Time Warner Inc.
75 Rockefeller Plaza
New York, NY 10019

July 26, 1999

Paula J. Bruening, Esq.
Office of Chief Counsel
National Telecommunications
and Information Administration
Room 4713
US Department of Commerce
14 Street and Constitution Avenue NW
Washington, DC 20230

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

Re: Section 1201 (g) of the Digital Millenium Copyright Act
(Docket No. 990428110-9110-01)

Dear Ms. Bruening and Mr. Feder,

I am grateful for the opportunity of submitting comments on behalf of Time Warner Inc. in response to the request for comments announced in the Federal Register Volume 64 No. 102.

Time Warner Inc is, as you know, one of the leading companies engaged in the production and distribution of copyrighted works including motion pictures and phonorecords. As such, it is vitally interested in adequate and effective protection of copyrights. In that connection, Time Warner devotes significant resources to fighting unauthorized uses of its copyrighted works in the United States and abroad.

Time Warner employs encryption technology in order to protect its audiovisual products from unauthorized uses and devotes significant resources to the development and implementation of protective technologies for its audio and audiovisual works. The Request for Comments seeks information with respect to, *inter alia*, the effects of Section 1201 (g) of the Digital Millenium Copyright Act on "protection of copyright owners against unauthorized access to their encrypted copyrighted works."

Section 1201 (g) which is headed “Permissible Acts of Encryption Research” provides that it is not a violation of Section 1201 (a) (1) (A) (which prohibits circumvention of technological measures that control access to protected works) for a person to circumvent a technological measure “in the course of an act of good faith encryption research” if certain criteria are met.

Among the criteria are (i) that such act is necessary to conduct such encryption research (Section 1201 (g) (2) (B)) and (ii) the researcher made a good faith effort to obtain authorization before the circumvention (Section 1201 (g) (2) (C)).

These provisions have the laudable purpose of supporting research into encryption and thus encouraging discovery of weaknesses in encryption systems that would render them ineffective as protectors of copyright. There are, however, threats to copyright protection that are apparent on the face of the provisions in question.

It is far too early (less than nine months after passage of the Digital Millenium Copyright Act) to have accumulated any hard evidence of the impact of Section 1201 (g) on protection of copyrights. Nevertheless, there has been sufficient history both prior to and since passage of the Act to warrant expressing a few cautions and some suggestions in connection therewith about the serious impact on copyright owners of misuse of “research” that could be encouraged by Section 1201 (g).

Where a copyright protection technology has been overcome, i.e. the encryption code broken, the “research” that led to that was not done by the iconic individual in his/her garage but, rather, by groups of persons having access to large computers in business or academic locations. Such research, more often than not, was not at the request or with the authorization of the owner of the encryption system or an authorized user thereof, and the motives for undertaking such “research” varied from scientific to pernicious.

Whatever the motives, because the “research” is not conducted by an isolated individual, word quickly gets around about how to break a particular encryption system.

When so-called “pirate smart cards” or similar devices are marketed, the advertising for them typically includes a disclaimer “for research only” – with much the same veracity as radar detectors for automobiles are advertised as “not intended to encourage speeding.”

What is needed in order to protect against “research” that has these damaging results are measures to assure that those who do the research are doing so for legitimate reasons and meet the criteria set forth in Section 1201 (g) (2) (A) –(D). Some factors to be used in determining whether a person qualifies for the exemption are set forth in Section 1201 (g) (3) but there are a few serious weaknesses in the regime so established which should be dealt with by an amendment or clarified by regulation.

Perhaps the most important requirement as a basis for exemption is that the person doing the research do so with actual written authorization of the owner of the encryption

system. There is no reason to suppose that owners of encryption systems would be unwilling to authorize legitimate researchers to test for weaknesses in the encryption systems. Leaving the criterion, however, at merely making "a good faith effort to obtain authorization" (Section 1201 (a) (2) (C)) could allow for illy motivated "researchers" to meet this qualification by sending off (or even claiming to send off) a letter, a fax or an e-mail which does not reach its destination. On the other side of this coin, such a requirement would impose on the owner of the encryption system a burden of attending to its mail, fax and e-mail communications with more speed than it may be able to muster.

Secondly, in this same context, the statute does not tell us what happens if a researcher does make "a good faith effort to obtain authorization" and the owner of the technology turns down the request. As suggested above, many of these problems could be resolved if actual written authorization were required.

Among the safeguards that would flow from a requirement for actual written authorization is the possibility that the owner of the technology might require, as a condition of granting authorization, that the researcher agree not to disclose any facts about the technology or about the results of the research. In the absence of such a non-disclosure agreement, the ability to break an encryption system becomes, as suggested above, widely known. Such a non-disclosure provision should be considered a reasonable condition of a grant of authorization.

Thank you for your consideration of these comments. My colleagues and I at Time Warner Inc. would be happy to meet with you to discuss these issues at your convenience.

Respectfully yours,

Bernard R. Sorkin
Senior Counsel