome of this litigation, affirmance of the Superior Court's decision would have serious anti-competitive consequences for CCIA members and the computer industry as a whole.

The individual researchers and technologists of USACM believe that reverse engineering is critical for systems interoperability and facilitates the research, development, and testing of information

processing systems. The software engineering and research communities also utilize reverse engineering to investigate security risks and develop programs that impede the spread of viruses and other kinds of malicious software, craft emergency fixes to newly-discovered flaws, address compatibility issues (e.g., Y2K compliance of old software), and determine whether provided software has "Trojan Horse" components that might violate privacy or legal interests of the end user. Although neither USACM, nor its individual members, have a direct financial interest in the outcome of this litigation, affirmance of the Superior Court's decision would have serious stifling consequences for software engineers, the computing community, and individual members of USACM involved in education and research, as well as the overall security of the information infrastructure and electronic commerce.

C. Need for Further Briefing.

Amici are familiar with the issue before the Court and the scope of its presentation. Amici believe that further briefing is necessary to consider how limiting principles of trade secrecy law, as

applied to the specific facts of this case, dovetail with the First Amendment considerations on which the parties' briefs focus. In particular, Amici are concerned with how the Court's decision will affect the balance struck between trade secret law and federal intellectual property law policy.

Amici respectfully submit that the expertise in trade secret law and federal intellectual property law and policy provided by Amici law professors, the industrial perspective on possible anti-competitive consequences provided by the CCIA, and the technical perspective on the importance of reverse engineering provided by the USACM, will assist the Court in resolving the issue before it.

CONCLUSION

For all of the foregoing reasons, Amici Curiae respectfully request that the Court accept the accompanying Brief Amici Curiae for filing in this case, and consider its contents in resolving the question before the Court.

Respectfully submitted,

Jennifer M. Urban (Bar No. 209845)
Samuelson Law, Technology and
Public Policy Clinic
University of California at Berkeley
School of Law (Boalt Hall)
396 Simon Hall
Berkeley, CA 94720-7200
(510) 642-7561

Dated: July 10, 2002

BRIEF AMICI CURIAE

INTRODUCTION

The DVD Copy Control Association (DVD CCA) hyperbolically asserts that the Court of Appeal's decision "effectively repeals the statutory protections afforded to trade secrets under California law, leaving DVD CCA and other trade secret owners, with no real remedy to address the misappropriation and dissemination of their technologies." DVD CCA Opening Brief on the Merits at 10. It also predicts that "[t]he effect of the Court of Appeal's ruling…[will be] that the value of trade secrets in California will be virtually destroyed." *Id.* at 11. With all due respect, this is complete nonsense.

Amici agree with DVD CCA that preliminary and permanent injunctions are commonly granted in trade secret cases without offending the First Amendment, and this is as it should be. In the ordinary trade secret case, the misappropriator of trade secrets is an errant licensee, a faithless employee or former employee, an abuser of a confidential relationship with the trade secret claimant, a trickster who used deceit or other wrongful means to obtain trade secrets, or a knowing recipient of misappropriated information. In these cases,

injunctions merely require parties to abide by express or implicit agreements they have made, to respect the confidences under which they acquired secret information, and not to engage in tortious acts or other wrongdoing. As the Court of Appeal observed, the trade secret cases on which DVD CCA has relied involve ordinary trade secret claims of this sort. *DVD Copy Control Ass'n v. Bunner*, 93 Cal. App.4th 648, 662-63, 113 Cal. Rptr. 338, 349 (2001). The present case is not, however, an ordinary trade secret misappropriation case. Indeed, Amici vigorously question whether it is a trade secret misappropriation case at all.

The Superior Court erred, as a matter of law, in ruling that reverse engineering of a mass-marketed product (which it presumed occurred in violation of a mass-market license agreement) constituted misappropriation of trade secrets learned from reverse engineering. The Superior Court failed to consider the many policy reasons why California law and federal intellectual property policy strongly favor allowing mass-marketed products to be reverse engineered and the results of reverse engineering to be used and disseminated as the reverse engineer chooses. The Superior Court committed further

legal error in ruling that Bunner's posting of the DeCSS program on the Internet was a continuation of the reverse engineer's purported misappropriation. By the time Bunner posted DeCSS on his website, DeCSS had already been broadly disseminated on the Internet. Even assuming that DeCSS contained CSS trade secrets (which is unclear), the availability of DeCSS on the Internet prior to Bunner's posting necessarily caused the loss of any such CSS trade secrets, even if DVD CCA is correct (which it is not) that the reverse engineer had misappropriated CSS trade secrets. Regrettably, the Court of Appeals did not fully analyze DVD CCA's trade secret claims, focusing instead on Bunner's claim that issuance of a preliminary injunction in this case violated the First Amendment.

The California Supreme Court should reaffirm the longstanding principle of trade secret law that reverse engineering of mass-marketed products is a lawful way to acquire a trade secret. It should repudiate the notion that an anti-reverse engineering clause in a mass-market license can override the right to reverse engineer. Maintaining this principle is essential if California's high technology industry—indeed, virtually all of its industries—is to thrive in coming years.

Although it may be unfortunate that the publication of trade secret information on the Internet can result in loss of trade secrecy protection, the California Supreme Court should follow precedents cited below that hold that broad dissemination of previously secret information on the Internet, such as the multiple postings of DeCSS, results in the dedication of that information to the public domain.[3] Amici thus urge the California Supreme Court to affirm the Court of Appeals' ruling in favor of Bunner. Amici take no position on Bunner's First Amendment claims; however, Amici believe that traditional limits of trade secrecy law, as applied to the specific facts of this case, dovetail with First Amendment considerations.

[3] The complaint indicates that DeCSS had been displayed on websites in at least eleven states and eleven countries throughout the world months before this lawsuit was initiated. Complaint for Injunctive Relief for Trade Secret Misappropriation, *DVD Copy Control Ass'n v. McLaughlin* (Dec. 28, 1999).

ARGUMENT

I. Trade Secrecy Law Protects Computer Programs And Information Embodied In Them Against Unfair Competitive Acts, But It Does Not Confer Exclusive Rights That Are Good Against The World.

Trade secrecy law provides significant protection to developers of technologies, such as the Content Scramble System (CSS). However, it does not grant, as patent and copyright laws do, exclusive rights that are good against the world without regard to whether the defendant is in a confidential relationship with the rights holders or knew of the existence of the rights claimed to be infringed.[4] Patent law, for example, allows qualifying inventors to sue those who independently invent the same machine or process and who are consequently wholly lacking wrongful intent. *See* 35 U.S.C. § 271(a); 2 Roger M. Milgrim, *Milgrim on Trade Secrets*, § 9.02[5][a] (2000).

