H021153

COURT OF APPEAL OF THE STATE OF CALIFORNIA FOR THE SIXTH APPELLATE DISTRICT

DVD COPY CONTROL ASSOCIATION, INC.,

Plaintiff and Respondent,

vs.

ANDREW BRUNNER,

Defendant and Appellant.

Appeal from the Superior Court of California, County of Santa Clara
Honorable William J. Elfving, Presiding Judge
Case No. CV-789804

BRIEF AMICI CURIAE OF AMERICAN COMMITTEE FOR INTEROPERABLE SYSTEMS AND COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION IN SUPPORT OF APPELLANT ANDREW BRUNNER

Edward J. Black
COMPUTER & COMMUNICATIONS
INDUSTRY ASSOCIATION
666 Eleventh Street, NW
Washington, DC 20001
(202) 783-0070
Internet: eblack@ccianet.org

Howard M. Freedland, Bar No. 142341
Counsel of Record
AMERICAN COMMITTEE FOR
INTEROPERABLE SYSTEMS
901 San Antonio Road
M/S PAL 1-521
Palo Alto, CA 94303-4900
(650) 336-0493
Internet: howard.freedland@sun.com

Dated: June 28, 2000

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

STATUTES

OTHER AUTHORITIES

INTEREST OF AMICUS

The American Committee for Interoperable Systems ("ACIS") is an informal organization of companies that develop innovative software and hardware products that interoperate with computer systems developed by other companies.[1] Computer & Communications Industry Association ("CCIA") members participate in many sectors of the computer, software, Internet, and telecommunications industry and range in size from small entrepreneurial firms to the largest in the industry.[2]

---

[1] The following companies have joined ACIS by subscribing to the ACIS Statement of Principles: Accolade, Inc., Advanced Micro Devices, Inc., Amdahl Corporation, America Online, Inc., Berkeley Software Design, Inc., Broderbund Software, Inc., Bull HN Information Systems, Inc., Clearpoint Research Corporation, Color Dreams, Inc., Comdisco, Inc., Emulex Corporation, Forecross Corporation, The Fortel Group, Fujitsu Systems Business of America, Inc., Hitachi Data Systems, ICTV, Insignia Solutions, Johnson-Laird, Inc., Landmark Systems Corporation, LCS/Telegraphics, MidCore Software, Inc., NCR Corporation, New York Systems Exchange, Inc., Passage Systems, Inc., Phoenix Technologies, Ltd., Plimoth Research Inc., QAD Inc., Seagate Technology, Inc., Software Association of Oregon (consists of over 550 software development firms, firms in associated industries, and individuals professionally involved in software development), Software Forum (consists of over 1,000 software entrepreneurs and developers), Storage Technology Corporation, Sun Microsystems, Inc., 3 Com Corporation, Tandem Computers, Trilium Consumer Electronics, Inc., TriTeal, Western Digital Corporation, and Zenith Data Systems Corporation.

[2] CCIA members include: Amdahl Corporation, AT&T Corporation, Bell Atlantic Corporation, Block Financial Corporation, CAI/SISCo, Cerebellum Software, Inc., Commercial Data Servers, Inc., Datum, Inc., E-Stamp Corp., Entegrity Solutions Corporation, Fantasma Networks,Fujitsu Limited, Giga Information Group, Government Sales Consultants, Inc., Hitachi Data Systems,

ACIS and CCIA members believe that computer programs deserve effective intellectual property protection to give developers sufficient incentive to create new programs. At the same time, ACIS and CCIA are concerned that improper extension of intellectual property law will impede innovation and inhibit fair competition in the computer industry.

ACIS and CCIA have long supported interpreting the intellectual property laws to permit reverse engineering performed to develop interoperable products. Both ACIS and CCIA filed *amicus* briefs with the U.S. Court of Appeals for the Ninth Circuit in *Sega Enterprises, Ltd. v. Accolade, Inc.*, 977 F.2d 1510 (9th Cir. 1992), which held that the reverse engineering technique known as disassembly was a fair use as a matter of law when it was the only way to obtain functional elements such as the information necessary for achieving interoperability. ACIS and CCIA also filed an amicus brief with that court in *Sony Computer Entertainment, Inc., v. Connectix Corp.*, 203 F.3d 596 (9th Cir. 2000), which affirmed its earlier holding in *Sega*.

Neither ACIS, CCIA, nor their members have a direct financial interest in the outcome of this litigation. However, affirmance of the Superior Court's

---

Inc., Intuit, Inc., MERANT, Mercator, NetCom Solutions International, Inc., NOKIA, Nortel Networks, Novak Biddle Venture Partners, NTT America, Inc., Okidata, Oracle Corporation, SABRE Inc., Sun Microsystems, Inc., Tantivy Communications, Inc., Telesciences, Inc., Time Domain Corporation, US West, Viatel, Inc., ViON Corporation, and Yahoo! Inc.

decision would have serious anti-competitive consequences for ACIS and CCIA members and the computer industry as a whole. The Superior Court ruled that a click-on license for a mass market product renders reverse engineering an improper means of acquiring a trade secret. Because of the prevalence of click-on or shrink-wrap licenses, this ruling would outlaw software development processes used every day in Silicon Valley and throughout the world.[3]

ARGUMENT

In issuing the preliminary injunction, the court below concluded that the DVD Copy Control Association (DVD CCA) was likely to prevail on the merits of its trade secrets claim. This conclusion, in turn, involved a finding that the DVD CCA was likely to prove that Jon Johansen acquired the trade secret at issue by improper means.[4] Johansen acquired the CSS algorithm and master keys by reverse engineering CSS. The court below correctly noted that in the legislative comment to California's Uniform Trade Secrets Act, "'[d]iscovery by reverse engineering, that is, by starting with the known product and working backwards to find the method by which it was developed,' is considered a proper

[3] ACIS and CCIA take no position on the First Amendment issues in this case.

