Emusic.com Incorporated
1991 Broadway, 2nd Floor
Redwood City, California 94063
Main: 650-216-0200
Fax: 650-556-9712
Web: http://www.emusic.com

The Source for Downloadable Music

July 26, 1999

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

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

Re: Request for Comments on Section 1201(g) of the Digital Millennium Copyright Act, Docket No. 990428110-9110-01

Dear Ms. Bruening and Mr. Feder:

EMusic.com welcomes this opportunity to submit comments on the impact that Section 1201(g) of the Digital Millennium Copyright Act, P.L. No. 105-304, 112 Stat. 2860 (October 28, 1998) ("DMCA"), will have on encryption research and the development of encryption technology. EMusic.com would like to focus, in particular, on the effect that Section 1201(g) will have an efforts to evaluate the effectiveness of industry-sponsored security and copyright management specifications that incorporate cryptography.

The Growing Importance of Industry-Sponsored Standards

One of the principal motivations behind the enactment of the DMCA was the recognition that a rapidly expanding amount of copyrighted content – be it text, video, audio, or otherwise – will be distributed in digital form. As the distribution of digital content proliferates, copyright owners will seek to develop methods of preventing unauthorized use of their content, such as the commercial distribution of unlicensed copies. Because most forms of digital media can be downloaded, stored, and replayed across an array of different devices, different industry sectors will likely seek to cooperate in the design and implementation of uniform specifications

for copyright management systems (subject, of course, to the limitations imposed by the antitrust laws). Several of these initiatives are already underway.

The design and implementation of industry-sponsored copyright management systems has the potential to profoundly influence the market for digital media and the manner in which digital media are distributed. The choices that different industry sectors make with respect to these systems are likely to result in significant investments in new technologies and distribution channels. Moreover, these decisions will undoubtedly influence the options that are available to consumers, both in terms of the ease with which they will be able to access copyrighted content and the equipment that they will require to do so. A misguided decision about a particular copyright management system could result in unproductive investments and, worse, could retard the emergence of new markets for digital media.

For these reasons, EMusic.com believes it is vitally important that copyright management systems be subject to rigorous scrutiny prior to their widespread adoption by industry and consumers. Moreover, once in place, copyright management systems should continue to be subject to intensive, real-world challenges, so long as those challenges are not motivated by a desire to gain unauthorized access to, or engage in unauthorized uses of, copyrighted works. Legitimate evaluation and criticism of copyright management systems is the only surefire means of ensuring their effectiveness and vitality.

EMusic.com is therefore deeply concerned about the possibility that advocates of particular copyright management systems will use the anti-circumvention provisions of the DMCA to thwart or deter good-faith efforts to evaluate and publicize the vulnerabilities of those systems. While originally intended as a means of going after those who seek to circumvent cryptography-based access controls for illegitimate purposes, the anti-circumvention provisions could also be used as a weapon against those who seek to demonstrate the ineffectiveness of such controls for entirely legitimate reasons. If this were to be permitted, advocates of particular standards could use the DMCA to squelch opposition to that standard and to coerce industry and consumer acceptance of a standard that has not been subject to open testing.

Ambiguities in the Encryption Research Exception

Given the potential misuse of the anti-circumvention provisions of the DMCA, EMusic.com believe that it is extremely important that the encryption research exception set forth in Section 1201(g) be construed to permit individuals and companies to evaluate and publicize the vulnerabilities of copyright management systems, whether proposed or implemented. Unfortunately, however, Section 1201(g) contains several troubling ambiguities that could be seized upon by those who would seek to use the anti-circumvention provisions of the DMCA as a means of deterring legitimate evaluations. In particular, EMusic.com is concerned that:

- Under Section 1201(g)(2)(C), a person who intends to circumvent a "technological measure," as that term is used in the Act, must make "a good faith effort to obtain authorization before

the circumvention," presumably from the owner of the underlying copyright. It is not clear whether attempting to obtain such consent and having the request denied would constitute such a "good faith effort." If not, the advocates of a particular security implementation could simply deny all requests from "outsiders" for authorization to test the implementation. That policy, especially if it is combined with aggressive legal threats and a policy of following up to see if the disapproved applicants have truly abandoned their testing plans, could seriously deter disclosure of any vulnerabilities that the technology might have. While there may be some situations in which it is possible to test the implementation in the context of uncopyrighted works or works to which the tester owns the copyright, there will be many situations in which it is only possible to test the implementation when it is applied to works that are copyrighted by others (for example, when the cryptography is used to establish a secure communications channel).

- Under Section 1201(g)(3)(A), one of the "factors" in determining one's qualification for the exception is 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" of copyrighted works.