[4] DVD CCA relies to a significant degree on caselaw that rejects First Amendment defenses in intellectual property cases, such as copyright cases, right of publicity cases, and trademark cases. DVD CCA Opening Brief on the Merits at 35-38. It omits mention of some cases in which First Amendment defenses were successful. *See, e.g., L.L. Bean, Inc. v. Drake Publishers., Inc.*, 811 F.2d 26 (1st Cir. 1987) (First Amendment important in defeating trademark dilution claims*); Hicks v. Casablanca Records*, 464 F. Supp. 426 (S.D.N.Y. 1978) (First Amendment considerations important factor in defeating right of publicity claim). As Section I will show, trade secret rights are more limited in scope than intellectual property rights involved in the cases DVD CCA relies upon. Even the exclusive rights of patent and copyright laws are muted by public policy limitations on the scope of rights, such as library and archival copy privileges, fair use, and first sale rights, and on the duration of protection. *See, e.g.*, 17 U.S.C. §§ 107-121.

Copyright law allows authors and publishers to sue those who innocently infringe copyrights, as when a bookstore unwittingly distributes infringing copies of a book. *See* 17 U.S.C. § 106(2); *D.C. Comics, Inc. v. Mini Gift Shop*, 912 F.2d 29, 35 (2d Cir. 1990) ("It is important to note that a finding of innocent infringement does not absolve the defendant of liability under the Copyright Act.").

Trade secrecy rights are much more limited in scope.[5] The Restatement of Unfair Competition points out that "[t]he owner of a trade secret does not have an exclusive right to possession or use of the secret information. Protection is available only against a wrongful acquisition, use or disclosure of the trade secret," American Law Institute, *Restatement of the Law of Unfair Competition*, § 43 cmt. a at 493 (1993), as when the use or disclosure breaches an implicit or explicit agreement between the parties or when improper means, such as trespass or deceit, are used to obtain the secret. American Law

[5] Trade secret rights are of more recent origin than patents or copyrights. DVD CCA is mistaken in asserting that trade secrecy law predates the U.S. Constitution. *See* DVD CCA Opening Brief on the Merits at 2, 12. See, e.g., James H.A. Pooley, *Trade Secret Law* § 1.03 (1999); Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of a Justification*, 86 Calif. L. Rev. 241, 251 (1998); Catherine Fisk, *Working Knowledge: Trade Secrets, Restrictive Covenants in Employment, and the Rise of Corporate Intellectual Property, 1800-1920*, 52 Hastings L.J. 441, 452 (2001). Hence, its arguments based on a presumed intent by the Framers that the First Amendment should not bar issuance of injunctions against dissemination of trade secrets are ill-founded.

Institute, *Restatement of Torts*, § 757 (1939); UTSA § 1. Even when a person or firm has misappropriated another firm's trade secret, injunctive relief may be limited in duration based in part on the court's estimation of how long it would take a reverse engineer to discover the secret lawfully. *See, e.g., K-2 Ski Co. v. Head Ski Co.*, 506 F.2d 471, 474 (9th Cir. 1974); *Sigma Chemical Co. v. Harris*, 794 F.2d 371, 374 (8th Cir. 1986). Like other nonpublic information, trade secrets sometimes leak even when firms have taken some steps to protect them. *See, e.g., Defiance Button Machine Co. v. C & C Metal Prods. Corp.*, 759 F.2d 1053 (1985) (trade secret status lost for information inadvertently left on laptop computer sold at auction, even though file was password protected); *Flotec, Inc. v. Southern Research, Inc.*, 16 F. Supp.2d 992, 1003, n. 5 (S.D. Ind. 1998) (drawings kept secret, but details revealed in testimony in open court). Trade secrets frequently leak out by reverse engineering. *See*, James H. A. Pooley, *Trade Secret Law* § 5.02[5] (1999) (almost inevitable that trade secrets will be reverse engineered). Innocent recipients of trade secrets are generally beyond the reach of trade secrecy law.

Because a firm does not need to file an application with the government to obtain trade secret protection, as one must do to obtain patent protection and as authors must generally do to litigate copyright claims, trade secret law insists upon specificity about the trade secrets alleged to have been misappropriated. California law requires those who claim trade secret misappropriation to "identify the trade secret with reasonable particularity." Cal. Civ. Code § 2019 cmt. d. *See also, e.g., Diodes, Inc. v. Franzen*, 260 Cal. App. 2d 244 , 67 Cal. Rptr. 19 (1968) (affirming dismissal of trade secret claim for failure to adequately specify trade secrets alleged to have been misappropriated). DVD-CCA has been unclear about what trade secrets it alleges were actually misappropriated and whether DeCSS contains any such secrets.[6]

[6] The Superior Court characterized the evidence of trade secret misappropriation as "fairly clear." *DVD Copy Control Ass'n v. McLaughlin*, 2000 WL 48512 at 2 (Cal. Super. Ct. 2000). Amici find this characterization puzzling in view of the large number of missing facts in the case. Although DVD CCA claims to be the exclusive licensor of CSS trade secrets, it did not hold these rights at the time of the reverse engineering that is alleged to be the basis of the trade secret misappropriation claim. *See* Declaration of John J. Hoy, ¶ 24. The record does not disclose who did hold the trade secret rights at that time. Exactly who was licensed by whom and on what terms is not clear. Moreover, it is possible that one or more licensees of CSS failed to take adequate precautions to protect the trade secrets and built a player from which some CSS secrets could be discerned. *See, e.g.*, Andy Patrizio, *Why The DVD Hack Was A Cinch, at* <http://www.wired.com/news/print/0,1294,32263,00.html> (Nov. 2, 1999). Also missing are facts about who purchased or otherwise acquired the DVD player that was allegedly reverse engineered, from whom the player was acquired and on what terms, whether there was actually a click-through license, who (if anyone) clicked "I agree" to license terms, who actually reverse engineered CSS, whether that person was the same person as the person who acquired the DVD player and/or

The CSS program itself cannot be considered a trade secret because it has been widely distributed in mass-marketed products. *See, e.g., Videotronics, Inc. v. Bend Electronics*, 564 F. Supp. 1471 (D. Nev. 1983) (rejecting trade secret misappropriation claims as to mass-marketed game program); *Sega Enters. Ltd. v. Accolade, Inc.*, 977 F.2d 1510, 1526, n.9 (9th Cir. 1992) (because Sega's game programs had been widely mass-marketed, Sega could not claim that these programs were unpublished works).