[4] For purposes of this brief, ACIS and CCIA assume that the Content Scrambling System (CSS) algorithm and master keys qualify as trade secrets under the California trade secret law, Cal. Civ. Code §3426.1 (West 2000).

means." *DVD Copy Control Ass'n, Inc., v. McLaughlin*, Case No. C 786804, Order Granting Preliminary Injunction (Cal. Super. Ct. January 21, 2000). The court went on to state that "the only way in which the reverse engineering could be considered 'improper means' herein would be if whoever did the reverse engineering was subject to the click license agreement which preconditioned installation of DVD software or hardware, and prohibited reverse engineering." *Id.* Using the terminology of the Uniform Trade Secrets Act, the reverse engineering could be an improper means of acquiring the trade secret only if it was in "breach of a duty to maintain secrecy" created by the click-on license.

The court below determined that DVD CCA was likely to show that Johansen clicked on the license, that the license created a duty to maintain secrecy, and that Johansen breached that duty by reverse engineering CSS. In this brief, ACIS and CCIA challenge that second finding -- that the click-on license created a duty to maintain secrecy. A click-on license for a mass market product, such as a DVD, *cannot* create a duty to maintain secrecy. Such a legal rule would conflict with the fundamental principle of trade secret law that one can acquire a trade secret by reverse engineering. If one could prevent reverse engineering with a click-on license in a mass market product, the reverse engineering privilege would have no utility, and the scope of trade secret could expand without limit. The manufacturer of every product -- be it software, soft

drinks, or spark plugs -- could prevent competitive research by distributing the product subject to a shrink-wrap or click-on confidentiality agreement.

This brief first addresses the importance of reverse engineering to the computer industry. It then explains how jurisdictions throughout the United States and around the world have specifically permitted software reverse engineering. The ruling of the court below would completely undermine this strong public policy favoring reverse engineering. Next, the brief demonstrates that the court's ruling conflicts with provisions of California trade secret law and is preempted by the Intellectual Property Clause of the U.S. Constitution. Finally, the brief argues that reversal will not prejudice any legitimate interests of the DVD CCA or the creators of other copyrighted content.

Before proceeding any further, we must stress that we are *not* arguing that a software firm can never prohibit reverse engineering by contract. If a truly confidential relationship is established between two parties, such as when one company is *beta* testing a product for another company, then breach of a license restriction on reverse engineering could constitute a breach of a duty to maintain secrecy. But when a product is widely distributed to the general public, we believe that a click-on license cannot create a duty to maintain secrecy; one cannot bind the world to secrecy.

Furthermore, ACIS and CCIA take no position on Mr. Johansen's motives for reverse engineering the CSS algorithm or Mr. Brunner's motives for posting DeCSS. We do not know whether these activities were directed at fostering Linux interoperability or facilitating copyright infringement. For purposes of the narrow legal issue addressed in this brief -- whether a click-on license for a mass market product can create a duty to maintain secrecy -- Mr. Johansen's and Mr. Brunner's motives have no relevance.

I. SOFTWARE REVERSE ENGINEERING IS CRITICAL TO COMPETITION AND INNOVATION IN THE COMPUTER INDUSTRY

In most copyright industries, there is little relation between intellectual property protection and competition. A film producer, for example, has no justification and little motivation for copying from another film (except in certain special cases, such as parody).

Software, however, is different. Unlike a film or novel, which stands by itself, a computer program can function only in conjunction with hardware and other software. For example, an application program, such as a word processor, must work together with an operating system in order to perform its task; otherwise, it is a useless set of magnetic impulses. Two software products can work together—*interoperate*—only if they conform to the same set of rules, or *interface specifications*.

If a company could exercise proprietary control over the interface specifications implemented by its software, that company could determine which products made by other firms could interoperate with its software. And should that company have a dominant position in a particular market, it could use its control over interoperability to drive competitors from that market or to expand its dominant position into adjacent markets.

Such a broad monopoly would have serious implications for consumer welfare.[5] In the absence of competition during the effective lifespan of the product, the first developer would have little incentive to develop more innovative and less costly products. These negative consequences would be compounded by the fact that the personal computer revolution and the emergence of the Internet have produced an overwhelming need for interconnection between different elements of computer systems. Within a given large corporation, literally thousands of personal computers and workstations scattered across the globe need to interact with each other and with the company's mainframes. Moreover, with the advent of the Internet, users around the world need to exchange vast quantities of data through their computers.[6] Prohibiting

---

[5] *See, e.g.,* Peter S. Menell, *An Analysis of the Scope of Copyright Protection for Application Programs*, 41 Stan. L. Rev. 1045, 1082, 1097 n.281 (1989).

