

March 30, 2007

The Honorable Ricardo H. Hinojosa  
United States Sentencing Commission  
One Columbus Circle, NE  
Suite 2-500  
Washington, DC 20002-8002

Re: Comments on Proposed Amendment 5 to Sentencing Guidelines Relating to Criminal  
Copyright Infringement

Dear Judge Hinojosa:

The Entertainment Software Association ("ESA") thanks the Sentencing Commission for the opportunity to comment on the January 30, 2007 amendments of the Sentencing Guidelines, specifically Amendment 5 "Re-Promulgation of Emergency Intellectual Property Amendment" ("Amendment"). The Amendment is being proposed, pursuant to the directive in the Stop Counterfeiting in Manufactured Goods Act, Pub. L. 109-181, to address, among other things, the adequacy of the Sentencing 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.

With the increased incidence of circumvention of the security technologies of video game consoles, we believe it is indeed timely to assess whether current criminal penalties for violations of the anti-circumvention provision of the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. §1201, are adequate to deter those who facilitate video game piracy through circumvention activities. We welcome this opportunity to offer our perspective.<sup>1</sup>

**A. The ESA and the Video Game Industry**

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

---

<sup>1</sup> I testified on behalf of the ESA at the March 20, 2007 hearing before the Sentencing Commission.

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, a publisher will invest millions more to market and distribute a video game. The reality is that only a small percentage of these titles actually achieve profitability, with many never even recovering 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.

## **B. The DMCA and Video Game Piracy**

Congress recognized the important role that technological measures play in controlling the piracy of digital content when it enacted the DMCA in 1998. The DMCA discourages the development and dissemination of technological burglars' tools that threaten the copyright industries. The DMCA implements two 1996 World Intellectual Property Organization ("WIPO") treaties: the WIPO Copyright Treaty, and the WIPO Performances and Phonograms Treaty. The purpose of this measure was to make digital networks safe places to disseminate copyrighted works for the benefit of consumers, the global economy, and copyright owners. The DMCA prohibits the circumvention of technological protection measures and criminalizes 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. Hackers are skilled programmers and technicians who are adept at breaching security systems and gaining unauthorized access to software and other content. Once they discover the way into a system or protected content, they often share this knowledge with other hackers, amplifying the potential damage to the victim. 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 seen its security measures hacked in just a few months. 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 protections are quite 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 bypass such measures and permit pirated versions of games to be played on these consoles.

Indeed, in the wake of each and every "hack" of a console's security technology, there inevitably follows widespread dissemination and sale of circumvention devices that exploit that hack. This, in turn, leads to a mushrooming of pirated games infesting the marketplace. For every step removed from the original hack, there is an ever widening circle of economic damage to the copyright owner. This is why it is vital to focus on the punishing and deterring of those who distribute piracy-enabling technologies.

The most prevalent forms of circumvention devices are semi-conductor chips that modify the lock-out systems incorporated into the consoles.<sup>2</sup> Each game console system has its own proprietary technological measures, so that the measures used in the Microsoft Xbox are different from the ones used in the Sony PlayStation 2. In addition, with each successive generation of consoles, the console makers have designed and incorporated into their console systems the latest access-control technologies, so that the Xbox 360 has a different, more sophisticated set of protection measures from the Xbox. Unfortunately, despite the enormous and continual investments made in state-of-the-art 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 console owner or any number of back alley chip jockeys who will do so for a fee), modify the console's processes to bypass its authentication system and thereby enable it to play illegal copies of games.

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 pirated copies of the games designed for that, and in some instances, other console(s). Different mod chips are designed and made to work on different game consoles. Mod chips are engineered as custom-tailored workarounds for a particular video game system's copy protection and access control systems and, as such, play a crucial role in furthering piracy.

