UNITED STATES SENTENCING COMMISSION

March 20, 2007 Hearing on
Proposed Amendments of Sentencing Guidelines, Policy Statements and Commentary

Statement of
Ric Hirsch, Senior Vice President, Intellectual Property Enforcement
Entertainment Software Association

Mr. Chairman and members of the Commission, thank you for the opportunity to comment on the January 30, 2007 proposed amendments of the Sentencing Guidelines, specifically Amendment 5 "Intellectual Property Re-Promulgation." ("Amendment"). The Amendment is being proposed, pursuant to the directive in the Stop Counterfeiting in Manufactured Goods Act, Pub. L. 109-81, to address, among other things, the adequacy of the Guidelines' definition of "infringement amount" to cover situations where "the item in which the defendant trafficked was not an infringing item but rather was intended to facilitate infringement," such as a circumvention device. As the entertainment software industry relies heavily on technological measures to protect its game software products from infringement, we have a great interest in the efforts of the Sentencing Commission to address the Sentencing Guidelines' treatment of those convicted of trafficking in circumvention devices in violation of 17 USC §1201.

I am testifying here on behalf of the members of the Entertainment Software Association (ESA). I am the ESA Senior Vice President, Intellectual Property Enforcement and, in that capacity, oversee the anti-piracy efforts that the association pursues on behalf of its members. The ESA serves the business and public affairs interests of companies that publish interactive games for video game consoles, personal computers, handheld devices, and the Internet. ESA members published more than 90 percent of the $7.4 billion in entertainment software sold in the United States in 2006. In addition, ESA's member companies produced billions more in exports of American-made entertainment software, helping to power a global game software market estimated to be approaching $30 billion in sales. The entertainment software industry is one of the nation's fastest growing economic sectors, more than doubling in size since the mid-1990s and in so doing, has generated thousands of highly skilled jobs in the creative and technology fields.

The entertainment software industry makes a tremendous investment in its intellectual property. For an ESA member company to bring a top game to market, it often requires a team of 40 to 50 professionals—sometimes twice that number—working for two or three years to fuse together the work of writers, animators, musicians, sound engineers, software engineers, and programmers into an end product which, unlike any other form of entertainment, is interactive, allowing the user to direct and control the outcome of the experience. On top of several million dollars in research and development costs, publishers will invest millions more to market and distribute the game. The reality is that only a small percentage of these titles actually achieve profitability, and many more never even recover their front-end R&D costs. Moreover, the commercial life of a video game is quite short compared to other entertainment content, as the average video game is estimated to earn roughly 75% of its total revenues in the two-month

period following its release. In this type of market, it is easy to understand how devastating piracy can be as it siphons off the revenue required to sustain the high creative costs necessary to produce successful products.

For this reason, and the susceptibility of digital content to widespread abuse and infringement, ESA members have invested heavily in the use of technological measures that are designed to prevent the piracy of their game software products. Such measures help to reduce the infringement of their software titles by restricting access to, or preventing the copying of, their digital content. Some of these measures are embedded in the disks or cartridges on which game publishers publish their games. Others are incorporated into the game consoles on which game software is played. The game consoles generally use access control measures through an authentication system that locks the machine out from playing an illegitimate copy of a game. In each case, members of the game software industry have taken affirmative steps, some involving significant expense, to preclude the infringement of their digital software products.

Congress recognized the important role that technological protection measures play in controlling the piracy of digital content when it enacted the Digital Millennium Copyright Act ("DMCA") in 1998. The provisions of this legislation, codified under 17 USC §1201, prohibit the circumvention of such measures and criminalize the activities of those engaged in the manufacture or trafficking of devices used to circumvent such measures, with "access protection" measures covered under §1201(a)(2) and "copy protection" measures covered under §1201(b).

Notwithstanding the enactment of the DMCA, because of the strong appeal of video games and the business opportunity that the popular demand for games fosters, the "hacker" community has targeted the technological protection measures used by the game software industry. Many of these "hackers" are resident abroad and are thus beyond the purview of the DMCA's prohibitions. With few exceptions, almost every game console system launched since the early 1990's has had its protection technology compromised within six to nine months of its release, sometimes sooner. As an example, the popular Wii game console, launched by Nintendo just this past November, has recently seen its security measures hacked. This track record is not a function of the low robustness or sophistication of the technological protection measures used in these systems, as most of these technological measures are quite technologically advanced, particularly the ones found in recent consoles. It is, rather, a result of the illicit profits to be made from the creation and commercialization of circumvention devices that will bypass such measures and permit pirate versions of games to be played on these consoles.

The most prevalent forms of circumvention devices are semi-conductor chips that modify the lock-out systems incorporated into game consoles. Each game console system has its own proprietary technological measures, so that the measures used on the Microsoft Xbox are different from the ones used in the Sony PlayStation 2. In addition, with new generations of consoles, the console companies have designed and incorporated into their newer consoles new and improved access-control technologies, so that the Xbox 360 has a different set of protection measures from the Xbox. Unfortunately, despite the investments made in improving such technological protections, hackers have succeeded in compromising each of these systems through the development of chips that, when installed in the console (by either the owner or any

of the many service providers who will do so for a fee), modify the console's processes to bypass its authentication system and thereby enable it to play an illegal copy of a game. These modification chips are commonly referred to as "mod chips." Once installed in a game console, a mod chip will allow that console to play an unlimited number of pirate copies of the games designed for that console. Different mod chips are designed and made to work on different game consoles, with some consoles suffering from several different mod chips designed to work to circumvent its security measures.