[6] *See* President's Information Infrastructure Task Force, *Global Information Infrastructure: Agenda for Cooperation* (U.S. Government Printing Office, Washington, D.C., Feb. 1995) at 14-16.

competitors from accessing the *de facto* standard interface specifications would lock users into a particular operating system or network software environment, and would inhibit the transfer of data between users with different computing environments.[7]

It should be stressed that interoperable products are *not* mere "clones" that offer only the same functionality as the products of the first comer, but at a lower price. While interoperable products must offer at least the same functionality, they typically offer additional features or modifications not found in the first comer's products. Thus, they compete with the first comers' products not only in terms of price (indeed, sometimes the interoperable products may be more expensive), but also in terms of innovation. In this respect, interoperable developers' use of preexisting interface specifications is a transformative use of the sort accredited by the Supreme Court in *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569 (1994).

In short, in the software industry, overly broad intellectual property protection directly restricts competition. For this reason, U.S. courts in recent years have held that interface specifications fall on the idea (or unprotected) side

[7] *See Lotus Dev. Corp. v. Borland Int'l.*, 49 F. 3d 807, 821 (1st Cir. 1995), *aff'd by an equally divided Court*, 516 U.S. 233 (1996) (J. Boudin, concurring).

of copyright's idea/expression dichotomy.[8] Significantly, the U.S. Government took this position in its case against Microsoft.[9]

But even though the interface specifications are not protected by copyright, a company seeking to interoperate must still learn what those interface specifications are. Because computer programs typically are distributed to the public in a form readable only by computers, a program's interface specifications usually are not readily apparent. In some instances, the developer of the program may be willing to provide the interface information to other companies. All too often, however, developers are not willing to provide the information, or the information they provide is tardy, incomplete, or under exceedingly restrictive terms.[10]

In these cases, the companies seeking to develop interoperable products have no choice but to perform painstaking research on the original program to

---

[8] *See, e.g., Computer Assocs. Int'l v. Altai, Inc.*, 982 F.2d 693 (2d Cir. 1992); *Lotus Dev. Corp. v. Borland Int'l, Inc.*, 49 F.3d 807 (1st Cir. 1995), *aff'd by an equally divided Court,* 516 U.S. 233 (1996); *Mitel, Inc. v. Iqtel, Inc.*, 124 F.3d 1366 (10th Cir. 1997); *Sega*, 977 F.2d at 1524-25; Jonathan Band & Masanobu Katoh, *Interfaces on Trial*, 131-146 (1995); 1 Paul Goldstein, Copyright § 2.15.2.1-2.15.2.2 (2d ed. 1998).

[9] *See* Jonathan Band & Taro Isshiki, *Peace at Last? Executive and Legislative Branch Endorsement of Recent Software Copyright Case Law*, Computer Lawyer, Feb. 1999 at 1.

[10] *See, e.g.,* Jeanette Bozo, *Bristol Has June 1 Date for Microsoft Lawsuit,* InfoWorld Daily News, Jan. 4, 1999; Richard Wolffe, *FTC says Intel Lawsuit 'Vital to Stop Abuse',* Financial Post, June 18, 1998 at 19.

discern the interface specifications. This research, known as *reverse engineering*, is a basic tool of software product development. Without reverse engineering, interoperability can be difficult, if not impossible, to achieve.

II. JURISDICTIONS THROUGHOUT THE WORLD HAVE ADOPTED EXCEPTIONS PERMITTING SOFTWARE REVERSE ENGINEERING

Software firms typically treat the interface specifications of their programs as trade secrets. However, as noted above, trade secret law universally recognizes reverse engineering as a proper means of acquiring a trade secret. *E.g., Kewanee Oil Co. v. Bicron Corp.,* 416 U.S. 470 (1974). Thus, trade secret law generally poses no impediment to software reverse engineering.

At the same time, copyright law has the potential of raising obstacles to software reverse engineering. Because of the nature of computer technology, software reverse engineering almost always requires the making of a reproduction or derivative work. For example, the reverse engineering method known as *disassembly* involves "translating" the publicly distributed, computer readable program into a higher level, human readable form. In another method referred to as *black box reverse engineering*, an engineer observes a program's behavior and interaction with its environment while executing the program on a

computer.[11] The computer automatically copies the program into the computer's random access memory (RAM) in order to run it.

Since the Ninth Circuit's 1992 decision in *Sega v. Accolade*, no less than five U.S. courts have permitted reproduction during the course of software reverse engineering under the "fair use doctrine."[12] Other courts have prevented enforcement under a copyright misuse theory.[13]

Moreover, the Digital Millennium Copyright Act (DMCA), the legislation enacted by Congress in 1998 to implement the World Intellectual Property Organization Copyright and Performances and Phonograms Treaties, permits the circumvention of technological protections for the purpose of engaging in software reverse engineering. 17 U.S.C. § 1201(f).[14] Citing *Sega*, the Senate

---

[11] Engineers refer to this method as black box reverse engineering because the externally visible characteristics of the program are observed without looking into the program itself; the actual contents of the program remain unknown.