While internal design elements of programs, such as algorithms and information pertinent to program functions, may be trade secrets if they are not readily ascertainable from mass marketed object code forms of programs, these secrets are susceptible to being discovered by reverse engineering (the implications of which are explored in the next section). As Amici understand the facts, DeCSS is a separate computer program from CSS. DVD CCA is unclear as to whether DeCSS embodies any code from CSS, any of its algorithms, or any

---

clicked through the license, as well as what trade secrets were allegedly misappropriated. This case piles one presumption about the facts on top of another to fabricate a house of cards in support of a weak legal claim. It is not enough to say, as the Superior Court did, that "CSS is a piece of proprietary information." *DVD Copy Control Ass'n v. McLaughlin*, 2000 WL 48512 at 1 (Cal. Super. Ct. 2000). CSS was embodied in a mass marketed product. This affects the ability of DVD CCA to claim trade secret status for CSS.

other information that DVD CCA can rightfully claim as a trade secret. It is possible that the developer of DeCSS may have needed to know some technical details about CSS in order to develop DeCSS, but that does not necessarily mean that DeCSS contains this information. If DeCSS does not contain any information that DVD CCA can rightfully claim as a trade secret, Amici question whether a third party such as Bunner (that is, someone who did not him- or herself misappropriate any trade secret information) can be enjoined from redistributing a program developed with aid of information that was at some point in the past a trade secret. Many trade secret claims have failed for lack of specificity. *See, e.g., Religious Technology Center v. Netcom Online Comm.*, 923 F. Supp. 1231, 1255 (N.D. Cal. 1995); *Metro Traffic Control, Inc. v. Shadow Traffic Network,* 22 Cal. App. 4th 853, 861-63, 27 Cal. Rptr. 573, 578-79 (1994) (affirming denial of preliminary injunction in trade secret case because of failure to adequately specify trade secrets).

II. Reverse Engineering A Mass-Marketed Product Is A Proper Means To Obtain Trade Secrets It May Contain As A Matter Of California Law And Federal Intellectual Property Policy.

Reverse engineering has always been a lawful way to acquire a trade secret, as long as "acquisition of the known product…[is] by fair and honest means, such as purchase of the item on the open market." Official Comment on § 1 of Uniform Trade Secrets Act (cited hereinafter as UTSA). California trade secret law expressly provides that reverse engineering is a lawful way to obtain a trade secret. Cal. Civ. Code § 3426.1(a). As there is no evidence in the record to the contrary, Amici presume that the DVD system from which CSS information was obtained was lawfully acquired.

Justification for trade secret law's recognition of a right to reverse engineer derives in part from purchase of the product in the open market which confers on its owner personal property rights, including the right to take the purchased product apart, measure it, subject it to testing, and the like. *See* Pamela Samuelson and Suzanne Scotchmer, *The Law and Economics of Reverse Engineering*, 111 Yale L. J. 1575, 1583 (2002). The time, money, and energy that

reverse engineers invest in analyzing products may also be a way of earning rights to the information they learn thereby. *Id.* Still another justification stems from treating the sale of products in the open market as a kind of publication of innovations they embody. This publication dedicates these innovations to the public domain unless the creator has obtained patent protection for them. *See, e.g, Tabor v. Hoffman*, 118 N.Y. 30, 23 N.E. 12 (Ct. App. 1889) (discussing the "publication" theory).

Trade secret law's right to reverse engineer is important in maintaining balance among intellectual property laws. Federal patent law allows innovators to have up to twenty years of exclusive rights to make, use and sell the invention, 35 U.S.C. § 154(a), but only in exchange for disclosure of significant details about their inventions to the public. 35 U.S.C. § 112 (setting forth disclosure requirements). This deal is attractive in part because if an innovator chooses to protect its invention as a trade secret, such protection may be short-lived if it can be reverse-engineered. If trade secrets were legally immune from reverse engineering, this would substantially undermine incentives for inventors to apply for patents because trade secret law

would then provide perpetual exclusive rights without the bother and expense of applying for a patent and disclosing the invention.

This helps to explain why courts and commentators agree that for state trade secrecy law to be compatible with federal intellectual property policy, it must provide a right to reverse engineer. In *Chicago Lock Co. v. Fanberg*, 676 F.2d 400 (9th Cir. 1982), for example, the plaintiff claimed that the Fanbergs misappropriated its trade secret key codes when they published a compilation of this information. The Fanbergs obtained much of this information by reverse engineering Chicago locks for their customers. The Fanbergs obtained similar information from other locksmiths for inclusion in the book. Because the Fanbergs obtained the key code information by reverse engineering or from reverse engineers, the Ninth Circuit concluded that publication of the book could not be enjoined. It observed that if state trade secret law did not allow reverse engineering, it "would, in effect, convert the Company's trade secret into a state-conferred monopoly akin to the absolute protection that a federal patent affords. Such an extension of California trade secrets

law would certainly be preempted by the federal scheme of patent regulation." *Id.* at 404.

Fanberg relied on the Supreme Court's decision in *Kewanee v. Bicron Corp.*, 416 U.S. 470 (1974) and other Supreme Court preemption decisions.[7] The Supreme Court in *Kewanee* overturned a ruling by the Sixth Circuit Court of Appeals that state trade secrecy law conflicted with federal patent policy because it undermined incentives to apply for federal patents. The majority in *Kewanee* concluded that no serious conflict existed because trade secrecy law was both weaker than and different from patent law. Reverse engineering was one of the features of trade secrecy law that made it weaker and different from patent law. As the Court explained:

> Trade secret law provides far weaker protection in many respects than patent law. While trade secret law does not forbid the discovery of the trade secret by fair and honest means, e.g., independent creation or reverse engineering, patent law operates 'against the world,' forbidding any use of the invention for whatever purpose for a significant length of time….Where patent law acts as a barrier, trade secret law functions relatively as a sieve.

[7] The *Chicago Lock* decision could have invoked the First Amendment as another federal constitutional interest reinforcing the court's conclusion that the Fanbergs had a legal right to publish the results of their lawful reverse engineering.

Kewanee, 416 U.S. at 489-90. *See also* Pooley, *supra*, § 5.02 at 5-16 (1999) (because reverse engineering makes trade secret law weaker than patent law, trade secret law is not preempted by patent law); 1 Melvin F. Jager, *Jager on Trade Secrets* § 5.04[3][a][i] at 5-39 (2001) ("The likelihood that unpatented objects in the public domain will be reverse engineered is part of the federal balance. It is an inducement to create patentable inventions."). Thus, recognition of a right to reverse engineer trade secrets is critically important in preserving the appropriate balance of federal intellectual property law. Any interpretation of California's trade secrecy law that contravened this principle would put this law into conflict with federal intellectual property policy.