  This is without question the most troubling of the ambiguities in Section 1201(g). The chief problem is that it posits a false dichotomy: the dissemination of cryptographic research either advances the state of knowledge, or it facilitates infringement – but not both. In fact, the dissemination of information relating to flaws in cryptographic implementations can both advance the state of knowledge and, incidentally, facilitate infringement by those who have such an intent. Indeed, practically every computer security alert has two effects – it encourages computer users to fix a security hole while at the same time telling hackers that the hole exists. It is virtually impossible to distinguish between these two effects, and equally impossible for persons with legitimate intentions to know with any reasonable degree of certainty whether they will be accused of falling on the wrong side of this (non-existent) line. The effect of this uncertainty will be to deter persons who are seeking to make information available about specific weaknesses in cryptographic implementations, even when their intention is solely to draw attention to the deficiencies of a proposed standard.

- Under Section 1201(g)(3)(B), an additional "factor" to consider in determining eligibility for the encryption research exception is whether the person who performs the act of circumvention "is engaged in a legitimate course of study, is employed, or is appropriately trained or experienced, in the field of encryption technology." If courts construe this factor too narrowly, the result could be to limit legitimate security evaluations to a relatively small community of academics and professional information security consultants. The information technology industry, however, has a rich tradition of individuals – often not associated with any corporation or organization, and often without any formal training – who seek to crack security implementations and publicly demonstrate their shortcomings. There is a large community of such individuals – sometimes referred to as "ethical hackers" – who engage in this activity not for any illegitimate purpose, but simply out of a belief that security

implementations should be subject to open testing in real-world environments. This tradition has kept constant pressure on the industry to develop new and stronger security implementations, and has prevented bad security implementations from gaining widespread acceptance. It is a kind of Darwinian selection process that benefits industry and consumers as a whole.

When coupled with the ambiguity in Section 1201(g)(3)(A) about the manner in which the results of cryptographic research are disseminated, the result of these provisions could be to deter these kinds of individuals from engaging in open testing of security implementations and publicizing the results. There are many examples of security implementations whose vulnerabilities were first publicized by persons without any formal training or professional affiliation in the information security industry. While there is a superficial appeal to the argument that these security implementations would have had a longer shelf-life had their vulnerabilities *not* been revealed, in the long run, there is greater benefit from having those vulnerabilities revealed. This is particularly true when reliance on a particular security implementation could lead to significant industry and consumer investment in hardware and software devices that support that implementation.

An Illustration

It might be helpful to illustrate the foregoing concerns with a scenario that could, as they say, be "ripped from today's headlines." Although this scenario is greatly simplified, it amply demonstrates the problems that could result from an overly-restrictive interpretation of Section 1201(g).

A group of film studios and hardware manufacturers get together and establish a uniform copyright management specification for the distribution of digital video products. The specification controls the number of copies that can be made, the period during which the video can be watched, whether it can be watched on machines other than the viewer's, and other similar parameters. The specification incorporates encryption as a means of enforcing these controls. In this manner, the encryption used in the specification "effectively controls access" to a copyrighted work, and is therefore within the scope of the anti-circumvention provision, § 1201(a)(1).

In one variant of the scenario, a film studio that was not a part of the standards-setting group decides that the adoption of the specification will hinder the overall development of the digital video market, as the manner in which it controls use of the video is likely to deter most consumers from purchasing titles that are subject to those controls, as well as the hardware that is necessary to play them. The film studio is concerned that widespread industry commitment to this standard will delay the expansion of the digital video market that it believes is required to justify a switch to digital-only distribution mechanisms. For these reasons, it wants to demonstrate that the specification is flawed, in part because the encryption that it incorporates can be compromised. As a known critic of the specification, however, it cannot obtain the proprietary hardware and software that it would need to subject one of its own film titles to the

controls, and test the specification on that basis. Therefore, it obtains a video that is subject to the controls in the open marketplace, and hires an information security expert to crack the encryption on which the controls are based. In order to promote industry opposition to the specification, the film studio publicizes its success in cracking the encryption and provides details of the manner in which it was able to do so.

In a second variant of the scenario, a technically-minded customer is opposed to the industry specification because of the controls that it imposes, because it requires consumers to buy new hardware, and because it will gradually render his vast collection of film titles recorded in another format obsolete. He starts a website to generate public opposition to the standard. Although he has no formal training in encryption technology and is not employed in that field, he manages to crack the encryption used in the specification. He publicizes his success on the website, providing specific details of the manner in which he was able to do so. It is his hope that the publicity surrounding his announcement, and the fact that a means of bypassing the controls is now public knowledge, will convince the industry to abandon the standard in favor of one that is more consumer-friendly. He does not use his ability to crack the encryption as a means of gaining unauthorized access to copyrighted content.