[12] *Atari Games Corp. v. Nintendo of America, Inc.*, 975 F.2d 832 (Fed. Cir. 1992); *Bateman v. Mnemonics, Inc.*, 79 F.3d 1532 (11th Cir. 1996); *DSC Communications Corp. v. DGI Techs.*, 898 F. Supp. 1183 (N.D. Tex. 1995), *aff'd*, 81 F.3d 597 (5th Cir. 1996); *DSC Communications Corp. v. Pulse Communications, Inc.*, 976 F. Supp. 359 (E.D. Va. 1997), *aff'd in part, rev'd in part, and vacated in part,* 170 F.3d 1354 (Fed. Cir. 1999); *Sony Computer Entertainment, Inc. v. Connectix Corp.*, 203 F.3d 596 (9th Cir. 2000).

[13] *DSC Communications Corp. v. DGI Techs.*, 81 F.3d 597 (5th Cir. 1996); *Alcatel U.S.A., Inc. v. DGI Techs., Inc.*, 166 F.3d 772 (5th Cir. 1999).

[14] *See also* note 9, *supra*.

Judiciary Committee Report states that this exception is "intended to allow legitimate software developers to continue engaging in certain activities for the purpose of achieving interoperability to the extent permitted by law prior to the enactment of this chapter."[15] The Report adds that the exception's objective is "to foster competition and innovation in the computer and software industry."[16]

Similarly, the 1991 European Union Software Directive contains a specific exception for software reverse engineering.[17] The Directive has been implemented throughout the European Union, as well as in the European Free Trade Association countries and throughout Eastern and Central Europe.[18] Thus, both the United States and the European Union have recognized the central role reverse engineering plays in maintaining legitimate competition in the computer industry.

---

[15] S. Rep. No. 105-190, at 13 (1998).

[16] *Id.*

[17] Council Directive 91/250/EEC on the Legal Protection of Software Programs, Articles 5 and 6 (May 14, 1991), O.J. No. L122/42,44 (May 17, 1991).

[18] *See Interfaces on Trial* at 258-62.

Pacific Rim countries also share this recognition. Within the past three years, Australia, Hong Kong, Singapore, and the Philippines have amended their copyright laws to permit software reverse engineering.[19]

Congress, numerous U.S. courts, and foreign legislatures have all determined that public policy strongly favors software reverse engineering. The ruling below would allow that public policy to be erased by one click on a boilerplate license for a mass market product.

III. A "CLICK-ON" PROHIBITION AGAINST REVERSE ENGINEERING OF A MASS MARKET PRODUCT DOES NOT, BY ITSELF, RENDER REVERSE ENGINEERING AN IMPROPER MEANS OF ACQUIRING A TRADE SECRET

The United States Supreme Court in *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 476 (1974), stated that "trade secret law ... does not offer protection against discovery by fair and honest means, such as ... by so called reverse engineering, that is by starting with the known product and working backwards to divine the process which aided its development or manufacture." Similarly, California's implementation of the Uniform Trade Secret Law specifically added the following sentence to the definition of "improper means:" "Reverse engineering or independent derivation alone shall not be considered

[19] Ord. No. 92 of 1997 (H.K.); Copyright (Amendment) Bill of 1998 (Sing.); Republic Act 8293 of 1996 (Phil.); Copyright Amendment (Computer Programs) Bill of 1999 (Austl.).

improper means." Cal. Civ. Code §3426.1(a) (West 2000). Since trade secret misappropriation consists of acquiring a trade secret by improper means, Section 3426.1(b), reverse engineering by itself cannot constitute trade secret misappropriation.

Reverse engineering can be converted into a trade secret misappropriation if the product being reverse engineered was not lawfully acquired, or if the reverse engineering occurred in breach of an express or implied relationship of confidence.[20] Thus, there is little doubt that a court would properly enforce a negotiated agreement prohibiting the reverse engineering of a narrowly distributed product. In that circumstance, the contract clearly creates a duty to maintain secrecy, which the licensee breaches by reverse engineering.

This case presents an altogether different circumstance. Here, the confidential relationship purportedly was established by means of a click-on license that appears on a user's screen when a user installs widely distributed DVD software in his computer. ACIS and CCIA submit that in this situation, a confidential relationship has not been established and thus the reverse engineering does not constitute trade secret misappropriation under California law. Further, if it did constitute trade secret misappropriation, it would be preempted by federal law.

---

[20] *See* 1 Roger M. Milgrim, Milgrim on Trade Secrets §1.05[5] at 1-244 (2000).

A. The Click On License Did Not Establish a Duty to Preserve Secrecy Within the Meaning of the California Trade Secret Law.

At the outset, it must be noted that it is unclear whether clicking on an "I agree" icon creates a binding contract. Courts around the country have just begun to consider the enforceability of click-on and shrink-wrap licenses, and a consensus has not yet emerged. [21] Moreover, numerous commentators have questioned the enforceability of such contracts. [22]

---

[21] *Compare Step-Saver Data Sys. v. Wyse Tech.*, 939 F.2d 91, 98-100 (3d Cir. 1991); *Novell, Inc. v. Network Trade Ctr., Inc.*, 25 F. Supp. 2d 1218, 1234-1230 (D. Utah 1997); *Morgan Labs., Inc. v. Micro Data Base Sys., Inc.* 41 U.S.P.Q.2d 1850 (N.D. Cal. 1997); *Arizona Retail Sys., Inc. v. The Software Link, Inc.*, 831 F. Supp. 759, 764-66 (D. Ariz. 1993); *and Foresight Resources Corp. v. Pfortmiller*, 719 F. Supp. 1006, 1010 (D. Kan. 1989); *with ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447, 1449 (7th Cir. 1996); *cf. Hill v. Gateway 2000, Inc.*, 105 F.3d 1147, 1150 (7th Cir. 1997), *cert. denied*,.118 S. Ct, 47 (1997).