Reverse engineering is also "an essential part of innovation," as the U.S. Supreme Court observed in *Bonito Boats, Inc. v. Thunder Craft Boats, Inc.*, 489 U.S. 141(1989), an activity likely to yield variations on the product that "could lead to significant advances in technology." *Id.* at 160. The Court added that "the competitive reality of reverse engineering may act as a spur to the inventor" to develop additional patentable ideas. *Id.* Even when reverse

engineering does not lead to additional innovation, the *Bonito Boats* decision suggests it may still promote consumer welfare by providing consumers with access to competing products which may be offered at a lower price. *Id*. at 164-65. Other commentators have observed that without a legal right to reverse engineer, the market power of trade secret holders may be unduly strong. *See, e.g.*, David Friedman, William M. Landes, & Richard A. Posner, *Some Economics of Trade Secret Law*, 5 J. Econ. Persp. 61, 70-71 (1991).

In *Bonito Boats* the U.S. Supreme Court struck down a Florida law that forbade manufacturers of boats from using existing boat parts as "plugs" for a molding process for producing competing products. The Court struck down this law because it "prohibit[ed] the entire public from engaging in a form of reverse engineering of a product in the public domain." *Bonito Boats*, 489 U.S. at 160. The Court noted that it was "difficult to conceive of a more effective method of creating substantial property rights in an intellectual creation than to eliminate the most efficient method for its exploitation." *Id*. at 164.

Drawing upon its earlier preemption rulings,[8] the Court said they protected "more than the right of the public to contemplate the abstract beauty of an otherwise unprotected intellectual creation—they assure its efficient reduction to practice and sale in the marketplace." *Id.* The Court went on to say that "[w]here an item in general circulation is unprotected by a patent, '[r]eproduction of a functional attribute is legitimate competitive activity.'" *Id.* Some commentators have interpreted the *Bonito Boats* decision as "endow[ing] the competitor's right to reverse engineer with constitutional underpinnings." *See, e.g.*, J.H. Reichman, *Legal Hybrids Between the Patent and Copyright Paradigm*, 94 Colum. L. Rev. 2432, 2473 (1994).

DVD CCA is not the first litigant to attempt to enforce a mass-market license term forbidding reverse engineering or to base a trade secret claim on reverse engineering in breach of such a license term. In *Vault Corp. v. Quaid Software Ltd.*, 847 F.2d 255 (5th Cir. 1988),

---

[8] The cases upon which the Court principally drew were *Sears, Roebuck & Co. v. Stiffel Co.*, 376 U.S. 225 (1964) and *Compco Co. v. Day-Brite Lighting, Inc.*, 376 U.S. 234 (1964). In these cases the Court ruled that state unfair competition law could not be used to protect unpatentable designs from competitive copying because this would interfere with federal patent policy.

such claims were denied. Vault was the maker of the Prolok computer program who sued another software developer, Quaid, because the latter had reverse engineered Prolok and developed a program capable of bypassing the copy-protection feature of the Prolok program. Vault alleged copyright infringement (because of the intermediate copying of the Prolok program undertaken in the reverse engineering process), contributory copyright infringement (because users of Quaid's Ramkey program could make copies of programs protected by the Prolok copy-protection system), breach of a shrinkwrap license that forbade reverse engineering (in violation of Louisiana's specially enacted shrinkwrap enforcement law), and misappropriation of the trade secrets embedded in Prolok. The Fifth Circuit Court of Appeals decided that the copyright claims were without merit. It also decided that enforcement of the shrinkwrap license's anti-reverse engineering clause would conflict with federal copyright policy. *Id.* at 268-70. It did not need to reach the trade secret claim because Vault failed to appeal the trial court's ruling that reverse engineering was a proper means to obtain program trade secrets. *Id.* at 268. *See also Symantec Corp. v. McAfee Assocs.*, 1998

WL 740798 (N.D. Cal. 1998) (holding that a state unfair business practice claim based on the reverse engineering of another firm's program in violation of a license agreement was preempted by federal copyright law).

The federal intellectual property policy favoring reverse engineering of computer programs has become more pronounced since the *Vault v. Quaid* decision. In the landmark case *Sega Enters. Ltd. v. Accolade, Inc.*, 977 F.2d 1510 (9th Cir. 1992), the Ninth Circuit ruled that reverse engineering of copyrighted computer programs was a lawful way to get access to information embedded in the programs about interfaces necessary to achieving interoperability. By distributing game programs in object code form, Sega had hoped to maintain internal interface information as a trade secret (which it licensed to numerous game developers for the Genesis system). Accolade had considered becoming a Sega licensee, but decided against it because the Sega license would have required Accolade to forego making its programs available for other platforms. The only way Accolade could get access to the Sega interface information, and hence to develop programs that could interoperate with the Sega

Genesis machine, was to reverse engineer Sega programs. Sega sought to use copyright law to protect these trade secrets by asserting that the intermediate copies Accolade made of Sega game programs in the course of reverse engineering infringed its copyrights in the programs.

The Ninth Circuit rejected Sega's copyright claims, observing that

> [i]f disassembly of copyrighted object code is per se unfair use, the owner of the copyright gains a de facto monopoly over the functional aspects of his work—aspects that were expressly denied copyright protection by Congress [under Section 102(b) of the Copyright Act of 1976].

Id. at 1526. The court went on to note that "the fact that computer programs are distributed for public use in object code form often precludes public access to the ideas and functional concepts contained in those programs and thus confers on the copyright owner a de facto monopoly over those ideas and functional concepts. That result defeats the fundamental purpose of the Copyright Act—to encourage the production of original works by protecting the expressive aspects of those works while leaving the ideas, facts, and functional concepts in the public domain for others to build upon." *Id.* at 1527. To obtain

a legal monopoly on functional aspects of computer programs, the Ninth Circuit said Sega must seek a patent. *Id.* at 1526. Sega had not done so, and hence the court decided that its efforts to insulate its programs from reverse engineering should not succeed.[9]

The Ninth Circuit recently reaffirmed the *Sega v. Accolade* ruling in *Sony Computer Entertainment, Inc. v. Connectix Corp*., 203 F.3d 596 (9th Cir. 2000). Connectix had reverse engineered Sony programs in order to make software that would emulate the functionality of the Sony PlayStation, thereby enabling owners of Sony PlayStation games to run them on Apple computers, rather than reverse engineering to make compatible games for a platform, as Accolade did. The Ninth Circuit perceived no legally significant difference between these two cases because reverse engineering in

