DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

LIBRARY OF CONGRESS

Copyright Office

[Docket No. 990428110-9110-01]

RIN 0660-ZA09

Request for Comments on Section 1201(g) of the Digital Millennium Copyright Act

COMMENTS OF
THE COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION (CCIA)

The Computer & Communications Industry Association (CCIA) strongly supported ratification and implementation of the World Intellectual Property Organization (WIPO) Copyright Treaty and the WIPO Performances and Phonograms Treaty, both of which were intended to update the Berne Copyright Convention to improve protections for digital works such as computer software and compact disks. The WIPO Copyright Treaty affirms that computer programs and other digital works are due the full copyright subject matter protection under the Berne Convention. WIPO also clarifies transmission rights for copyrighted works in digital, electronic formats, and requires "adequate and effective" remedies to protect against the circumvention of anti-copying technologies and alteration or removal of electronic rights management information.

Following the adoption of WIPO by the treaty delegates, the Administration introduced implementing legislation in the 105th Congress. However, these bills, S. 1121 and H.R. 2281, went beyond the revisions necessary to conform American law to our treaty obligations and conferred broad new rights on the owners of copyrighted material. As introduced, these bills would have made it illegal for competitors to analyze operating systems or software platforms for the purpose of creating interoperable products. Computer scientists conducting encryption research and security testing would have also been in danger of running afoul of the law. In addition, online service providers could have been subject to broad liability for the actions of others engaging in copyright piracy utilizing their services, regardless of whether the service provider played any role or had any knowledge of such activity.

Working on behalf of its members, CCIA was actively involved throughout consideration of this legislation (the Digital Millennium Copyright Act (DMCA) (Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998)). In addition to working to limit the legislation's impact on the broad issues of service providers' liability and fair use, CCIA and other interested parties were able to preserve the practice of reverse engineering for interoperability purposes.

CCIA also spearheaded the effort leading to the exception for encryption research, the subject of this Request for Comments. We believed then, and continue to believe, that this language is essential to maintaining research and academic study in the field of cryptography. We also believe that the language as enacted must be interpreted to protect and encourage legitimate encryption research. If interpreted too strictly, the requirements of the Act could lead to unintended and detrimental consequences.

In its report on the DMCA, the Senate Judiciary Committee made clear that:

> [t]he effectiveness of [technological copyright protection] measures depends in large part on the rapid and dynamic development of better technologies, including encryption-based technological protection measures. The development of encryption sciences requires, in part, ongoing research and testing activities by scientists of existing encryption methods, in order to build on those advances, thus promoting and advancing encryption technology generally.

[S. Rept. 105-190, p. 15]

Circumvention of technological protection measures, which (with some limited exceptions) is otherwise prohibited by the DMCA, is essential in the field of encryption research. In order to perform the research necessary to improve or learn about a computer security system, a researcher must often circumvent technological protection measures, such as encryption. As in the physical world, the only way to really know the strength and effectiveness of an electronic lock is by trying to break it. Circumvention of technological protection measures is a standard operating procedure for these researchers.

Section 1201(g) of the DMCA specifies that it is not a violation of the Act

> for a person to circumvent a technological measure as applied to a copy, phonorecord, performance, or display of a published work in the course of an act of good faith encryption research if--
>
> (A) the person lawfully obtained the encrypted copy, phonorecord, performance, or display of the published work;
> (B) such act is necessary to conduct such encryption research;
> (C) the person made a good faith effort to obtain authorization before the circumvention; and
> (D) such act does not constitute infringement under this title or a violation of applicable law other than this section . . . .”

Of particular concern to CCIA and its members who conduct or benefit from legitimate encryption research is subsection (C), which requires a "good faith effort to obtain authorization" prior to circumventing an access control technology. If interpreted broadly, this clause could be very problematic to the research community.

In particular, the distinction between general encryption systems and copyright enforcement systems is not at all clear, and can be expected to become even less so in the future. A particular encryption algorithm or program may be put to a variety of uses, and there are likely to be numerous parties (hundreds or even thousands) using any given system (or aspect of a system) that an encryption researcher wishes to test for flaws and vulnerabilities. The Act could be interpreted to require the researcher to try to obtain permission from each one of them.