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 charged defendants with both DMCA violations and copyright infringement. Recently, ESA's investigations into game piracy across the United States have seen an increase in the number of enterprises that will offer to sell mod chips or modify game consoles, without directly engaging in copyright infringement. This may be attributable to a perception among such illegal businesses that installing mod chips is less likely to attract the attention of law enforcement than enterprises that engage in more direct forms of software piracy. 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 tend to be very active, with many of these businesses estimated to take in several thousands of dollars in sales per month.

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

---

<sup>2</sup> Mod chips are only one of the tools used to circumvent console copy-protection and access controls. Unauthorized bypass may also be accomplished through the assistance of software, such as Swap Magic, that tricks the console into thinking that a bootleg copy is legitimate. Creating the bootleg copies themselves involves yet other software used to replicate the disc embodying the game.

### C. Option 1

Of the three options outlined in the Amendment, the ESA believes Option 1 offers the best approach for determining 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.” Trafficking in circumvention devices inevitably results in more pirated copies of games making their way into the stream of commerce. Thus, we agree that trafficking in circumvention devices warrants an elevated penalty comparable to that which currently applies to those who upload, manufacture, or import infringing copies. We also agree that establishing a minimum sentencing level of 12 will provide a useful benchmark for judges.

The Sentencing Commission’s approach to calculating the “infringement amount” under Option 1 is conceptually attractive. It involves multiplying the number of accessed works by the “price the user would have paid to access lawfully the copyrighted work.” In theory, this would provide a straightforward means of assessing the economic harm to the copyright owner. But arriving at the correct data points to insert into that calculation could be problematic, particularly where the person has sold mod chips or modified consoles but has not “accessed” pirated copies of games.

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 pirated games a person using a mod chip would play and then multiply that figure by the retail value the person would have paid for legitimate versions of those games. This is a difficult and conjectural calculation, as it requires an assessment of how many pirated games are played by those using mod chips and then requiring a deep knowledge and understanding of retail game software prices. ESA fears that such a formulation will often result in an infringement amount that is disproportionately low. That being said, we agree with the Sentencing Commission that the two-level enhancement and a “floor” offense level of 12 are necessary to establish the gravity of the offense, regardless of the infringement amount.

We suggest one modification to Option 1. It should be expanded to embrace all of §1201, and not just §1201(b). That particular section of the DMCA covers only trafficking in devices that circumvent copy-protection controls. It does not reach those who circumvent access controls, which is covered under §1201(a)(2) of the DMCA. Through its parallel prohibitions, the DMCA recognizes that the circumvention of access controls (the means by which mod chips further piracy) is just as damaging to copyright owners as circumvention of copying controls.

A bootleg copy of a game played upon a modified console requires the infringer to bypass both the copy-control/access control features of the game as well as the copy-control/access control features of the playback hardware. For this reason, both forms of circumvention facilitate copyright infringement.<sup>3</sup> The Sentencing Guidelines should reflect this reality,<sup>4</sup> just as the DMCA does.

Technologies that protect games also benefit consumers. For example, protection technologies permit publishers to distribute "try before you buy" game demos. These allow consumers to experiment with playing a game to see if they like it before purchasing it. Absent the ability to protect the conditional access technology that permits such sampling of game content, these free offerings to consumers might vanish. Additionally, unlike any other type of software, consumers enjoy the opportunity to rent video games. This would not be economically feasible were it not for security technologies that mitigate the risk of rampant piracy resulting from such rentals.<sup>5</sup>

#### **D. Options 2 & 3**

Options 2 and 3 are problematic and therefore less preferable than Option 1.

Option 2 understates the value of the "infringement amount" as it uses a calculation that factors the 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 pirated games played on a console after it has been

---

<sup>3</sup> Infringement does not benefit rights holders, consumers, and the economy, as some have claimed. Money paid for pirated copies does not go to copyright owners. Sales of pirated software depress demand for genuine copies. The less revenue a game publisher earns, the less money it has for hiring new people, investing in new equipment, and bankrolling further projects. Also, these off-the-book transactions deprive states and localities of tax revenues.

