UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF KENTUCKY
AT LEXINGTON
CIVIL ACTION NO. 02-571-KSF

LEXMARK INTERNATIONAL, INC. PLAINTIFF

vs. **BRIEF AMICUS CURIAE OF COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION**

STATIC CONTROL COMPONENTS, INC. DEFENDANT

* * * * * * * *

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

STATUTES

OTHER AUTHORITIES

INTEREST OF AMICUS

Computer & Communications Industry Association ("CCIA") members participate in many sectors of the computer and telecommunications industry and range in size from small entrepreneurial firms to the largest in the industry.[1] CCIA members believe that computer programs deserve effective intellectual property protection to give developers sufficient incentive to create new programs. At the same time, CCIA is concerned that improper extension of intellectual property law will impede innovation and inhibit fair competition in the computer industry.

CCIA has long supported interpreting the intellectual property laws to permit reverse engineering performed to develop interoperable products. CCIA filed an *amicus* brief 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. CCIA also filed an *amicus* brief with that court in *Sony Computer Entertainment, Inc. v. Connectix Corp,* 203 F.3d 596 (9th Cir), *cert denied* 531 U.S. 831 (2000), which affirmed its earlier holding in *Sega*. Additionally, when Congress was considering the Digital Millennium Copyright Act (DMCA), CCIA advocated the inclusion of an

[1] CCIA's current roster of members is available at: www.ccianet.org/membership.php3#members

exception permitting circumvention of technological measures during the course of reverse engineering pursued for the purpose of achieving interoperability.

Neither CCIA nor its members have a direct financial interest in the outcome of this litigation. However, an improper interpretation of the DMCA's reverse engineering exception could have serious anticompetitive consequences for CCIA members and the computer industry as a whole.[2]

ARGUMENT

This brief first addresses the importance of interoperability to the computer industry. It then explains how jurisdictions throughout the United States and around the world have specifically permitted reverse engineering, a process essential to the development of interoperable products. Next, the brief discusses the reverse engineering exception inserted by Congress into the DMCA to promote interoperability. This exception appears to absolve Static Control Components from liability under §1201 of the DMCA. For that reason, this Court should deny Lexmark International Inc.'s (Lexmark) motion for preliminary injunction with respect to counts II and III of the complaint.

I. INTEROPERABILITY 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

[2] CCIA takes no position on first count of the complaint.

justification and little motivation for copying from another film (except in certain special cases, such as parody).

The nature of computer products, however, is different. Unlike a film or novel, which stands by itself, a computer product 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 computer 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 products, that company could determine which products made by other firms – if any -- 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 expand its dominant position into adjacent markets. Moreover, such authority would extend the rights under copyright beyond what is necessary to protect the original expressive elements that have traditionally been offered protection under American copyright law.

Such a broad monopoly would have serious implications for consumer welfare.[3] In the absence of competition during the effective lifespan of the product, the first developer would have little incentive to develop more

[3] *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).

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

It should be stressed that interoperable products often are *not* mere "clones" that offer only the same functionality as the products of the first comer, but at a lower price. Even interoperable products that offer similar functionality as the original product typically offer additional features 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

[4] *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.

expensive), but also in terms of innovation. Furthermore, many other products that interoperate with other copyrighted products do not mimic the functionality of the original product at all, but fulfill entirely different purposes or needs. In many cases – such as with a computer operating system and applications – these new products rely on the underlying program as a platform. In these respects, 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 computer industry, overly broad intellectual property protection directly restricts competition and innovation. For this reason, U.S. courts in recent years have held that interface specifications fall on the idea (or unprotected) side of copyright's idea/expression dichotomy.[5] Significantly, the U.S. government took this position in its case against Microsoft.[6]

---

[5] *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).

[6] Jonathan Band & Taro Isshiki, *Peace at Last? Executive and Legislative Branch Endorsement of Recent Software Copyright Case Law*, Computer Lawyer, Feb. 1999 at 1. Additionally, the D.C. Circuit condemned in harsh terms Microsoft's attempt to justify anticompetitive actions by asserting its right to use its intellectual property as it saw fit, so long as its intellectual property rights were lawfully obtained. *United States v. Microsoft Corp*., 253 F.3d 34, 63 (D.C. Cir. 2001) (*per curiam*) ("That is no more correct than the proposition that use of one's personal property, such as a baseball bat, cannot give rise to tort liability.").