[22] *E.g.*, Michael J. Madison, "*Legal Ware: Contract and Copyright in the Digital Age*," 67 Fordham L. Rev 1025 (1998); Apik Minassian, *The Death of Copyright: Enforceability of Shrinkwrap Licensing Agreements*, 45 UCLA L. Rev. 569 (1997); Jason Kuchmay, Note, *ProCD, Inc. v. Zeidenberg: Section 301 Copyright Preemption of Shrinkwrap Licenses - A Real Bargain for Consumers?*, 29 U. Tol. L. Rev. 117 (1997); Kell Corrigan Mercer, Note, *Consumer Shrink-Wrap Licenses and Public Domain Materials: Copyright Preemption and Uniform Commercial Code Validity in ProCD v. Zeidenberg*, 30 Creighton L. Rev. 1287 (1997); Robert J. Morrill, Comment, *Contract Formation and the Shrink Wrap License: A Case Comment on ProCD, Inc. v. Zeidenberg*, 32 New Eng. L. Rev. 513, 537-50 (1998); Christopher L. Pitet, Comment, *The Problem With "Money Now, Terms Later": ProCD, Inc. v. Zeidenberg and the Enforceability of "Shrinkwrap" Software Licenses*, 31 Loy. L.A. L. Rev. 325 (1997); Stephen P. Tarolli, Comment, *The Future of Information Commerce Under Contemporary Contract and Copyright Principles*, 46 Am. U. L. Rev. 1639 (1997); Mark A. Lemley, *Intellectual Property and Shrinkwrap Licenses*, 68 S. Cal. L. Rev. 1239, 1248-59 (1995); L. Ray Patterson & Stanley W. Lindberg, *The Nature of Copyright* 220 (1991).

The National Conference of Commissioners of Uniform State Laws in 1999 adopted the Uniform Computer Information Transactions Act (UCITA), which generally renders click-on licenses enforceable. So far, only Maryland and Virginia have adopted UCITA.[23] Several states began considering UCITA but tabled it because it was too controversial.[24] Indeed, Iowa enacted legislation expressly rejecting UCITA.[25]

Even if UCITA were considered to accurately articulate the state of the law regarding the enforceability of click-on licenses, the enforceability under UCITA of the license at issue here is still suspect in two respects. First, UCITA establishes procedural requirements for click-on licenses in the mass-market context. *See* UCITA §209. The record is unclear whether those procedural requirements were met here. Second, the Reporter's notes to Section 105(b) specifically refer to contract terms prohibiting reverse engineering as an example

---

[23] H.B. 19, 414th Leg. Sess. (Md. 2000); S.B. 372, 2000 Leg. Sess. (Va. 2000). Jaikumar Vijayan, *UCITA*, Computerworld, June 5, 2000 at 72.

[24] Kevin Washington, *Software Licensing Foes See Route to Harm*, Baltimore Sun, June 19, 2000 at 1C. UCITA and its earlier incarnation, draft Article 2B of the Uniform Commercial Code, have been criticized as too pro-licensor by the American Law Institute, the staff of the Federal Trade Commission, and the Attorneys-General of 24 states, including California. *Id.*

[25] H.B. 2205, 78th Leg., 2d Sess. (Iowa 2000). Cliff Edwards, *Debate Hot Over Legislation In States Over Software Licensing*, Chattanooga Times, June 4, 2000 at G9.

of the kind of term which may be unenforceable under UCITA because it violates a "fundamental public policy." UCITA Final Comments at 20 (March 2000).

Assuming *arguendo* that clicking the "I agree" icon formed an enforceable contract, the specific term prohibiting reverse engineering did not establish a duty to maintain secrecy in the meaning of the California Uniform Trade Secrets Act. It appears from the record that a license similar to the one at issue here is included in virtually all DVD products distributed to the general public. If the license in fact established a duty to maintain secrecy, millions of DVD purchasers would be bound to secrecy, and would have entered into a confidential relationship with members of the DVD CCA.

This, of course, is an absurd result that could not have been contemplated by the California legislature when it enacted the Uniform Trade Secrets Act. *See* Milgrim on Trade Secrets §1.05[5] at 1-245-48. Under this reasoning, Coca-Cola could prevent reverse engineering by Pepsi-Cola by printing on the side of a Coke can that anyone who flips open the lid agrees not to reverse engineer the formula for Coca-Cola. Similarly, Honda could prohibit reverse engineering by General Motors by including a statement in the owners' manual that anyone who opens the hood agrees not to reverse engineer the engine.

Further, such a broad interpretation of the California trade secret law would render ineffective two other provisions of the trade secret law. First, as

noted above, the statute expressly states that "reverse engineering or independent derivation alone shall not be considered improper means." Cal. Civ. Code §3426.1(a) (West 2000) 3426.1(a). If one can render reverse engineering improper simply by attaching a click-on license to a mass market product, this provision is a nullity.