[9] Other federal intellectual property laws also protect reverse engineering. For example, the Semiconductor Chip Protection Act, 17 U.S.C. § 901 et seq., specifically privileges reverse engineering activities. *Id.* at § 906(a). The Plant Variety Protection Act, 7 U.S.C. § 2321 et seq., contains a research exemption that serves a similar function: "The use and reproduction of a protected variety for plant breeding or other bona fide research shall not constitute an infringement of the protection provided under this Act." *Id*. at § 2544. No reverse engineering right, as such, exists in patent law. However, the purchase of a product embodying the patented invention is generally free under the first sale principle of patent law to reverse engineer it. *See, e.g*., Julie E. Cohen and Mark A. Lemley, *Patent Scope and Innovation in the Software Industry*, 89 Calif. L. Rev. 1, 30-35 (2000).

both cases had been performed in order to achieve compatibility. Courts in other circuits have also followed the *Sega v. Accolade* ruling. *See, e.g., DSC Communications Corp. v. DGI Techs., Inc.*, 81 F.3d 597, 601 (5th Cir. 1996); *Bateman v. Mnemonics, Inc.*, 79 F.3d 1532, 1539 n.18 (11th Cir. 1996); *Mitel, Inc. v. Iqtel, Inc.*, 896 F.Supp. 1050, 1056-57 (D. Colo. 1995), *aff'd on other grounds*, 124 F.3d 1366 (10th Cir. 1997). *See also Atari Games Corp. v. Nintendo of Am., Inc.*, 975 F.2d 832 (Fed. Cir. 1992) (fair use to reverse engineer program to develop programs compatible with Nintendo console); *Secure Services Tech., Inc. v. Time & Space Processing, Inc.*, 722 F.Supp. 1354 (E.D. Va. 1989) (lawful to reverse engineer embedded software in secure facsimile machines for purposes of making competing, compatible facsimile machine). While many cases have involved reverse engineering for purposes of achieving interoperability, some have not. *See, e.g., E.F. Johnson Co. v. Uniden Corp. of Am.*, 623 F. Supp. 1485 (D. Minn. 1985) (reverse engineering to determine whether defendant's program infringed copyright).

The overwhelming majority of legal commentators endorse *Sega v. Accolade* and its progeny. *See, e.g.*, Jonathan Band and

Masanobu Katoh, *Interfaces on Trial: Intellectual Property and Interoperability in the Global Software Industry* (1995); *Brief Amicus Curiae of Eleven Copyright Professors, Sega Enters. Ltd. v. Accolade, Inc.*, 33 Jurimetrics J. 147 (1992); Julie E. Cohen, *Reverse Engineering and the Rise of Electronic Vigilantism: Intellectual Property Implications of 'Lock-out' Programs*, 68 S. Cal. L. Rev. 1091 (1995); Lawrence Graham & Richard O. Zerbe, Jr., *Economically Efficient Treatment of Computer Software: Reverse Engineering, Protection and Disclosure*, 22 Rutg. Comp. & Tech. L.J. 61 (1996); Dennis S. Karjala, *Copyright Protection of Computer Software, Reverse Engineering and Professor Miller*, 19 U. Dayton L. Rev. 975 (1994); Robert A. Kreiss, *Accessibility and Commercialization in Copyright Theory*, 43 UCLA L. Rev. 1 (1995); Ronald S. Laurie & Stephen M. Everett, *Protection of Trade Secrets in Object Form Software: The Case for Reverse Engineering*, Computer Law, at 1 (July 1984); Mark A. Lemley & David McGowan, *The Law and Economics of Network Effects*, 86 Calif. L. Rev. 479 (1998); Jessica Litman, *Copyright and Information Policy*, 55 Law & Contemp. Probs. 185, 196-201 (1992); Charles R.

McManis, *Intellectual Property Protection and Reverse Engineering of Computer Programs in the United States and the European Community*, 8 High Tech. L. J. 25 (1993); J.H. Reichman, *Computer Programs as Applied Scientific Know-How: Implications of Copyright Protection for Commercialized University Research*, 42 Vand. L. Rev. 639 (1989); David A. Rice, Sega *and Beyond: A Beacon for Fair Use Analysis…At Least As Far As It Goes*, 19 U. Dayton L. Rev. 1131 (1994); Pamela Samuelson, Randall Davis, Mitchell D. Kapor, & J.H. Reichman, *A Manifesto Concerning the Legal Protection of Computer Programs*, 94 Colum. L. Rev. 2308 (1994); Timothy Teter, Note, *Merger and the Machines: An Analysis of the Pro-Compatibility Trend in Computer Software Copyright Cases*, 45 Stan. L. Rev. 1061 (1993). Other countries have adopted similar rules. *See* Band and Katoh, *supra*, at 227-82 (discussing developments in the European Union, Eastern Europe, and Australia).[10]

[10] DVD-CCA is also incorrect in asserting that the Court of Appeal decision "threatens to put the United States in breach of one of its international trade agreements, the Agreement on Trade-Related Aspects of Intellectual Property Rights." DVD CCA Opening Brief on the Merits, p. 19. *See, e.g.*, Charles R. McManis, *Taking TRIPS on the Information Superhighway: International Intellectual Property Protection And Emerging Computer Technology*, 41 Vill. L. Rev. 207 (1996)

Legal commentators have also expressed strong reservations about enforcement of anti-reverse engineering clauses in mass-market software license agreements.[11] Some think such clauses should be rejected on copyright preemption grounds because they interfere with achieving the purposes of copyright law in enabling access to information that copyright does not protect. *See, e.g.*, Charles R. McManis, *The Privatization (or "Shrinkwrapping") of American Copyright Law*, 87 Calif. L. Rev. 173 (1999); David A. Rice, *Public Goods, Private Contract and Public Policy: Federal Preemption of Software License Prohibitions Against Reverse Engineering*, 53 U. Pitt. L. Rev. 543 (1992). Others have argued that such clauses should be preempted on patent policy grounds. *See, e.g.*, John E. Mauk, Note, *The Slippery Slope of Secrecy: Why Patent Law Preempts Reverse Engineering Clauses in Shrinkwrap Licenses*, 43 Wm. & Mary L. Rev. 819, 843 (2001). Some have asserted that such clauses

---

(arguing that reverse engineering of computer programs is acceptable within the TRIPS framework).

