



Chilling Effects of the U.S. DMCA on Cryptographic Research

ISOC MEMBER BRIEFING #8

October 2002

Authors: Timothy D. Casey and Jeffrey L. Magenau

Definition:

Digital rights management refers generally to the efforts of owners of intellectual property, in particular copyrights, to protect their property in digital media. Encryption research refers to efforts to advance the state of knowledge in encryption technology, including the development of commercial encryption products, by analyzing the flaws and vulnerabilities therein.

Background:

The advent of digital media and networks designed to efficiently disseminate it has prompted some copyright owners to attempt to protect their property in digital form through various technological measures, such as encryption. Contemporaneously, the owners have also urged governments around the world to outlaw the circumvention of such protective measures, including the dissemination of products or information that would further circumvention efforts. Such laws, however, can reach far beyond the intended objective of protecting copyrights. One such law is the U.S. Digital Millennium Copyright Act (DMCA). Section 1201 of the DMCA prohibits (1) the circumvention of a technological measure that "effectively controls access to" protected material; and (2) the "manufacture, import, offer[ing] to the public, provid[ing] or traffic[king] in any technology, product, service, device, component or part thereof" that is "primarily designed or produced for the purpose of" circumventing technology that either (i) controls access to a protected work, or (ii) otherwise protects a copyright owner's rights. Although such laws may have an adverse effect on a wide range of conduct, including innovation, research and education, a central question for encryption researchers is whether publishing research results can amount to providing or trafficking in "technology" primarily produced to circumvent protection in violation of the DMCA.

Legal analysis:

The DMCA prohibits both the circumvention of technological measures controlling access to a copyrighted work and the

Expanded Coverage from ISOC

In-depth articles, papers, links and other resources on a variety of topics are available from the ISOC site at: www.isoc.org/internet/issues

Examples in the News

CNET News.com

October 11, 2002

Anti-Hacking Copyright Law to Get Review

The United States Copyright Office is launching a rare round of public comment on rules that bar people from breaking through digital copy-protection technology on works such as music, movies, software or electronic books. Regulators aren't looking to change the law, but they are looking for public suggestions on what kinds of activity should be legalized in spite of the rules.

Coverage : <http://news.com.com/2100-1023-961783.html>

Comment page :

http://www.copyright.gov/1201/comment_forms

For More Information

US Copyright Office :

www.copyright.gov/reports/studies/dmca/dmca_study.html

dissemination of technology that can be used to engage in such circumvention. Both prohibitions, however, enjoy a limited exception for encryption research.

For example, it is not prohibited to circumvent measures controlling access, in this case encryption, in the course of good faith encryption research if: (i) the researcher lawfully obtained the encrypted work; (ii) the circumvention was necessary to conduct the research; (iii) the researcher made a good faith effort to obtain authorization prior to circumvention; and (iv) such circumvention does not violate other laws, such as the Computer Fraud and Abuse Act (accessing a computer without authorization). It is not specified what kind of authorization is required prior to circumvention, but presumably it requires permission from the copyright owner. This assumes, however, that the encryption researcher is aware that the encrypted material is protected by copyright. Because U.S. law does not require copyrighted works, encrypted or not, to include a discernible copyright notice, encryption researchers -- and anyone else for that matter -- may unintentionally violate the DMCA's prohibition by accessing what turns out to be protected material.

Likewise, it is not a violation of the DMCA to develop technology to circumvent encryption used to control access to a protected work "for the sole purpose of... performing encryption research" or to provide such technology to "another person with whom [the researcher] is working collaboratively" on encryption research, including for the purpose of the collaborator verifying the researcher's findings. With respect to technologies that protect the rights of copyright owners in ways other than by controlling access to a protected work, however, the exemption for encryption research does not apply. For example, publishing code designed to circumvent technology used to prevent or limit digital copies, or to prevent the display of a copyrighted work on certain devices, is prohibited by the DMCA. While encryption technology generally is used to control access rather than directly control the underlying rights of copyright owners, this may not be true of all uses of encryption. For example, publishing code designed to de-crypt a technology that allows the owner of a particular copy of a protected work to make limited copies of that work, would not be exempt from the DMCA's prohibitions.

The DMCA sets out criteria for determining whether the exemption applies, namely, whether: (1) the information derived from the research was disseminated "in a manner reasonably calculated to advance the state of knowledge or development of

H.R.2281 - Digital Millennium Copyright Act :
<http://thomas.loc.gov/cgi-bin/query/z?c105:H.R.2281.ENR>:
DMCA Legislative History :
<http://www.hrrc.org/html/DMCA-leg-hist.html>

Relevant IETF RFC's
RFC 1984 (<ftp://ftp.rfc-editor.org/in-notes/rfc1984.txt>)
IAB and IESG Statement on Cryptographic Technology and the Internet

Related Organizations
The Anti DCMA Web Site :
<http://www.anti-dmca.org/>
The Electronic Frontier Foundation :
<http://www.eff.org/>

ISOC Public Policy Activities and Digital Rights Management

In a recent press release, the Internet Society stated that it strongly opposes attempts to impose governmental technology mandates that are designed to protect only the economic interests of certain owners of intellectual property over the economic interests of much larger portions of society. The Society believes that technology mandates are inherently anti-innovative. The entire concept of a mandate is that it freezes a particular technology at a point in time, and inhibits research and development on new and better technology.

encryption technology, versus whether it was disseminated in a manner that facilitates infringement"; (2) the encryption researcher is "engaged in a legitimate course of study, is employed, or is appropriately trained and experienced in the field of encryption technology"; and (3) the researcher provides the owner of the copyrighted work with "notice of the findings and documentation of the research."