In both variants of the scenario, the industry association that developed the standard brings suit under Section 1203 of the DMCA, arguing that the circumvention of the encryption violated Section 1201(a). It also seeks criminal prosecution under Section 1204. With regard to the dissident film studio, it argues that the encryption research exception does not apply because the film studio did not make a "good faith effort to obtain authorization before the circumvention," § 1201(g)(2)(C), and because the film studio disseminated information about its successful circumvention of the encryption "in a manner that facilitate[d] infringement" of copyrighted works, § 1201(g)(3)(A). With regard to the activist consumer, the industry association further argues that the exception does not apply because the consumer is not "engaged in a legitimate course of study" or "employed … trained or experienced in the field of encryption technology," § 1201(g)(3)(B).

If the industry association were to prevail in either one of these suits, the message would be clear: proponents of industry standards can use Section 1201 to squelch legitimate criticism and analysis of those standards, including criticism and analysis that is not in the least bit motivated by a desire to gain unauthorized access to copyrighted works. This threat would be felt by both companies and private individuals. Proponents of particular standards could use this threat to conceal the vulnerabilities of those standards and to encourage widespread industry and consumer acceptance of a standard that will ultimately be shown – by persons with less noble intentions – to be ineffective.

The public harms that would result from this "squelching effect" could be significant and long-lasting. In the scenario sketched out above, for example, the inability of companies and individuals to reveal the vulnerabilities of the digital video specification early on could lead to significant industry and consumer investment in hardware and software devices that support the specification. The shortcomings of the specification might only be revealed as it

became evident that a large number of people were hacking around the controls in order to engage in unauthorized uses of protected content. As such persons are not generally inclined to publicize their successes in cracking security implementations, it might take some time for the weaknesses of the system to emerge. In the meantime, however, the industry may have made significant investments in devices that support the specification, thereby influencing consumer choices and shaping the structure of the market for the (allegedly) protected content. In the worst case, the slow demise of the specification as its weaknesses were revealed could require industry and consumers to invest in an entirely new standard, thereby starting the cycle all over again. Clearly, both industry and consumers – but mostly consumers – would have been better off if the vulnerabilities of the specification had been revealed early on by companies or persons whose only intention was to demonstrate the ineffectiveness of its security.

Recommendations

As this illustration demonstrates, there are compelling reasons to be concerned about the potentially detrimental impact of the anti-circumvention provisions of the DMCA and, in particular, about an overly-restrictive interpretation of Section 1201(g). EMusic.com believes that, in their report to Congress, NTIA and the Copyright Office should identify these concerns and ambiguities, and should propose specific interpretations of Section 1201(g) – if not outright legislative amendments – that would address these issues. In particular, the report should recommend that:

- Under Section 1201(g)(2)(C), the requirement of a "good faith effort" to obtain authorization for an attempted circumvention of a technological measure should not automatically preclude an individual from testing the technological measure if such authorization is denied, so long as the act of circumvention otherwise qualifies for the exception.

- Under Section 1201(g)(3)(A), the "dissemination" factor should be clarified so that an individual may benefit from the exception so long as he or she disseminates the results of his or her research without any apparent intention of facilitating infringement, as judged by the surrounding circumstances. In particular, the dissemination of information whose sole purpose is to criticize or reveal the shortcomings of a proposed or adopted standard should qualify the disseminator for the exception. Indeed, any other interpretation of Section 1201(g)(3)(A) would almost certainly violate the First Amendment.[1]

[1] It is well established that the First Amendment protects individuals from civil or criminal liability for the dissemination of information that could theoretically be used for an illegal purpose. It is only where speech is likely to incite "imminent lawless action," and is in fact intended to do so, that First Amendment protections do not apply. See, e.g., *Brandenburg v. Ohio*, 395 U.S. 444, 447 (1969). With one well-publicized exception, courts have never found that the mere publication of information that could facilitate the commission of a crime satisfies this standard. See *Rice v. Paladin Enterprises, Inc.*, 128 F.3d 233 (4th Cir. 1997) (publisher liable for murders facilitated by hit-man "how-to" manual, where manual was clearly intended for use by potential murderers). Plainly, then, the dissemination of information relating to the vulnerabilities of a cryptographic implementation is protected by the First Amendment. Congress seems to have recognized this fact in Section 1201(c)(4) of the DMCA, which states that "Nothing in this section shall enlarge or diminish any rights of free speech or the press for activities using consumer electronics, telecommunications, or computing products."

- Lastly, Section 1201(g)(3)(B) should be clarified so that the lack of formal training or employment in the area of information security is not an absolute bar to qualifying for the exception, so long as the act of circumvention otherwise qualifies for the exception.

EMusic.com greatly appreciates the opportunity to submit these comments on a matter of important public concern, and would be happy to meet with you and your respective offices to discuss these concerns in more detail.

Respectfully submitted,

Peter F. Harter
Vice President, Global Public Policy & Standards
EMusic.com, Inc.