[11] A related question is whether parties can agree to restrictions on disclosure of information that is not a secret. *See, e.g.*, Restatement (Third) of Unfair Competition § 41, cmt. d at 89 (1995) ("A promise to refrain from the use or disclosure of commercial information is ordinarily unenforceable unless the information is sufficiently secret to justify the restraint.") (citing cases). *See also Sarkes Tarzian, Inc. v. Audio Devices, Inc.*, 166 F. Supp. 250, 265-66 (C.D. Cal. 1958).

should be considered a misuse of intellectual property rights. *See, e.g.*, Mark A. Lemley, *Beyond Preemption: The Law and Policy of Intellectual Property Licensing*, 87 Calif. L. Rev. 111, 129 (1999). Others have suggested enforcing such license terms in negotiated licenses, but not in non-negotiated standard form contracts. *See, e.g.*, David Nimmer, Elliot Brown, & Gary N. Frischling, *The Metamorphosis of Contract Into Expand*, 87 Calif. L. Rev. 17, 68 (1999); J.H. Reichman & Jonathan A. Franklin, *Privately Legislated Intellectual Property Rights: Reconciling Freedom of Contract With Public Good Uses of Information*, 147 U. Pa. L. Rev. 875, 939 (1999). Although purchasers of computer programs generally do not want to reverse engineer them and so might willingly agree to anti-reverse engineering clauses, the effect of enforcing such clauses would be socially harmful in the long run because it would impede third-party development of programs. *See, e.g.*, David McGowan, *Free Contracting, Fair Competition, and Article 2B: Some Reflections on Federal Competition Policy, Information Transactions, and "Aggressive Neutrality,"* 13 Berkeley Tech. L.J. 1173 (1998). *See also IEEE-USA Position on Reverse Engineering, at*

<http://www.ieeeusa.org/forum/POSITIONS/reverse.html> (November 1997) (explaining the fundamental importance of reverse engineering to the ongoing development of computer programs and taking a stance against the enforcement of mass market licenses purporting to override the right to reverse engineer).

The Superior Court's conclusion that breach of an anti-reverse engineering clause in a mass-market license is an improper means to obtain trade secret information in computer programs is unprecedented in American law. It undermines California's stated policy that reverse engineering is a proper means to acquire trade secrets from mass marketed products, and it runs counter to federal intellectual property policy. DVD CCA seems to believe that enforcing this mass-market license term and holding that breach of such a term is trade secret misappropriation is necessary to protect California's high technology industry. *See* DVD CCA Opening Brief on the Merits, at19. Quite the reverse is true.

The high technology industry, in California and elsewhere, depends on the continued ability to reverse engineer existing products. Without reverse engineering, it is impossible to make compatible

products and it may be very difficult to make competing products. Moreover, the high technology industry is not the only California industry with interests at stake in this case. It would be exceptionally harmful to many California industries if the California Supreme Court affirmed the Superior Court's issuance of a preliminary injunction in this case. If it did so, virtually any firm could state in the product packaging that by opening the package or using the product, the user had agreed not to reverse engineer the product. *See, e.g.*, John E. Mauk, Note, *The Slippery Slope of Secrecy: Why Patent Law Preempts Reverse Engineering Clauses in Shrinkwrap Licenses*, 43 Wm. & Mary L. Rev. 819, 847 (2001) (giving examples of the "slippery slope" of harmful consequences that would likely flow from enforcement of anti-reverse-engineering clauses of shrinkwrap licenses). This would have a devastating impact on competition and innovation in California.

The California Supreme Court should reject the underlying premise of DVD CCA's trade secret claim that breach of a mass-market license restriction on reverse engineering can constitute misappropriation of trade secrets. However, it should also recognize

that for it to do otherwise would starkly conflict with federal intellectual property law and policy. Averting such a conflict is yet another reason why the California Supreme Court should reject the underlying premise of DVD CCA's trade secret claim.

III. One Who Obtains Information Without Participating In Misappropriation Of A Trade Secret And Without Knowing Or Having Reason To Know Of Misappropriation Cannot Be Enjoined From Using Or Disclosing The Information On The Internet Or Otherwise.

Trade secret claims can be brought against misappropriators of trade secrets or those who obtained the secret from another when the recipient knew or had reason to know that the information was a trade secret and that the information was acquired by improper means or from someone under a duty not to disclose it. Cal. Civ. Code § 3426.1. In this section, Amici argue that Bunner cannot be held liable for trade secret misappropriation of CSS, even if Jon Johansen could have been, because Bunner was not a participant in the misappropriation, nor did he act in concert with a misappropriator. Furthermore, Bunner did not obtain DeCSS knowing of any trade secret misappropriation, nor had he reason to suspect this. *See, e.g.*,

Tenax Corp. v. Tensar Corp., 15 U.S.P.Q.2d (BNA) 1789 (D. Md. 1990) (discussing limits on third party liability for trade secret misappropriation). By the time Bunner obtained a copy of DeCSS, it had already been broadly disseminated on the Internet. *See DVD Copy Control Ass'n v. Bunner*, 93 Cal. App.4th 648, 652, 113 Cal. Rptr. 338, 341 ("Soon after its initial publication on the Internet, DeCSS appeared on numerous websites throughout the world"). There is, as a consequence, too much remoteness between Bunner and any act of misappropriation to hold him responsible for it. The correct principle can be succinctly 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." *Underwater Storage, Inc. v. United States Rubber Co.*, 371 F.2d 950, 955 (D.C. Cir. 1966). In our view, Bunner is part of the rest of the world, not the misappropriator nor a privy to misappropriation.[12]

The braggadocio expressed in Slashdot discussions—excerpts

[12] DVD CCA does not claim that Bunner was a party to a license agreement forbidding reverse engineering. License agreements, like trade secrecy law, do not create rights that are good against the world, but only rights that are good against the parties. *See, e.g.*, Robert P. Merges, *The End of Friction? Property Rights and Contract in the "Newtonian" World of On-Line Commerce*, 12 Berkeley Tech. L.J. 115 (1997).

of which were cleverly included in the DVD CCA complaint—may bespeak disrespect for the law, but the statements cannot be reasonably interpreted as conferring on Bunner knowledge that DeCSS was the result of stolen trade secrets.[13] It is more reasonable to impute to Bunner knowledge that the most pertinent caselaw and other authorities cited above regard anti-reverse engineering clauses of mass-market licenses as unenforceable because they undermine public policies that support reverse engineering of a mass-marketed product.[14]

---

[13] At most, the statements indicate awareness that posting DeCSS risked running afoul of the DMCA anti-circumvention rules. *See Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001) (posting DeCSS held to violate the DMCA rules). This is quite distinct from knowledge that DeCSS contained stolen trade secrets.