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 or incomplete.[7]

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

The U.S. Supreme Court has long recognized that there is nothing inherently wrong with studying a competitor's product to understand how it works and to figure out how to make a better product. Thus, in *Kewanee Oil Co v. Bicron Corp.* 416 U.S. 470, 476 (1974), the Court stated that "trade secret

[7] 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.

law … does not offer protection against discovery by fair and honest means, such as … by so-called reverse engineering, that is by starting with a known product and working backward to divine the process which aided in its development or manufacture."

The Court has also recognized the benefits of reverse engineering: "Reverse engineering … often leads to significant advances in technology." *Bonito Boats, Inc., v. Thunder Craft Boats, Inc*., 489 U.S. 141, 160 (1989). Further, the Court has noted that "the competitive reality of reverse engineering may act as a spur to the inventor, creating an incentive to develop inventions that meet the rigorous requirements of patentability." Id.

Copyright law, however, 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.[8]

[8] 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.

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."[9] Other courts have prevented enforcement under a copyright misuse theory.[10]

Similarly, the 1991 European Union Software Directive contains a specific exception for software reverse engineering.[11] The Directive has been implemented throughout the European Union, as well as in the EFTA countries and throughout Eastern and Central Europe.[12] 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.

---

[9] *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., v. Connectix*, 203 F.3d 596 (9th Cir.), *cert. denied*, 531 U.S. 871 (2000).

[10] *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).

[11] 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).

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

Pacific Rim countries share this recognition. Recently, Australia, Hong Kong, Singapore, and the Philippines have all amended their copyright laws to permit software reverse engineering.[13]

III. SECTION 1201(f) OF THE DMCA PERMITS CIRCUMVENTION FOR THE PURPOSE OF ACHIEVING INTEROPERABILITY

Section 1201 of the DMCA, passed by Congress in October, 1998, implements the provisions of the World Intellectual Property Organization Internet Treaties relating to technological protection measures. Specifically, Section 1201 restricts the development, distribution, and use of technologies that circumvent other technologies that protect an author's copyrights. While the DMCA was pending before Congress, developers of interoperable computer products, including CCIA, explained to Congress that the act of reverse engineering – the uncovering of the interface specifications – could be viewed as a circumvention of a technological protection measure. Moreover, the incorporation of these specifications in competitive products could run afoul of the DMCA's prohibition on the manufacture and distribution of circumvention technologies. This would particularly be the case when a company placed a software "lock" on a program that prevented access to the program, and the competitor circumvented that software lock to achieve interoperability. Thus, Section 1201 could prevent a developer of interoperable products from exercising his fair use privileges recognized in *Sega* and its progeny.

---

[13] 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.).

Accordingly, Congress created an exception explicitly directed at the development of interoperable products. Section 1201(f) allows software developers to circumvent technological protection measures in a lawfully obtained computer program in order to identify the elements necessary to achieve interoperability of an independently created computer program with other programs. A person may engage in this circumvention only if the elements necessary to achieve interoperability are not readily available and the reverse engineering is otherwise permitted under the copyright law.[14] Furthermore, a person may develop, distribute, and employ the means to circumvent technological protection measures for the purpose of achieving interoperability. Section 1201(f), therefore, provides a complete defense to Section 1201 liability to qualifying developers of interoperable products. It also provides a defense to users of these products.[15]

The Senate Judiciary Committee report on the DMCA explains the policy underlying Section 1201(f). It states that this exception was "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."[16] The Committee evidently understood that if a company placed on its

---

[14] 17 U.S.C. § 1201(f) (1998).

