UNITED STATES COPYRIGHT OFFICE

Long Comment Regarding a Proposed Exemption Under 17 U.S.C. § 1201

Please submit a separate comment for each proposed class.

[ ] Check here if multimedia evidence is being provided in connection with this comment

ITEM A. COMMENTER INFORMATION

DVD Copy Control Association

The DVD Copy Control Association ("DVD CCA"), a not-for-profit corporation with its principal office in Morgan Hill, California, licenses the Content Scramble System ("CSS") for use in protecting against unauthorized access to or use of prerecorded video content distributed on DVD discs. Its licensees include the owners of such content and the related authoring and disc replicating companies; producers of encryption engines, hardware and software decrypters; and manufacturers of DVD players and DVD-ROM drives.

Advanced Access Content System Licensing Administrator

The Advanced Access Content System Licensing Administrator, LLC ("AACS LA"), is a cross-industry limited liability company with its principal offices in Beaverton, Oregon. The Founders of AACS LA are Warner Bros., Disney, Microsoft, Intel, Toshiba, Panasonic, Sony, and IBM. AACS LA licenses the Advanced Access Content System ("AACS") technology that it developed for the protection of high definition audiovisual content distributed on optical media. That technology is associated with Blu-ray Discs. AACS LA's licensees include the owners of such content and the related authoring and disc replicating companies; producers of encryption engines, hardware and software decrypters; and manufacturers of Blu-ray disc players and Blu-ray disc drives.

As ultra-high definition products are entering the marketplace, AACS LA has developed a separate technology for the distribution of audiovisual content in ultra-high definition digital

format. This technology is identified as AACS2, and not AACS 2.0. This distinction in nomenclature is significant, as the latter would suggest that it replaced AACS distributed on Blu-ray. It has not. AACS2 is a distinct technology that protects audiovisual content distributed on Ultra HD (UHD) Blu-ray discs, a distinct optical disc format which will not play on legacy (HD) Blu-ray players. To the extent a proposal mentions CSS and/or AACS, but does not explicitly include AACS2, such mention should not be inferred to include AACS2. Indeed, AACS2 is not subject to the proposed exemptions put forward by any Class 11 proponents.

REPRESENTATIVES

COUNSEL TO DVD CCA AND AACS LA:

Michael B. Ayers
Michael B. Ayers Technology Law
5256 S. Mission Rd., Suite 703-2215
Bonsall, CA 92003-3622
michael@ayerstechlaw.com
(760) 607-6434

Dean S. Marks
13236 Weddington St.
Sherman Oaks, CA 91401-6036
deansmarks@yahoo.com
(818) 469-7185

David J. Taylor
Right Size Law PLLC
621 G ST SE
Washington, DC 20003
david.taylor@rightsizelaw.com
202-546-1536

ITEM B. PROPOSED CLASS ADDRESSED

Proposed Class 11: Computer Programs — Jailbreaking

ITEM C. OVERVIEW

DVD CCA and AACS LA object to the proposed class to the extent that it could be read to permit circumvention of DVD and Blu-ray players.

ITEM D. TECHNOLOGICAL PROTECTION MEASURE(S) AND METHOD(S) OF CIRCUMVENTION

The TPMs of concern to DVD CCA and AACS LA are the Content Scramble System ("CSS") used to protect copyright motion picture content on DVDs and the Advanced Access Content System ("AACS") used to protect copyrighted motion picture content on Blu-ray Discs.

ITEM E. ASSERTED ADVERSE EFFECTS ON NONINFRINGING USES

Outline of Discussion

I. *Introduction*

DVD CCA and AACS LA object to the proposed class to the extent it is intended to create an exemption that would permit circumvention of technical protection measures ("TPMs") of DVD and Blu-ray players. Manufacturers are incorporating streaming functionality into DVD and Blu-ray players; and, while proponents have not specifically identified optical disc player devices, as explained below, their discussion suggests that the proposed class (i) could include such players generally and (ii) most certainly includes such players which incorporate streaming functionality. For similar reasons provided in the other proposed classes, this class is impermissibly broad, as it will swallow any device that connects to a TV for viewing content. Jailbreaking a device contemplates modification of the device, and the precedent of this proceeding has not found jailbreaking (repair or modification) to be noninfringing in the most relevant context, which is repair and modification of video game consoles – a proposed class addressing devices that make use of expressive copyrighted works (video games) in a similar manner that players make use of motion pictures. That precedent also makes clear that the statutory factors do not warrant the creation of an exemption for the proposed class. While the proposed class should be denied for the foregoing reasons, should the Register nonetheless find that an exemption is warranted, then the Register should refine the exemption to exclude DVD and Blu-ray players, as the proponents have not proffered any evidence with respect to these devices.