Note, however, that these criteria apply only to the encryption research exemption for the act of circumvention, and not to the exemption for "offering to the public" technology that may be used by others to engage in circumvention. This is curious, as the criteria specifically refer to dissemination. Researchers are therefore without guidance in determining the scope of the permissible act of providing "technological means" to "another person" with whom the researcher is working collaboratively. Taken as a whole, however, it would seem reasonable to conclude that Congress contemplated researchers widely disseminating, e.g., publishing, their findings. It would be nonsensical to suggest, as the DMCA appears to, that disseminating "information derived from the encryption research" is permissible to "advance the state of knowledge" while prohibiting "offer[ing] to the public or otherwise traffic[king] in" that same information. Obviously, the state of knowledge cannot be advanced if the research findings cannot be disseminated. Further, the prohibition on trafficking applies to "technology, product[s], service[s], device[s], component[s], or part[s] thereof." Arguably, "information derived from" encryption research is none of these things.

More problematic, is the criterion weighing whether research findings were disseminated "in a manner that facilitates infringement." This implies that the intent of the researcher is immaterial if the findings were disseminated to someone who used the information to circumvent protections on, and thus infringe, copyrighted material. Fortunately, the prohibitions on "offering to the public" apply only when the circumventing technology is "primarily designed or produced" for the purpose of circumventing copyright protection. It would seem unlikely, therefore, that the publishing of findings from research on encryption widely used for, say, privacy protection would be prohibited by the DMCA.

Implications:

The anti-circumvention provisions of the DMCA, as well as other proposed legislation variously mandating or prohibiting the use of certain technologies, may have an adverse effect on the freedom to innovate, share information, and engage in

About the Authors

Timothy D. Casey, Partner
(caseyti@ffhsj.com)

Fried, Frank, Harris, Shriver &
Jacobson



Timothy D. Casey is a partner at Fried Frank Harris Shriver & Jacobson in Washington, DC, where he is chairman of the firm's intellectual property & technology department. His practice focuses on business and technology-related transactions; IP and technology development, management and utilization, including licensing, litigation and policy. Prior to joining Fried Frank, Casey was Chief Technology Counsel, Senior Vice President for MCI WorldCom, Inc. (1995-2000), and at SGI (1992-1995) and Apple Computer (1989-1992).

Jeffrey L. Magenau, Associate
(magenje@ffhsj.com)

Fried, Frank, Harris, Shriver &
Jacobson



Jeff Magenau is an associate in the Technology Transactions and Services practice group at Fried, Frank, Harris, Shriver & Jacobson in Washington, DC. He concentrates his practice in the area of technology law, including: Counseling on general intellectual property matters, including

heretofore permissible activity. One field at risk is encryption research. It would appear, however, that legitimate encryption researchers have a strong argument that their research and the publication of their findings are exempt from the anti-circumvention provisions of the DMCA, at least with respect to encryption controlling access to copyrighted works.

Nonetheless, researchers are left to guess as to the potential reach of the DMCA's prohibitions. Congress did not make its intentions clear, the U.S. Copyright Office has not yet issued interpretive guidelines, and no final verdict has been reached in a criminal action. As such, the most prudent course of action may be to engage in encryption research (which may include circumventing encryption to gain access to a protected work) while closely adhering to the criteria set out in the DMCA, which courts will use to determine the applicability of the encryption research exemption, but to delay or proceed with extreme caution in publishing the findings until greater certainty develops. This is particularly true when it is known or appears likely that the encryption technology being studied is commonly used to control access to copyrighted material. At the same time, researchers should avoid publishing findings on encryption used to protect the rights of copyright owners in ways other than by controlling access to a protected work.

ISOC Position:

The Internet Society strongly opposes attempts to impose governmental technology mandates that are designed to protect the economic interest of certain owners of intellectual property over the economic interests of much larger portions of society. The current debate in many countries of the world regarding digital rights management (DRM) has illustrated the inevitable conclusion of technology mandates in law: a world where all digital media technology is either forbidden or compulsory. The effect of these mandates is to grant veto power over new technologies to special interest groups who have continually opposed innovation. The Internet Society deprecates the situation that researchers are put in by the DMCA.

For a detailed statement by the Internet Society on Digital Rights Management, see the ISOC press release of 15 August 2002 : <http://www.isoc.org/isoc/media/releases/020815pr/shtml>

copyright, trademark, and trade secrets; Intellectual property, technology, and software licensing; Internet and e-commerce counseling, including regulatory compliance, legislative considerations, network infrastructure and technology issues, and content liability.

Acknowledgments

The ISOC Member Briefing series is made possible through the generous assistance of ISOC's Platinum Program Sponsors: APNIC, ARIN, Microsoft, and Ripe NCC. *More information on the Platinum Sponsorship Program :* <http://www.isoc.org/isoc/membership/platinum.shtml>

About the Background Paper Series

Published by:

The Internet Society
1775 Wiehle Avenue, Suite 102
Reston, Virginia 20190 USA
Tel: +1 703 326 9880
Fax: +1 703 326 9881
4, rue des Falaises
CH-1205 Geneva
Switzerland
Tel: +41 22 807 1444
Fax: +41 22 807 1445

Email: info@isoc.org
Web: <http://www.isoc.org/>
Series Editor: Martin Kupres