Before the Copyright Office of the Library of Congress
Docket No. RM 2002-4

In the Matter of Rulemaking
Exception to Prohibition on Circumvention Protections Systems
For Access Control Technologies

Comments of the USACM

Introduction

Pursuant to the Copyright Office's Notice of Inquiry dated October 15, 2002, the following statement represents the comments of USACM, the U.S. Public Policy Committee of the Association for Computing Machinery. ACM is the leading nonprofit membership organization of computer scientists and information technology professionals dedicated to advancing the art, science, engineering and application of information technology. USACM serves the ACM membership and community by providing policymakers, courts, and the public with a deeper understanding of computer and Internet issues and their convergence with legislative and regulatory initiatives.

Proposed class or classes of copyrighted work(s) to be exempted

Literary works, including computer programs and databases, protected by access control mechanisms that fail to permit access to recognize shortcomings in security systems, to defend patents and copyrights, to discover and fix dangerous bugs in code, or to conduct forms of desired educational activities.

Brief summary of the argument(s)

USACM has found section 1201(a)(1) to have substantial negative impacts on the conduct of basic research in the U.S., particularly in cryptography and other computer security areas. The section interferes with many legal, non-infringing uses of digital computing and prevents scientists and technologists from circumventing access technologies in order to recognize shortcomings in security systems, to defend patents and copyrights, to discover and fix dangerous bugs in code, or to conduct forms of desired educational activities. Examples are provided below.

USACM Comments

USACM's comments in this matter address the adverse affects of section 1201(a)(1) of the Copyright Act, which provides that "no person shall circumvent a technological measure that effectively controls access to a work protected under this title". USACM has found section 1201(a)(1) to have substantial negative impacts on the conduct of basic research in the U.S., particularly in cryptography and other computer security areas. The section interferes with many legal, non-infringing uses of digital computing and prevents scientists from circumventing access technologies in order to recognize shortcomings in security systems.

In particular, please consider the following examples of legitimate activities that are prevented by section 1201(a)(1), undermining efforts to create a robust system that can endure rigorous scrutiny:

*A financial institution received a digital object protected by code obfuscation using means other than encryption. Employees of the firm suspected it contained a highly destructive computer virus or worm. The only way to find out if these suspicions were valid would be to circumvent the obfuscation techniques to see what the code actually did. Because the code -- including a

possible virus -- qualifies as an "original work of authorship," the act of its circumvention is prohibited.

* A contractor is employing software technology from a third party in a system widely used by law enforcement. In the course of use, a serious flaw ("bug") is discovered that makes the system fail unexpectedly. The third party is suspected to be a "front" for a crime organization and is not trusted to provide a fix for the software. Because the software is protected as an original work of authorship, no reverse engineering or circumvention is allowed to fix the flaw in a trusted manner.

*A firm might want to test a computer system before purchasing it to ensure that it is trustworthy and secure or to check for patent and licensing violations in the code itself. Circumventing a technical measure without the producer's permission is prohibited.

*Scientists and educators are prohibited from teaching many of the standard security techniques to investigate security risks.

*A copyright owner might suspect that a user is infringing his work. The only way to test his assumptions would be to bypass the encryption scheme of the suspected work to assess the material. Bypassing the encryption scheme is prohibited.

USACM Conclusion

The fundamentally flawed approach of section 1201(a)(1) that criminalizes multi-use technologies rather than penalizing infringing behavior undermines efforts to enhance cyber-security, to defend patents and copyrights, to discover and fix dangerous bugs in code, or to conduct forms of desired educational activities. During the proceeding, USACM urges you to recognize the distinction between circumvention for the purpose of obtaining unauthorized access to a work and circumvention for the purpose of developing new techniques to protect computer systems and networks against attacks, negligence, malfeasance, and vandalism, or to advance the continued innovation of software and digital computing.

Thank you for this opportunity to offer our comments. Please contact us with additional questions.

Respectfully submitted,

Barbara Simons, Ph.D.
Eugene H. Spafford, Ph.D.

Co-Chairs
U.S. ACM Public Policy Committee (USACM)
Association for Computing Machinery