Second, "trade secret" is defined as information that "[i]s the subject of efforts that are reasonable under the circumstances to maintain its secrecy." Cal. Civ. Code §3426.1(d)(2) (West 2000). If one can impose a duty to maintain secrecy on all purchasers of a mass market product, this provision also become a nullity. If everyone in the world knows a secret, it is no longer a secret, even though everyone has "promised" to keep it secret.

None of the cases cited by DVD CCA as supporting the court's ruling on the improper nature of the reverse engineering are on point. In none of the cases did a court find that the reverse engineering of a mass market product was improper because of a shrink-wrap or click-on restriction on reverse engineering. Indeed, one of the cases demonstrates how far the court below and DVD CCA have strayed from fundamental trade secret principles.

Alcatel U.S.A., Inc. v. DGI Techs., 166 F.3d 772 (5th Cir. 1999), concerned operating systems and microprocessor cards for telecommunications switches -- sophisticated equipment marketed to telecommunications companies.

The plaintiff, DSC, developed both operating systems and microprocessor cards. The defendant, DGI, developed microprocessor cards compatible with the DSC operating system. To ensure compatibility between its cards and the DSC operating system, DGI had to reverse engineer the DSC operating system. The only way DGI could obtain a DSC operating system was to deceive a customer to which DSC had licensed the operating system pursuant to a confidentiality agreement. It was this theft of the DSC operating system that contaminated DGI's subsequent reverse engineering.

In other words, the instant case could not be more different from *Alcatel*. Alcatel involved sophisticated products licensed to a small number of companies in the telecommunications market. This case, by contrast, involves products sold to the mass market. In *Alcatel*, the reverse engineer obtained the target product by duplicity. Here, there is no evidence in the record to suggest that the reverse engineer obtained the DVD by improper means; DVDs are readily obtainable in thousands of retail outlets throughout the world.

Interestingly, DVD CCA neglects to mention the one true similarity between *Alcatel* and this case: an overreaching license agreement. To use the DGI cards, a customer had to install the DSC operating system in the cards' memory. The DSC license agreement with its customers, however, prohibited the running of the DSC operating system on non-DSC cards. The jury found that

DSC's license agreement constituted copyright misuse, and the Fifth Circuit agreed with its finding: "DSC has used its copyright to indirectly gain commercial control over products DSC [has] not copyrighted, namely its microprocessor cards." *Alcatel,* 166 F.3d at 793.

In an earlier related case, the Fifth Circuit similarly concluded that "DSC seems to be attempting to use its copyright to obtain a patent-like monopoly over unpatented microprocessor cards."[26] The Court reasoned,

> Any competing microprocessor card developed for use on DSC phone switches must be compatible with DSC's operating system software. In order to ensure that its card is compatible, a competitor such as DGI must test the card on a DSC phone switch. Such a test necessarily involves making a copy of DSC's copyrighted operating system, which copy is downloaded into the card's memory when the card is booted up. If DSC is allowed to prevent such copying, then it can prevent anyone from developing a competing microprocessor card, even though it has not patented the card.[27]

Likewise, this Court should not allow DVD CCA to use -- or misuse -- its license to impose a duty of secrecy on the world.

---

[26] *DSC,* 81 F.3d at 601.

[27] *Id.*

B. The Ruling Below Is Preempted by the Federal Intellectual Property System.

The Superior Court's interpretation of California trade secret law also conflicts with the federal intellectual property system, and thus is preempted.[28] This constitutional preemption, based on the U.S. Constitution's Supremacy Clause, Article VI, and its Intellectual Property Clause, Article I, Section 8, occurs either when the federal and state laws directly conflict, so that it is physically impossible for a party to comply with both, or when a state law "stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress." *California Fed. Sav. & Loan Ass'n v. Guerra*, 479 U.S. 272, 281 (1987).[29]

The Constitution's Intellectual Property Clause empowers Congress to establish copyright and patent regimes; the ruling below conflicts with both. The leading case treating constitutional preemption under the copyright laws is *Goldstein v. California*, 412 U.S. 546 (1973). In that case, the Supreme Court

---

[28] The DVD CCA presumably is pursuing this case under a trade secret theory rather than a contract theory in order to secure relief against parties not in contractual privity with DVD CCA. Had DVD CCA pursued a breach of contract claim, the preemption arguments set forth below would have applied with equal force.

[29] In *ProCD, Inc., v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996), the Seventh Circuit found that Section 301(a) of the Copyright Act did not preempt enforcement of a shrink-wrap license prohibiting the copying of telephone listings. The *ProCD* court, however, did not consider the issue of constitutional preemption.

considered whether the Copyright Act of 1909, then in force, preempted state protection for subject matter not included within that Act. In deciding that such state copyright rules were not preempted, the Court distinguished three types of situations — areas in which federal law mandated protection, areas in which federal law mandated no protection, and areas in which federal law was silent:

> Where the need for free and unrestricted distribution of a writing is thought to be required by the national interest, the Copyright Clause and the Commerce Clause would allow Congress to eschew all protection. In such cases, a conflict would develop if a State attempted to protect that which Congress intended to be free from restraint or to free that which Congress had protected. However, where Congress determines that neither federal protection nor freedom from restraint is required by the national interest, it is at liberty to stay its hand entirely.

