Before the
COPYRIGHT OFFICE, LIBRARY OF CONGRESS
Washington, D.C. 20024-0400

Exemption to Prohibition of Copyright Protection Systems For Access Control Technologies	)	RM Docket No. 2002-4A

COMMENTS OF THE COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION

Exemptions to Section 1201(a) Proposed by Static Control Components
March 10, 2003

The Computer & Communications Industry Association (CCIA) appreciates the opportunity to submit the following comments in response to the Copyright Office's February 10, 2003 notice of inquiry entitled "Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies." We write to urge the Copyright Office to add the exception as articulated in the notice.

CCIA is an association of electronic commerce, Internet, telecommunications, computer and software companies ranging from small, entrepreneurial companies to some of the largest in the industry. CCIA's members include equipment manufacturers, software developers, telecommunications and online service providers, resellers, systems integrators, and third-party vendors. Its member companies employ well over a half-million employees and generate annual revenues exceeding $300 billion.

At the outset, we note our historical involvement in the area of intellectual property. CCIA has long maintained the need for a balance in copyrights. While all our members use the protections afforded by intellectual property rights, we have witnessed the expansive use of intellectual property to unnecessarily foreclose competition. As such, we have interjected ourselves into the legislative and judicial process to advocate pro-competitive and economically justified exceptions to the copyright laws, such as those that permit reverse engineering for the purpose of achieving interoperability. In *Sega Enterprises, Ltd v. Accolade, Inc.,* 977 F.2d 1510 (9th Cir. 1992) and *Sony Computer Entertainment, Inc. v. Connectix Corp*, 203 F.3d 596 (9th Cir. 2000), Ninth Circuit agreed that reverse engineering was a fair use, a position CCIA advanced in *amicus* briefs.. More recently, CCIA participated in the negotiations that led to the reverse engineering exception codified at Section 1201(f) of the Digital Millennium Copyright Act (DMCA).

CCIA strongly believes that the exemptions requested by Static Control Components (SCC) should be granted. The policy issues raised by "unauthorized" access to software embedded in hardware are completely different from those raised by "unauthorized" access to software and other copyrighted works that are distributed separately from hardware. When it enacted Section 1201(a) of the DMCA, Congress assumed that when a person tried to obtain unauthorized access to a technologically protected "stand-alone" copyrighted work, the person was trying to obtain access to that work without payment, or was trying to access the work in a manner that could harm the copyright owner – i.e., by a device that could make serial copies of the work. If the person had paid for the work, or obtained the appropriate complementary device that protected the interests of the copyright owner, the person would have received the password or the decryption algorithm necessary to access the work.

In short, the copyright owner's objective when employing an access control to a stand-alone work was presumably to protect the market for the copyrighted work. Likewise, Congress's objective when prohibiting the circumvention of such access controls was protection of the market for the copyrighted work, in essence preserving the value of the limited monopoly granted by the copyright. In particular, Congress sought to

protect the *online* market for copyrighted works. As the Senate Judiciary Committee report makes abundantly clear, Section 1201 was aimed at preventing the dissemination of infringing copies of works over the Internet, because the threat of such dissemination would cause "copyright owners to hesitate to make their works readily available on the Internet…."[1] 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."[2]

Congress's objectives with respect to stand-alone works do not apply with respect to embedded software. When the copyright owner controls access to embedded software, his objective typically is not to protect the market for the software, but rather to protect the market for the hardware in which the software is embedded, or other hardware components controlled by the software. Thus, applying Section 1201 to the circumvention of access controls to embedded software would have the effect of restricting competition in replacement parts in a wide range of products from automobiles to weapon systems. It would in no way promote the development of an online market for the embedded software or any other copyrighted work. It would just lock consumers into purchasing parts from the original equipment manufacturer.

In some instances, the circumvention of access controls to embedded software might be permitted by Section 1201(f), which allows acts of circumvention, and the manufacture of circumvention devices, necessary to achieve interoperability. However, Section 1201(f) is worded narrowly, and might not permit circumvention in all appropriate cases. For example, it might be construed to permit circumvention to achieve interoperability between two software elements, but not between software and hardware.

Thus, to eliminate any chilling effect on the market for replacement parts, an exemption should be granted for the three classes proposed in SCC's petition. Significantly, granting the petition would not leave the owner of the copyright in the embedded software vulnerable to massive copyright infringement. Because the software is embedded in hardware, it cannot be easily copied; it must first be extracted from the hardware. Moreover, any copying that does occur would still be subject to the Copyright Act.

Allowing for interoperability has always been a positive policy choice. The competitive harm resulting from closed systems that lack interoperability are great. Preventing other market entrants from developing and supplying components that interoperate denies consumers the pricing and innovation advantages that derive from a competitive marketplace. A manufacturer may be free, to the extent permitted by the antitrust laws, to employ "secret handshakes" and other access controls to embedded software in an effort to frustrate competition. The Digital Millennium *Copyright* Act,

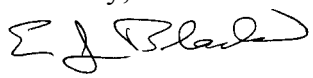
---

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

[2] Id. at 2.

however, should not be applied in a manner that makes competition in replacement parts impossible by preventing a rival from engaging in activity that infringes no copyright. Such a scheme does nothing to protect copyright but merely gives legal force to anticompetitive efforts by the copyright owner to extend his lawful copyright monopoly into adjacent markets

Sincerely,



Edward J. Black
President,
The Computer and Communications Industry Association