[15] Section 1201(f) provides an exception to all the prohibitions of Section 1201: Section 1201(a)(1)'s prohibition on the circumvention of access controls, Section 1201(a)(2)'s prohibition on the manufacture and distribution of devices which circumvent access controls, and Section 1201(b)'s prohibition on the manufacture and distribution of devices which circumvent copy controls

[16] S. Rep. 105-190 at 32 (1998).

program a technological measure that prevented interoperability, a legal prohibition on circumventing that technological protection could preclude other companies from developing products capable of operating in that company's computing environment. Citing *Sega*, the Committee states that "[t]he objective is to ensure that the effect of current case law interpreting the Copyright Act is not changed by enactment of this legislation for certain acts of identification and analysis done in respect of computer programs."[17] The Committee concludes by noting that "[t]he purpose of this section is to foster competition and innovation in the computer and software industry."[18]

CCIA obviously is not familiar with the technical details of the products at issue in this case. However, based on the allegations in the complaint, Static Control Components (SCC) appears to qualify for the Section 1201(f) exception. Lexmark controls access between its Toner Loading Program and its Printer Engine Program by means of an undisclosed authentication sequence. SCC evidently reverse engineered the Lexmark programs to learn the authentication sequence, and then programmed its chips to mimic the sequence. By mimicking the authentication sequence, the program in the SCC chip can interoperate with the Lexmark Toner Program.

Congress intended Section 1201(f) to permit precisely this sort of activity. Section 1201(f)(1) provides that notwithstanding subsection 1201(a)(1), a person "may circumvent a technological measure that effectively controls access to a particular portion of that program for the sole purpose of identifying and analyzing those elements

---

17 *Id.*

18 *Id.*

of the program that are necessary to achieve interoperability of an independently created computer program with other programs…." This provision permits SCC to reverse engineer the Lexmark Toner Loading and Printer Engine programs to learn the authentication sequence so that SCC's independently created program embedded in its chip can interoperate with the Printer Engine Program.

Further, subsection 1201(f)(2) provides that notwithstanding subsection 1201(a)(2) – the subsection Lexmark alleges SCC to have violated – "a person may develop and employ technological means to circumvent a technological measure … for the purpose of enabling interoperability of an independently created computer program with other programs, if such means are necessary to achieve such interoperability…." Subsection 1201(f)(3) then provides that these means "may be made available to others … solely for the purpose of enabling interoperability…." These provisions permit SCC to manufacture its chip that mimics the authentication sequence, and to distribute it to manufacturers of toner cartridges. By Lexmark's own admission, the authentication sequence is necessary for achieving interoperability, and SCC mimicked it so that its chips could interoperate with Lexmark's Print Engine Program.[19]

Lexmark seeks to apply Section 1201 in a manner not intended by Congress. As the Senate Judiciary Committee report makes abundantly clear, Section 1201 is aimed at

[19] The only other limit subsection 1201(f)(2) places on the manufacture and distribution of the means of circumvention are is that such manufacture and distribution do not infringe copyright. As discussed above, courts have found that copyright does not protect interface specifications. Thus, SCC would infringe Lexmark's copyright, and lose 1201(f)2) immunity, only if it copied more of Lexmark's work than necessary to achieve interoperability.

preventing the dissemination of infringing copies of works over the Internet, because the threat of such dissemination will cause "copyright owners to hesitate to make their works readily available on the Internet…."[20] By providing additional protection for works, Section 1201 "creates the legal platform for launching the global digital online market for copyrighted works. It will also make available via the Internet the movies, music, software, and literary works that are the fruit of American creative genius."[21] Significantly, Congress did not intend for Section 1201 to be used to prevent competition in the toner cartridge market, or any other element of a computer system. This court should employ Section 1201(f) to prevent Lexmark from manipulating Section 1201 to lock its printer customers into purchasing Lexmark toner cartridges.

[20] Sen. R. 105-190 at 8.

[21] Id. at 2.

IV. CONCLUSION

Interoperability is critical to competition in the computer industry. In turn, reverse engineering and subsequent use of the interface specifications learned through reverse engineering are critical to achieving interoperability. Congress inserted a reverse engineering exception into the DMCA to insure that the prohibition of circumvention of technological protection measures did not interfere with interoperability. The court should not interpret and apply the reverse engineering exception in a manner that frustrates Congress's intent. Therefore, CCIA respectfully request the Court to deny Lexmark's motion for preliminary injunction with respect to counts II and III.

Respectfully submitted,

January 31, 2003

Jason M. Mahler
COMPUTER & COMMUNICATIONS
INDUSTRY ASSOCIATION
666 Eleventh Street, NW
Washington, DC 20001
(202) 783-0070
Internet: jmahler@ccianet.org