<sup>4</sup> Some have argued that the penalty imposed by Option 1 may result in criminal penalties even absent actual copying or distribution of a copyrighted work. But this assertion fails to recognize that actual copying or distribution is not an element of a violation under Section 1201. It also does not account for the reality that most people use these circumvention technologies for infringing purposes.

<sup>5</sup> Under federal law, video games are the only form of software that may be rented without the permission of the copyright holder, and over the years video game rentals have become a huge business, generating over \$558 million in 2006. The threat of significant criminal penalties for circumvention is a necessary deterrent to discourage the unauthorized use of rental copies as source material for the creation of infringing copies, which would require circumvention of technological protection measures.

modified), the retail value of each mod chip is a fraction of the value of the damage it inflicts on legitimate game sales.<sup>6</sup>

One commenter suggested that the Sentencing Commission could expand Option 2 to include enhanced punishment for those convicted under §1201(b) who also copied or distributed the copyrighted work. We see no sound reason to limit any such enhancement only to those who have engaged in copying or distribution of a copyrighted work. To impose an actual infringement requirement would leave out a large swath of culprits: those who put piracy-enabling technologies into the hands of bootleggers. Traffickers are no less culpable than bootleggers. Besides, the DMCA “de-links” circumvention from actual infringement. It would frustrate the purpose of that statute to adopt a contrary view in the Sentencing Guidelines.

While Option 3 attempts to address the understatement problem 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.” These calculations suffer from the same ambiguities we cited in our comments to Option 1. If, in any event, the Sentencing Commission adopts Option 3, at the very least it should expand its scope to cover all of §1201.<sup>7</sup>

#### **E. Issues for Comment**

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

The Sentencing 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 it is ESA’s experience that, in most cases involving intellectual property infringement, the infringement amount *understates* the seriousness of the offense, rather than the opposite. In the rare instance, where the seriousness of the case might be overstated by the infringement amount, ESA believes that federal judges already factor this into their

---

<sup>6</sup> See, e.g., Press Release, Department of Justice, Game Store Owners Charged with Copyright Infringement for Selling Modified Xbox Systems with Pirated Games (Dec. 19, 2005) (defendant agreed to install a mod chip and new hard drive on an Xbox console and load it with 77 pirated games for \$265) available at <http://www.cybercrime.gov/jonesCharge.htm>.

<sup>7</sup> Before moving on to the “Issues for Comment,” ESA takes this opportunity to address one final point with respect to the calculation of the infringement amount. The suggestion offered by one commenter that prosecutors are uninvolved in reviewing industry’s figures when computing the “infringement amount” is inaccurate. In our experience, a prosecutor is deeply involved in collecting and reviewing industry data for a case well in advance of sentencing. It is the prosecutor, not the video game industry, who is responsible for calculating the infringement amount.

determination of the punishment to be imposed. ESA does not see the need for any additional provision in the Sentencing Guidelines embodying a principle already being applied in practice.

The Sentencing Commission has also asked for comment on Application Note 4 providing for an adjustment to be made under §3B1.3 "in any case in which the defendant de-encrypted or otherwise circumvented a technological security measure to gain initial access to an infringed item." The Sentencing Commission has received comment that not every de-encryption or circumvention requires a "special skill" as defined in §3B1.3. The ESA's comment is that the Sentencing 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, generally refers to 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 are able to figure out how to penetrate the security measures in order to access the digital content of game software and would thus meet the "special skills" requirements of §3B1.3. As ESA believes that Application Note 4 is intended to cover such activity, in accordance with the original statutory purposes of the No Electronic Theft (NET) Act, it would recommend that the Sentencing Commission not make any change in such Application Note.

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

Sincerely,

A handwritten signature in black ink, appearing to read "Ric Hirsch", written in a cursive style.

Ric Hirsch  
Sr. Vice President, Intellectual Property Enforcement  
Entertainment Software Association