Goldstein, 412 U.S. at 559. In resolving the constitutional preemption question regarding reverse engineering, therefore, a court must decide whether allowing a click-on license to prevent the reverse engineering of a mass market product would have the effect of protecting that which the copyright laws intended to be free from restraint.

It clearly would. The copyright laws are not unrestricted grants of property rights. Rather, copyright strikes a delicate balance between the rights of various parties with an interest in copyrighted material.[30] While the Copyright

---

[30] *Twentieth Century Music Corp. v. Aiken,* 422 U.S. 151,156 (1975); 1 Paul Goldstein, *Copyright: Principles, Law, and Practice* 1.14, at 1:40 (1995).

Act provides a series of exclusive rights to copyright owners in 17 U.S.C. § 106, many other provisions of the Act (notably 17 U.S.C. § 102(b) and 17 U.S.C. §§ 107-120) expressly create certain user privileges in copyrighted material.

Courts have interpreted these privileges as permitting the reverse engineering of software to learn the information necessary to achieve interoperability. Indeed, the *Sega* court explained that reverse engineering furthered the public policy of the Copyright Act. A legal prohibition on the reverse engineering of programs would:

> preclude[] public access to the ideas and functional concepts contained in those programs, and thus confer[] 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 elements of those works while leaving the ideas, facts, and functional concepts in the public domain for others to build on.

Sega, 977 F.2d at 1527.

In this passage, the Ninth Circuit echoes the Supreme Court's teachings in *Feist,* where the Court explained why a compilation of phone book information could not receive protection:

> It may seem unfair that much of the fruit of the compiler's labor may be used by others without compensation. As Justice Brennan has correctly observed, however, this is not 'some unforeseen byproduct of a statutory scheme.' It is, rather, 'the essence of copyright,' and a constitutional requirement. The primary objective of copyright is not to reward the labor of authors, but 'to promote the Progress of Science and useful Arts.' To this end, copyright assures authors the right to their

> original expression, but encourages others to build freely upon the ideas and information conveyed by a work.... *This result is neither unfair nor unfortunate. It is the means by which copyright advances the progress of science and art.*

Feist Publications, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 349-50 (1991) (emphasis added; citations omitted).

Similarly, as noted above, Congress created exceptions to the Digital Millennium Copyright Act's prohibition on circumvention of technological protections specifically to permit the reverse engineering permitted by *Sega.* The Senate Judiciary Committee Report on the Act stated the exception was "intended to allow legitimate software developers to continue engaging in certain activities ... to the extent permitted by law" so as "to foster competition and innovation in the computer and software industry." S. Rep. No. 105-190, at 13 (1998).

Interpreting state trade secret law as allowing software vendors to impose terms that prohibit reverse engineering of mass-market products would frustrate the policy of encouraging the creation of new, interoperable software products. Not surprisingly, the one reported decision to consider the issue squarely found that federal copyright law preempts state laws enforcing contractual restrictions on reverse engineering. *Vault Corp. v. Quaid Software Ltd.*, 847 F.2d 255 (5th Cir. 1988), examined the enforceability of a state statute that expressly validated shrinkwrap license terms precluding users from reverse engineering computer

since 1992, the collapse of the software industry has yet to occur. To the contrary, the software industry remains extremely robust.

Harvard's Professor Arthur Miller similarly called the Ninth Circuit's recognition in *Sega* of a privilege to reverse engineer computer programs "singularly ill-suited to vindicating the public interest." Arthur R. Miller, *Copyright Protection for Computer Programs, Databases, and Computer-Generated Works: Is Anything New Since CONTU?*, 106 Harv. L. Rev. 977, 1020 (1993). Again, despite widespread adoption in the courts of such a reverse engineering privilege, the public interest seems alive and well. As discussed above, Congress has explicitly endorsed this privilege as necessary "to foster competition and innovation in the computer and software industry."

There is no reason to believe that reversal of the unprecedented ruling below will do any serious damage to the thriving computer industry. To the contrary, we believe that such a reversal will maintain competitive conditions in the industry and thereby prevent "monopolistic stagnation." [32] *Altai*, 982 F.2d at 696.

Any concerns the DVD CCA has with respect to motion pictures is similarly misplaced. Even if the reverse engineering here is not considered a

---

[32] Indeed, since 1991 the European Union has expressly prohibited contractual restrictions on reverse engineering, to no ill effect. *See Interfaces on Trial* at 246, 255.

programs. Relying on the constitutional preemption cases, the Fifth Circuit refused to enforce the term because it "conflicts with the rights of computer program owners under [17 U.S.C.] § 117 and clearly 'touches upon an area' of federal copyright law." *Id.* at 270. *See also* Milgrim on Trade Secrets §1.05[5] at 1-247-48.

In similar fashion, the Second Circuit in *Wright v. Warner Books, Inc.*, 953 F.2d 731, 741 (2d Cir. 1991), ruled that a contractual restriction on a biographer's use of a manuscript in a library would offend the fair use privilege of the Copyright Act. The court found that "[t]o read [the restriction] as absolutely forbidding any quotation, no matter how limited or appropriate, would severely inhibit proper, lawful scholarly use and place an arbitrary power in the hands of the copyright owner going far beyond the protection provided by law." By the same token, permitting a click-on license to prohibit reverse engineering would place an arbitrary power in the hands of the software developer.