[14] Bunner's posting DeCSS on the Internet might have been challenged on other grounds. *See, e.g., Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001) (holding a journalist liable for posting DeCSS as a violation of the anti-circumvention rules of the Digital Millennium Copyright Act, 17 U.S.C. § 1201(a)(2)). Hence, if DVD CCA loses this trade secret case, as Amici believe it should, there may be other ways to seek the remedy sought in this case.

DVD CCA wrongly asserts that "[t]rade secret law is founded on the core principle that businesses will not invest money, labor, or equipment in an effort to create innovations that cannot be copyrighted or patented if trade secrecy law does not fill the gap to enable them to profit from their labors." DVD CCA Opening Brief on the Merits, at 15-16. Trade secret law is not a general-purpose gap-filler law. As Sections I and II have shown, trade secrecy law is limited in scope by design, and its consistency with federal intellectual property law depends on preservations of these limitations. Nor can the grave weaknesses in DVD CCA's trade secret claims be overcome by DVD CCA's expressions of concerns that the posting of DeCSS on the Internet by Bunner and others might facilitate copyright infringements. *Id.* at 15. Trade secret law is designed to protect trade secrets, not all intellectual property rights. It is no more proper for trade secret law to be stretched to protect copyrights than it is for copyright law to be stretched to protect trade secrets, as Sega sought to do in the *Accolade* case. *See Sega Enters. Ltd. v. Accolade, Inc.*, 977 F.2d 1510 (9th Cir. 1992).

Among the failed trade secret cases that resembles *Bunner* is *Religious Technology Center, Inc. v. Lerma,* 908 F. Supp. 1362 (E.D. Va. 1995). Religious Technology Center (RTC) claims copyright and trade secret interests in certain texts that the Church of Scientology uses in its religious practices. RTC sued the *Washington Post* and two of its reporters for copyright infringement and trade secret misappropriation based on the *Post*'s duplication of documents containing the alleged trade secrets and publication of portions of the RTC texts in a newspaper. The information had been available in unsealed court records as an appendix to an affidavit in a California courthouse for more than two years, notwithstanding RTC's efforts to maintain its trade secret status by sending agents to the courthouse to block others from getting access to the documents. The documents had also been posted on the Internet for ten days. *Id*. at 1368. It is worth noting that the *Post* knew that RTC claimed this information as a trade secret and, in fact, returned to RTC's lawyers a document that RTC alleged had been stolen. However, the *Post* was able to obtain another copy of the document from a court clerk in California. "Although *The Post* was on notice that the RTC made certain

proprietary claims about these documents, there was nothing illegal," said the court, "about *The Post* going to the Clerk's Office for a copy of the documents or downloading them from the Internet." *Id*. at 1369. *See also Cabot Corp. v. Thai Tantalum, Inc.*, 25 U.S.P.Q.2d (BNA) 1619 (Del. Ch. 1992) (denying preliminary injunction where the plaintiff sought to impute knowledge of misappropriation to non-misappropriating defendant based upon its knowledge of a lawsuit initiated against alleged misappropriator).

Because the information had been available in open court records and posted on the Internet, the court ruled that it was no longer a trade secret, saying: "Once a trade secret is posted on the Internet, it is effectively part of the public domain, impossible to retrieve. Although the person who originally posted a trade secret on the Internet may be liable for trade secret misappropriation, the party who merely downloads Internet information cannot be liable for misappropriation because there is no misconduct involved in

interacting with the Internet." *Lerma*, 908 F. Supp. at 1368.[15] *See also Religious Technology Center v. F.A.C.T.NET*, 901 F. Supp. 1519, 1526 (D. Colo. 1995) (rejecting similar trade secret misappropriation claims against a website critical of the Church of Scientology because information from these texts had already been "made available on the Internet through persons other than Lerma, with the potential for downloading by countless users"); *Religious Technology Center v. Netcom On-line Commun. Servs., Inc.*, 923 F. Supp. 1231, 1256 (N.D. Cal. 1995) ("Although Ehrlich cannot rely on his own improper postings to support the argument that the Church's documents are no longer secrets…, evidence that another has put the alleged trade secrets in the public domain prevents RTC from further enforcing its trade secret rights in those materials.").

Given the specific facts of the *Lerma* case, the District Court was correct in ruling that the public availability of information had destroyed RTC's trade secret claim. However, Amici believe that

[15] Although the court in *Lerma* did not invoke the First Amendment in support of its ruling, its application of limiting principles of trade secrecy law comported with the First Amendment interests of the *Washington Post*, its reporters, and readers eager to know about Scientology practices.

posting information on the Internet should not automatically cause it to cease to be a protectable trade secret. If, for example, information is posted on an obscure site and its presence on the Internet is detected quickly, a trade secret owner may be able to obtain a court order to remove the information from that Internet site and to enjoin reposting of it.

Such an outcome is consistent with other trade secret cases in which, for example, lawyers initially failed to seek a court order to seal documents containing trade secrets as part of court filings but realized this promptly and thereafter sought a protective order. Just because the document might have been, in theory, publicly accessible for a short period of time does not necessarily mean it has lost its trade secret status, particularly if very few persons have actually seen the information. *See, e.g., Gates Rubber Co. v. Bando Chemical Indus., Ltd*., 9 F.3d 823, 849 (10th Cir. 1993) (inadvertent and inconsequential disclosures of trade secret at trial and short delay in sealing court records did not cause loss of trade secret status).

However, the longer information is available on the Internet, the more sites where it is available, the larger the number of people

who have accessed the information, the farther word has spread about the availability of the information (e.g., through newsgroups or in chatrooms), the greater is the likelihood that trade secret status will be lost. This is unfortunate, of course, but there is always an inherent risk in relying upon trade secrecy law that the information will leak out, particularly where the information is susceptible to being reverse engineered.

In issuing a preliminary injunction in the *Bunner* case, the Superior Court worried that not enjoining defendants from posting of DeCSS would "encourage misappropriators 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. Such a holding would not be prudent in this age of the Internet." *DVD Copy Control Ass'n v. McLaughlin*, 2000 WL 48512 at 3 (Cal. Super. Ct. 2000). Amici agree that that the Internet poses risks for trade secret claimants—as indeed it poses for many others (e.g., copyright owners and children who may be exposed to harmful materials)—but these risks are not so grave that courts should distort trade secret law to make the rules stricter in cyberspace than in other realms.

