July 26, 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

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 Ms. Bruening and Mr. Feder:

The Business Software Alliance[*] (BSA) is please to provide the following remarks and observations in response to your request for comments on Section 1201(g) of the Digital Millennium Copyright Act. The Digital Millennium Copyright Act brings United States law into compliance with two new international treaties (the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty). The objective of these Treaties is, in part, to ensure the efficient development of Internet-based electronic commerce by providing certain legal protections to owners of copyright against theft and piracy.

BSA's member companies are the leading American developers of computer software and computing technologies. The remarkable development of the Internet is making it possible for these companies to make available and sell their computer programs online. Today, a consumer can locate and download a computer program through a series of simple clicks of a mouse. Unfortunately, this very same technology has also created a substantial and growing piracy problem on the Internet. To address this problem, many BSA members are relying on a variety of technological security measures to inhibit such theft. For example, companies are beginning to sell computer programs online, or plan to do so in the near future. For the user to gain access to the downloaded program, a separate decryption algorithm will need to be applied. Such decryption algorithms are sent to the purchaser through a separate e-mail.

[*] Since 1988, the Business Software Alliance (BSA) has been the voice of the world's leading software developers before governments and with consumers in the international marketplace. Its members represent the fastest growing industry in the world. BSA educates computer users on software copyrights; advocates public policy that fosters innovation and expands trade opportunities; and fights software piracy. BSA worldwide members include Adobe Systems Incorporated, Attachmate Corporation, Autodesk, Inc., Bentley Systems, Inc., Corel Corporation, Lotus Development Corp., Macromedia, Inc., Microsoft Corp., Network Associates, Inc., Novell, Inc., Symantec Corporation and Visio Corporation. Additional members of BSA's Policy Council include Apple Computer, Inc., Compaq Computer Corporation, IBM, Intel Corporation, Intuit Inc., and Sybase. BSA websites: www.bsa.org; www.nopiracy.com.

1150 18th Street, N.W., Suite 700, Washington, D.C. 20036
TEL 202.872.5500 FAX 202.872.5501 EMAIL info@bsa.org

BSA's member companies are also among the leading developers of technological security products, especially encryption technologies. These products are widely used to provide security at all levels of e-commerce transactions. They are applied to financial aspects of the sale, to the servers, and networks used to conduct the transaction, as well to the specific products.

For these reasons, the BSA's member companies have a strong interest in both the basic prohibitions on circumvention contained in Section 1201(a), as well as the defense for encryption research contained in Subsection (g).

It is our understanding that both the Senate Judiciary Committee and the House Commerce Committee have considered the impact Section 1201(a) might have on the progress of encryption sciences. Both Committees agreed that security was a key element necessary for the smooth evolution of electronic commerce. The Senate Judiciary Committee report phrased the issue as:

"…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…. The goals of Section 1201 would be poorly served if these provisions had the undesirable and unintended consequence of chilling legitimate research activities in the area of encryption."

This concern of the Congress was a result of the primary ways in which encryption sciences are advanced. It is usual for a new encryption technology to be subject to a variety tests to establish its robustness, and to determine whether the claims made by the developer are true and accurate. It is industry practice for the developer of the encryption technology to, in effect, invite "attacks" or testing of the technology, often offering bounties or cash rewards to those who find flaws. In some instances, such testing may be done without the specific consent or knowledge of the developer. Under those conditions, the Congress felt that such legitimate acts of testing might create a cause of action under section 1201, thus potentially chilling such research and testing.

In addition, as specifically highlighted in the Report of the House Commerce Committee, the software and computer tools used to conduct encryption testing may raise issues. So called "cracker" and "hacker" utilities, as well as programs used to recover lost passwords, are not prohibited provided they are used for the permitted purpose of good faith encryption testing. To further safeguard against abuse, both the Commerce Committee report and the Report of Conferees make clear that there are limits on the dissemination and use of the information obtained through such efforts.

Based on these considerations, Congress concluded that it was advisable to enact a limited encryption-testing defense to Section 1201, Subsection (g), to ensure that good faith testing of the robustness of encryption technologies did not run afoul of the law. In creating this defense, the Congress weighed two sets of facts (1) ensuring that the prohibitions on circumvention do not impede encryption research; and, (2) ensuring that the limited defense established by Section 1201(g) does not become perverted into a loophole for malfeasants intent on circumventing for purposes of piracy and theft.

It is our understanding, based on your note requesting comments and our analysis of the DCMA and the associated Committee and Conference reports, that you are to consider three issues: 1) the impact of the DCMA on the development of new encryption technologies; 2) the availability of technologies to protect against piracy; and, 3) whether changes need to be made to the DCMA.

Based on the experiences of the BSA's member companies — both as developers of encryption technologies, and as users of such technologies to prevent piracy of copyrighted software — that the provisions of Subsection 1201 (g) provide a sound balance, and that current marketplace experience does not require any changes to the law. We reach these conclusions based on the fact that an ever-growing variety of technological measures are now available to inhibit piracy. While the specific effectiveness of these measures varies, as a general matter, they are providing improving security. The companies that develop such technologies have not experienced specific problems of which we are aware in their development efforts attributable to the DCMA. For these reasons, and current developments in the marketplace, it is our current assessment that changes to the law are not needed.

We are prepared to provide any additional information you may need in making your report.

Sincerely,

Robert W. Holleyman, II
President and CEO