This arbitrary power would also interfere with the operation of the federal patent system. *Bonito Boats, Inc. v. Thunder Craft Boats, Inc.,* 489 U.S. 141 (1989), concerned a Florida statute that prohibited the unauthorized use of a direct molding process to replicate manufactured boat hulls. The Supreme Court in a unanimous decision held that the statute conflicted with the federal patent law and thus was invalid under the Supremacy Clause. The Court stated that "the

States may not offer patent-like protection to intellectual property creations which would otherwise remain unprotected as a matter of federal law." *Id.* at 156. The Court further stated that "[i]n essence, the Florida law prohibits the entire public from engaging in a form of reverse engineering of a product in the public domain." *Id.* at 160. The Court concluded that "the efficient operation of the federal patent system depends upon substantially free trade in publicly known, unpatented design and utilitarian conceptions." *Id.* at 156.

Like the Florida statute, allowing a click-on license to prohibit software reverse engineering would "offer patent-like protection to intellectual property creations which otherwise would remain unprotected as a matter of federal law." *Id.* at 156. The utilitarian interface specifications could not be used by competitors even though the specifications had not endured the rigors of a patent examination and been found to meet the statutory requirements of novelty and nonobviousness. Similarly, the click-on license would prohibit millions of licensees "from engaging in a form of reverse engineering of a product" distributed to the general public. *Id.* at 160. Without question, such restrictions would interfere with the "free trade" in publicly distributed, "unpatented . . . utilitarian conceptions," and thereby impede the "efficient operation of the federal patent system." *Id.* at 156. Accordingly, "the *Bonito Boats* decision strongly suggests that federal patent law is an alternative to federal copyright law

for preempting both state legislation and judicial cases that uphold the enforceability" of contractual restrictions on software reverse engineering.[31]

IV. REVERSING THE RULING BELOW WILL NOT UNDERMINE INCENTIVES FOR THE DEVELOPMENT OF COPYRIGHTED WORKS

It can be anticipated that the DVD CCA will contend that reversing the ruling below will expose the motion picture industry specifically, and all copyrighted works more generally, to rampant piracy. This is not the first time we have heard such predictions from the copyright industries. Indeed, there seems to be a pattern of predicting dire consequences whenever courts place any limit on intellectual property protection.

For example, when the Second Circuit in 1992 adopted in *Computer Association v. Altai* a less expansive interpretation of copyright protection for computer programs than prior courts had done, two IBM lawyers called the decision "a legal Chernobyl" and warned that it would surely destroy the software industry. Anthony L. Clapes & Jennifer M. Daniels, *Revenge of the Luddites: A Closer Look at Computer Associates v. Altai*, 9 Computer Law., Nov. 1992, at 11. Despite unanimous adoption of the Second Circuit's approach

---

[31] Charles R. McManis, *Intellectual Property Protection and Reverse Engineering of Computer Programs in the United States and the European Community*, 8 High Tech. L. 25, 94 (1993). *See* Steven W. Lundberg & John P. Sumner, *Patent Preemption of Shrink-Wrap Prohibitions on Reverse Engineering*, 4 Computer Law., Apr. 1987.

trade secret violation, the motion picture industry still has at least three lines of defense. First, and most obviously, it can continue to pursue its claims in federal court under the anti-circumvention provisions of the Digital Millennium Copyright Act. As this court is aware, a federal district court in New York has already concluded that the motion picture industry is likely to succeed in its DMCA claims and on this basis entered a preliminary injunction against the posting of DeCSS. Reversal of the ruling below on the grounds discussed in this brief will have absolutely no impact on the DMCA case in New York.

Second, the motion picture industry will be able to bring a copyright action against any person who uses DeCSS to make an unlawful reproduction of a motion picture. Similarly, the motion picture industry can bring a contributory copyright infringement action against anyone who produces or distributes DeCSS, provided the industry can show that DeCSS has no substantial non-infringing use. Again, reversal of the ruling below will in no way prejudice the motion picture industry's ability to pursue these remedies.

Third, the DVD CCA can employ more powerful security measures than CSS. By contemporary standards, CSS is a very weak form of protection. Indeed, several ACIS and CCIA members have developed far more powerful encryption systems, which they would be happy to license to the DVD-CCA.

In sum, reversal of the ruling below will not expose the copyright industries in general, and the motion picture industry in particular, to widespread theft. They still will have numerous legal and technological defenses at their disposal.

V. CONCLUSION

For the foregoing reasons, ACIS and CCIA respectfully request the Court to reverse the ruling below.

Respectfully submitted,

Howard M. Freedland, Bar No. 142341
Counsel of Record
AMERICAN COMMITTEE FOR
INTEROPERABLE SYSTEMS
901 San Antonio Road
M/S PAL 1-521
Palo Alto, CA 94303-4900
(650) 336-0493
Internet: howard.freedland@sun.com

Edward J. Black
COMPUTER & COMMUNICATIONS
INDUSTRY ASSOCIATION
666 Eleventh Street, NW
Washington, DC 20001
(202) 783-0070
Internet: eblack@ccianet.org

Dated: June 28, 2000