Encryption Research Study

From: <hal@finney.org>
To: <dmca@ntia.doc.gov>; <crypto@loc.gov>
Sent: Monday, July 12, 1999 6:46 PM
Subject: Comments on Digital Millennium Copyright Act

July 12, 1999

Paula J. Bruening
Office of Chief Counsel
National Telecommunications and Information Administration (NTIA)
Room 4713
U.S. Department of Commerce
14th Street and Constitution Avenue N.W.
Washington, DC 20230

and

Jesse M. Feder
Office of Policy and International Affairs
U.S. Copyright Office
Copyright GC/I&R
P.O. Box 70400 Southwest Station
Washington, D.C. 20024

Dear Sir and Madam:

Thank you for the opportunity to comment on the effects on encryption research of the Digital Millennium Copyright Act.

I am presently employed in the field of cryptography. I design and implement cryptographic algorithms for the software libraries used by my employer, Network Associates, Inc. NAI is one of the largest companies providing cryptographic software in the United States, particularly the well known encryption program, PGP.

Encryption is a crucially important technology as we enter the 21st century. As we move into a world of electronic communications, cryptography is becoming the primary tool for controlling the flow and dissemination of information. It is necessary that research in this area continue unfettered so that we know what is possible and, more importantly, where we are failing to achieve our goals.

It appears that the DMCA may have a very unfortunate chilling effect on cryptographic research. The act has a number of provisions which

specify under what circumstances cryptographic research may occur which relates to investigating the strength of copyright protections. The problem is that these are written in an ambiguous style which will put researchers at risk of violating the law. Prudent researchers who do not want to risk criminal prosecution will avoid work in this area.

The result will be that the only people working on breaking copyright protection will be criminals. Legitimate users will have no way of knowing whether the technology to which they are entrusting their secrets is working properly or not. That's the problem which researcher Bruce Schneier points out with regard to encryption: bad cryptography looks much the same as good cryptography. Only with expert analysis and challenge can we determine whether our algorithms are breakable. By driving the legitimate experts into other avenues of research, the DMCA will leave the field to those who care nothing about laws. To paraphrase another slogan, if you outlaw cryptographic research, only outlaws will do cryptographic research.

Let us look at the specific provisions of the DMCA which lead to this unfortunate result.

> ``(g) Encryption Research.--
> ``(1) Definitions.--For purposes of this subsection--
> ``(A) the term `encryption research' means activities necessary to identify and analyze flaws and vulnerabilities of encryption technologies applied to copyrighted works, if these activities are conducted to advance the state of knowledge in the field of encryption technology or to assist in the development of encryption products; and
> ``(B) the term `encryption technology' means the scrambling and descrambling of information using mathematical formulas or algorithms.

Here we see a problem which is symptomatic of this section of the Act. We have an attempt to specifically define what encryption research is, so that it may be exempted. However the definition, although wordy, is far from clear. It relies on determining the purpose of the activities which are undertaken: are they intended to advance the state of knowledge, and/or to assist in developing encryption products. But it will be very difficult to prove what the purposes are of any particular instance of defeating copyright protection. A criminal may claim that he intended to disseminate his results, or a legitimate researcher who delays publication while he gathers more data may find himself accused of criminal actions.

> ``(2) Permissible acts of encryption research.--
> Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection 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, including section 1030 of title 18 and those provisions of title 18 amended by the Computer Fraud and Abuse Act of 1986.

These provisions will impose a considerable burden on the researcher.

(A) requires him to retain documentation on all copyrighted material which he has in his possession in order to show that he obtained it lawfully. But this may not be at all reasonable, for if the material is encrypted it may be widely available for download. There is no technology available to prove that a given piece of data was freely available at some time in the past. This provision is going to be intolderably burdensome in many cases.

(B) has the problems listed above in interpreting what constitutes encryption research.

Provision (C) can only be described as bizarre. There is no requirement elsewhere in the exemptions to receive authorization from the copyright holder. Apparently, whether authorization is granted or not makes no difference, but nevertheless the researcher is required to seek authorization? This is completely illogical.

Furthermore, this provision will face many of the same documentation problems as section (A), as in many cases the copyright holder may not be known or reachable. What constitutes a good faith effort in that case? The researcher who fails to guess correctly on this point faces criminal prosecution.

(D) can only increase the uncertainty felt by a researcher considering entering this minefield.

The net result is that these provisions carve out an exception which is loaded with traps, where inadequate documentation can lead to criminal penalties, and where illogical actions are required for no purpose. This is sure to drive many qualified researchers from the field.

``(3) Factors in determining exemption.--In determining whether a person qualifies for the exemption under paragraph

(2), the factors to be considered shall include--

``(A) whether the information derived from the encryption research was disseminated, and if so, whether it was disseminated in a manner reasonably calculated to advance the state of knowledge or development of encryption technology, versus whether it was disseminated in a manner that facilitates infringement under this title or a violation of applicable law other than this section, including a violation of privacy or breach of security;

``(B) whether the person is engaged in a legitimate course of study, is employed, or is appropriately trained or experienced, in the field of encryption technology; and

``(C) whether the person provides the copyright owner of the work to which the technological measure is applied with notice of the findings and documentation of the research, and the time when such notice is provided.

These provisions further increase the uncertainty and risks which will be faced by researchers. Not only his intentions are being judged, but the judgement criteria are left vague and menacing.

Under provision (A) he has to disseminate his results in an acceptable way. What does that mean? If he notifies his colleagues, which is a common practice in the research community, is he now open to prosecution? If some colleagues use the information irresponsibly, is the original researcher to be penalized? He faces a dilemma whether he publishes or keeps his results secret.

As for provision (B), are we now creating a de-facto classification of "licensed cryptographers" who are allowed to do cryptographic research? Imposing criminal penalties based on whether a judge views the researcher as having adequate training, experience, and employment is absurd without some kind of objective certification. This is a fast-moving field and many of the most creative results have come from individuals without formal training in cryptography (which is offered at very few institutions). I personally have nospecific training in the field other than a degree in computer science. Would this pass muster under this provision? There is no way to know.

Provision (C) is astonishingly vague. It seems to be trying to hint that a break should initially be reported only to the copyright holder, then later to the research community, and finally it can be made public. But for some reason the Act is not willing to say so plainly.

This provision is representative of the flaws in this entire section of the Act. It is legislation by innuendo, enforcement by intimidation. These requirements are not stated clearly, rather we have an ill

defined set of guidelines which may be interpreted in any way desired by the judge. It is impossible to conduct research safely in such a regime.

In summary, the attempts by the DMCA to carve out an exception for legitimate cryptography researchers are seriously flawed. Anyone doing research in this area faces severe record-keeping burdens, and risks having their actions misconstrued. With criminal penalties as the result of anything determined to be a violation, it is likely that this Act will drive cryptographic researchers from the field.

The result will be a loss of confidence in cryptographic technology as users realize that the best and brightest researchers are no longer able to do research in this field. This will harm electronic commerce and damage American interests domestically and internationally. As currently written, it appears that the DMCA will have exactly the opposite effect from what was intended, in that it will reduce the protections to copyright holders and delay widespread electronic distribution of copyrighted material.

Thank you for your attention.

Hal Finney
Senior Software Engineer
Network Associates, Inc.
hal@finney.org