There have, in fact, been relatively few instances of trade secret misappropriation via the Internet. The trial court opinion below is the only case of which Amici are aware in which the posting of alleged trade secrets on the Internet has been enjoined. One reason why trade secrecy status is so rarely lost via the Internet is because misappropriators of trade secrets typically do not want to publish the secrets to the world (as would generally occur by Internet publication), but rather to exploit the secret for their own commercial purposes. Moreover, the caselaw is clear that a trade secret misappropriator cannot escape liability simply by posting secrets on the Internet. *See, e.g*., *Lerma*, 908 F. Supp. at 1368. Firms can take a number of steps to protect trade secrets from Internet misappropriation. *See, e.g.*, David G. Majdali, Note, *Trade Secrets Versus the Internet: Can Trade Secret Protection Survive the Internet?*, 22 Whittier L. Rev. 125, 145-55 (2000); Ryan Lambrecht, Note, *Trade Secrets and the Internet: What Remedies Exist for Disclosure in the Information Age*, 18 Rev. Litig. 317, 339-40(1999). A significant deterrent to publication of trade secrets on the Internet is the potential for criminal prosecution under the Economic Espionage

Act. *See* 18 U.S.C. § 1343 (Supp. 1998). *See also* Lambrecht, *supra*, 18 Rev. Litig. at 361-62 (discussing criminal sanctions for trade secret misappropriation).

Thus, the dangers of lost trade secrets on the Internet, while substantial, are not as great as some commentators have feared. *See, e.g.*, Bruce T. Adkins, *Trading Secrets In the Information Age: Can Trade Secret Law Survive the Internet?*, 1996 U. Ill. L. Rev. 1151 (1996) (emphasizing risks to trade secrets on the Internet). They are certainly not so great as to require courts to be more liberal in issuing broad injunctions than traditional principles would call for. Traditional limiting principles of trade secrecy law, as well as First Amendment considerations, support this conclusion, as applied to this case.

CONCLUSION

For all of the foregoing reasons, Amici law professors, CCIA and USACM respectfully request the California Supreme Court to affirm the Court of Appeal's decision.

Respectfully submitted,

_____

Jennifer M. Urban (Bar No. 209845)
Samuelson Law, Technology and
Public Policy Clinic
University of California at Berkeley
School of Law (Boalt Hall)
396 Simon Hall
Berkeley, CA 94720-7200
(510) 642-7561

Dated: July 10, 2002

APPENDIX A

AMICI LAW PROFESSORS

Stephen R. Barnett
Elizabeth Josselyn Boalt Professor of Law
University of California at Berkeley School of Law

Margreth Barrett
Professor of Law
University of California Hastings College of Law

Yochai Benkler
Professor of Law
New York University School of Law

James Boyle
Professor of Law
Duke Law School

Dan L. Burk
Julius E. Davis Professor of Law 2001-2002
University of Minnesota

Julie E. Cohen
Professor of Law
Georgetown University Law Center

Rochelle C. Dreyfuss
Pauline Newman Professor of Law
New York University

Dennis S. Karjala
Willard Pedrick Distinguished Research Scholar and Professor of Law
Arizona State University

David L. Lange
Professor of Law
Duke Law School

Mark Lemley
Professor of Law
University of California at Berkeley School of Law

Lawrence Lessig
Professor of Law
Stanford Law School

Jessica Litman
Professor of Law
Wayne State University

R. Anthony Reese
Assistant Professor of Law
School of Law, The University of Texas at Austin

Jerome H. Reichman
Bunyan S. Womble Professor of Law
Duke University School of Law

Pamela Samuelson
Chancellor's Professor of Law and Information Management
University of California at Berkeley School of Law

Jonathan Zittrain
Assistant Professor of Law
1525 Massachusetts Ave
Cambridge, MA 02138

CERTIFICATE OF COMPLIANCE

I certify that this brief complies with the type-volume limitation of the California Rules of Court Rule 14(c)(1).

Exclusive of the exempted portions in California Rules of Court Rule 14(c)(3), the brief contains 8323 words.

Jennifer M. Urban (Bar No. 209845)
Samuelson Law, Technology and
Public Policy Clinic
University of California at Berkeley
School of Law (Boalt Hall)
396 Simon Hall
Berkeley, CA 94720-7200
(510) 642-7561

Dated: July 11, 2002

PROOF OF SERVICE

I, Rhaman Serbellon, certify and declare as follows:

I am over the age of 18 years, and not a party to this cause and employed in the county where the mailing took place. My business address is Center for Clinical Education, University of California at Berkeley School of Law (Boalt Hall), 396 Simon Hall, Berkeley, CA 94720-7200, which is located in Alameda County.

On July 11, 2002, I served the following document(s):

BRIEF AMICI CURIAE OF INTELLECTUAL PROPERTY LAW PROFESSORS, THE COMPUTER & COMMUNICATIONS INDUSTRYASSOCIATION, AND THE UNITED STATES PUBLIC POLICY COMMITTEE OF THE ASSOCIATION FOR COMPUTING MACHINERY, SUPPORTING AFFIRMANCE

by placing a true copy thereof in a sealed envelope and served to each party herein by overnight delivery via Federal Express to:

Court of Appeal of the State of California
Sixth Appellate District
Attn: Mr. Willy Magsaysay
333 West Santa Clara Street
Suite 1060
San Jose, CA 95113

Santa Clara County Superior Court
Attn: Hon. William S. Elfving
191 North First Street
San Jose, CA 95113-1090

Attorneys for Petitioner, DVD Copy Control Association, Inc.:

Jared Bobrow
Christopher J. Cox
WEIL, GOTSHAL & MANGES LLP
201 Redwood Shores Parkway
Redwood Shores, CA 94065

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

Attorneys for Respondent, Andrew Bunner:

James R. Wheaton
David Green
First Amendment Project
1736 Franklin Ave., 9th Floor
Oakland, CA 94612

Thomas E. Moore, III
Tomlinson Zisko Morosoli & Maser LLP
200 Page Mill Road, 2nd Floor
Palo Alto, CA 94306

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

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

Attorneys for Amicus Curiae:

Edward J. Black
Computer & Communications Industry Association
666 Eleventh Street, NW
Washington, D.C. 20001

Howard M. Freedland
American Committee for Interoperable Systems
901 San Antonio Road
M/S PAL 1-521
Palo Alto, CA 94303-4900

Annette L. Hurst
Institute of Electrical Engineers, Inc.
Howard, Rice, Nemerovski, Canady, Falk & Rabkin
Three Embarcadero Center, 7th Floor
San Francisco, CA 94111-4065

David E. Kendall
Thomas G. Hentoff
Suzanne H. Woods
Julia B. Shelton
Williams & Connolly LLP
725 Twelfth Street, NW
Washington, D.C. 20005

I certify and declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct and that this declaration was executed at Berkeley, Alameda County, California, on July 11, 2002.

_____

Rhaman Serbellon