Therefore, in many cases it may not be feasible, practical, or even possible for some researchers to make this "good faith effort."

For instance, some copyright protection schemes work by encrypting the copyrighted data or by requiring the user to authenticate to some trusted “license manager.” However, these same – or similar – algorithms and protocols could be used for a wide range of other computer and communications security applications, including protection of sensitive user data (file and message encryption), access-control of computer systems or networks, secure financial transactions, etc. Some copyright protection measures discourage copying by embodying some of the sensitive user data in software that has been specially designed to resist reverse engineering and decompilation, but these same design techniques could be used to design more secure software for electronic commerce, distributed systems, and software license management. In order to make these (non-copyright protection) applications trustworthy enough to use commercially, the research and engineering communities must be able to do exactly the kind of open engineering, analysis, and exchange of tools and sharing of partial results that could be prohibited under §1201(g), simply because someone, somewhere, happens to be using similar technology for copyright protection.

The Senate Judiciary Committee’s Report on the DMCA repudiates such a broad reading of 1201(g):

> [T]esting of an encryption algorithm or program that has multiple uses, including a use as a technical protection measure for copyrighted works, would not fall within the prohibition of section 1201(a) when that testing is performed on the encryption when it is in a form not implemented as a technical protection measure.

[S. Rept. 105-190, p. 15]

Furthermore, it is not evident what advantage the copyright holder gains by such a notice requirement, except the general ability to discourage research, since there is no requirement that permission actually be obtained. The disadvantages to legitimate research of complying with the requirement, however, are quite serious.

In particular, it puts researchers and their companies at a significant competitive disadvantage to have to disclose their plans to others prior to proceeding on a course of research. Encryption research by its very nature is an adversarial process. It is also essential for cryptographers to be able to advance the science by attempting to find vulnerabilities in encryption as that encryption is actually applied. In many cases, a researcher will look at many systems as part of a plan to try to create an improved system, something one would very much want and expect to keep secret, for obvious commercial and intellectual property reasons. However, under the Act, a researcher would be required to at least make a “good faith effort” to notify parties who may be potential industry competitors, rival intellectual property claimants, or hostile security officers before he or she even began the research.

The chilling effect on research and innovation should be obvious and of great concern. In many cases, the content owner is unlikely to authorize this research even if he has no competitive interest in the field. Most content owners have no particular interest in the advancement of the

field, particularly if it involves finding weaknesses in a system on which he is relying to protect copies of a work that he is distributing broadly for a fee. Even if the content owner were inclined to grant approval for the research, the research process would inevitably be retarded as the general counsels of universities and encryption firms would prohibit researchers from proceeding until all necessary authorizations had been received in writing.

Members of CCIA are extremely concerned about this provision and troubled by the potential harm a strict application of the DMCA's language could have on the field of encryption research and the development of secure security systems based on encryption. We believe this research and study is essential to the further advancement of electronic commerce and secure digital networks, and hope that the Administration and Congress will take steps to ensure that such activity is protected.

Respectfully Submitted,

Jason M. Mahler
Vice President and General Counsel
Computer & Communications Industry Association
<jmahler@ccianet.org>

CCIA Members:

Amdahl Corporation
AT&T Corporation
Bell Atlantic Corporation
Block Financial Corporation
CAI/SISCo
Commercial Data Servers, Inc.
CommonRoad Corporation
Datum, Inc.
Entegrity Solutions Corporation
Fujitsu Limited
Giga Information Group
Government Sales Consultants, Inc.
Hitachi Data Systems, Inc.
Intuit, Inc.
Leasing Solutions, Inc.
MERANT
Netscape Communications Corporation
NOKIA, Inc.
Nortel Networks
NTT America, Inc.
Okidata
Oracle Corporation
RedCreek Communications, Inc.

SBC Communications, Inc.
Sun Microsystems, Inc.
Telesciences, Inc.
Sabre Inc.
TSI International Software, Ltd.
VeriSign, Inc.
Viatel, Inc.
ViON Corporation
V-SPAN, Inc.
Yahoo! Inc.