Since the enactment of the DMCA, the entertainment software industry has supported enforcement of its provisions against individuals and enterprises in the United States engaged in the trafficking of mod chips and other circumvention devices. In most cases, when the defendants have been engaged in pirate activities in addition to the sale and installation of circumvention devices, federal prosecutors have been more likely to charge the defendants with copyright infringement than with violations of the DMCA, even though the latter activities are ultimately responsible for more harm being done to rights holders. While ESA and its members are appreciative of the cases brought against these individuals, there is the sense that prosecutors might be more inclined to charge defendants with DMCA violations if an enhanced level of punishment were recommended for such crimes.

Unfortunately, ESA's investigations into game piracy across the United States over the past years have seen an increase in the number of enterprises that will offer to sell or modify game consoles, without any other infringing activities, such as the sale of copies of pirate game software. So, there appear to be an increasing number of individuals and enterprises engaging only in circumvention activities with respect to game consoles and thus subject only to charges of violating the DMCA. While these enterprises are usually not large, there are many of them and they can be very active, with some of these businesses estimated to take in several thousands of dollars per month.

Thus, the Sentencing Commission's Amendment to enhance the level of punishment available against individuals convicted of DMCA violations is very timely and could serve to increase the level of deterrence against mod chip enterprises.

ESA has reviewed the three options outlined in the Amendment. Of the three, Option 1 seems to offer the best approach for enhancing the level of punishment for trafficking in circumvention devices. Option 1 provides for a two or more level enhancement to a minimum level of 12 for anyone convicted of "trafficking in devices used to circumvent a technological measure." The approach underlying Option 1 provides a simple and straightforward recognition of the greater amounts of infringement that circumvention devices facilitate. The only deficiency ESA has identified within Option 1 is that it applies only to defendants convicted under §1201(b), which covers only trafficking in devices that circumvent copy-protection measures, rather than §1201 generally, or §1201(a)(2) additionally, which would cover defendants convicted of trafficking in devices that circumvent access controls, which are what mod chips effectively circumvent. We would recommend that the Commission reconsider the coverage of Option 1 to include all convictions under §§1201 and 1204. This is consistent with the scope of coverage in other portions of the Amendment.

By contrast, in the context of game piracy and mod chips for game consoles, Option 2 understates the value of the "infringement amount" as it uses a calculation that factors the average retail value of the circumvention device multiplied by the number of such devices. As most mod chips retail for $30-50, equivalent to the retail value of one legitimate game, such a calculation produces a minimal infringement amount. Given that the installation of a mod chip in a game console facilitates dozens of infringements (i.e., the number of pirate games played on a console, after it has been modified), the retail value of each mod chip is a fraction of the value of the damage it inflicts on legitimate game sales.

While Option 3 attempts to address this understatement by offering an alternative formulation, it does so in a way that makes it very difficult to calculate the "infringement amount." Option 3 specifies that the infringement amount is the greater of the amount calculated under Option 2's formula or the number of circumvention devices "multiplied by the price a person legitimately using the device to access or make use of a copyrighted work would have paid." In the context of someone convicted of trafficking in mod chips, such a calculation would require that a federal judge make a judgment on how many pirate games a person using a mod chip would play and then multiplying that by the retail value that the person would have paid for legitimate versions of those games. This is an extremely difficult and conjectural calculation, as it requires an assessment of how many pirate games are played by those using mod chips and then requiring a deep knowledge and understanding of retail game software prices. ESA sees this calculation as extremely difficult to make and, for that reason, fears that such a formulation is imprecise and could result in an infringement amount that is disproportionately low.

ESA would also like to take this opportunity to address the two issues raised for comment at the end of the proposed amendment.

The Commission has requested comment on whether it should "provide a downward departure provision for cases in which the infringement amount overstates the seriousness of the offense." ESA would suggest that no such provision is required as its experience is that, in most cases involving intellectual property infringement, the infringement amount understates the seriousness of the offense, rather than the opposite. In the few cases, where the seriousness of the case is overstated by the infringement amount, ESA believes that federal judges already factor this into their determination of the punishment to be imposed. ESA does not see the need for any additional provision embodying a principle already being applied in practice.

The Commission has also asked for comment on Application Note 4 providing for an adjustment to be made under §3.B1.3 "in any case in which the defendant deencrypted or otherwise circumvented a technological security measure to gain initial access to an infringed item." The Commission has received comment that not every de-encryption or circumvention requires a "special skill" as defined in §3.B1.3. The ESA's comment is that the Commission should not make any change to Application Note 4 as it sees this as applying to de-encryptions and circumventions of technological measures to gain "initial" access to protected content. Such instances of de-encryption and circumvention where initial access to protected content is achieved describes situations where hackers have achieved the first breakthrough in compromising a technological measure. As opposed to some less complex acts of circumvention, these "cracks" in security measures invariably do require "special skills." In the

game software context, these initial "cracks" of protected game software are performed by groups of individuals working together through the Internet, commonly known as "warez" groups. These groups will "crack" the copy protection of a newly released game (sometimes, even prior to release), strip out the protection technology and then release an unprotected downloadable version for dissemination on the Internet. Within days, if not hours, thousands of copies are being copied and downloaded throughout the Internet. The "crackers" in these groups are individuals with high technological skills who able to figure out how to penetrate the security measures in order to access the digital content of game software and would thus meet with the "special skills" requirements of §3.B1.3. As ESA believes that Application Note 4 is intended to cover such activity, in accordance with the purposes of the No Electronic Theft (NET) Act, it would recommend that the Commission not make any change in such Application Note.

ESA is grateful for the Commission's efforts reflected in the Proposed Amendment to address this important aspect of the law governing enforcement against digital piracy and is appreciative of this opportunity to provide its comments on such efforts.