A. The Robustness and Compliance Rules Preserve DVD and Blu-ray Player Content Protection

Modification of DVD and Blu-ray players, including jailbreaking, whether done clumsily or skillfully, can disrupt DVD and Blu-ray players manufacturers' efforts to comply with the robustness and compliance rules which they are obligated to implement in their devices. As DVD

CCA and AACS LA have explained in comments relative to other current proposals,[1] these devices are an integral aspect of a secure digital ecosystem promoting the distribution of high-quality content to consumers. To preserve the integrity of the digital ecosystem, licensed manufacturers must build their playback devices in compliance with requirements that these devices resist "attacks" that (i) jeopardize the technological protection measures employed to protect the content or (ii) would otherwise permit access to the product's signal when content is "in the clear" (unencrypted) passing from one device element to the next. These requirements are set forth in what are generally called "robustness rules". As jailbreaking a streaming device is just another way to describe permitting modification of the device, jailbreaking presents the identical harm to the security of DVD and Blu-ray players, particularly as such modifications would certainly undo those manufacturer design elements, developed in compliance with the robustness rules, leaving the technological protection measures compromised and/or the unencrypted content exposed.

The integrity of the digital ecosystem also depends on preserving the particular distribution offering that rights holders have intended to offer to consumers. For example, digital copies of motion pictures distributed on DVD or Blu-ray discs should not "leak" into other distribution models and displace those other models rightsholders intend to offer to consumers. Accordingly, manufacturers wanting to participate in a particular distribution platform, such as the production and sale of DVD or Blu-ray disc players, agree to rules governing how these products will handle the content entrusted to their products, namely, by specifying some boundaries regarding the products' functionality. For instance, such rules require that when the content on the optical disc

[1] Those other proposals that DVD CCA and AACS LA are objecting to with like or similar objections are Class 12, which would permit circumvention for the purpose of repair or modification of software-enabled devices, and Class 16, which would permit circumvention for FOSS-dependent devices.

is decrypted by the player for transmission in full resolution via a digital output to another device, such as a screen, it must be re-encrypted with another specified TPM that serves to maintain the protection provided by the original TPM. Further, such rules require that any decrypted content going out certain outputs (*e.g.,* unprotected analog outputs) be at something less than the maximum possible audio and/or video resolution. These requirements prescribing how protected content should be handled are embodied in what are referred to as "compliance rules," and the compliance rules are intended to keep copies of copyrighted works distributed on any one particular platform from swallowing up other distribution models. The proponents explain the ability to access and exercise "root privileges" is determined by "access controls that can be configured to restrict access to nearly any of a device's functions, including the ability to add or remove software from a device."[2] What proponents identify as the means to modify the device to permit the ability to add additional software also makes it possible to alter the content protection functions of DVD and Blu-ray players that manufacturers use to limit the functionalities of those devices in accordance with the applicable compliance rules. Consequently, the proposed jailbreaking would permit activities that are contrary to the manufacturers' obligations to limit certain device functionalities as required under the compliance rules.

Any circumvention enabling jailbreaking of DVD or Blu-ray players poses the same risk identified in the other classes, namely exposing player decryption keys or compromising some other element intended to comply with the applicable robustness or compliance rules. Jailbreaking disrupts the careful licensing arrangement between rights holders and manufacturers. It introduces the possibility that decryption keys will be discovered and misused, or other elements compromised, and, ultimately, it threatens the very integrity of the digital ecosystem protecting

[2] EFF Initial Comments at 5.

high-value audiovisual content being offered to consumers. Therefore, DVD CCA and AACS LA object to the proposal to permit circumvention for purpose of jailbreaking streaming devices to the extent it may also be read to permit the circumvention of DVD and Blu-ray players.

II. *The Proposed Class Does Not Constitute A Proper Class*

A. The Requests Would Go Beyond the Statutory Limitation Requiring Exemptions from This Rulemaking to Apply Only to Those Beneficiaries Specifically Determined Pursuant to the Rulemaking

Congress created a temporary exemption for persons in situations for which the Librarian has "determined, pursuant to the rulemaking …," that such persons "are, or are likely to be, adversely affected" by virtue of the circumvention prohibition "in their ability to make noninfringing uses . . . ."[3] The statute thus limits the rulemaking to exempt certain uses from the general prohibition against circumventing TPMs based on the determination resulting from the rulemaking proceeding. The plain language of the statute requires identification of the persons who are adversely affected and a determination based on the rulemaking that those adverse effects exist in relation to noninfringing uses. There are to be no beneficiaries of the exemption based on vague references or suggestions. In this context, the proponents are not adversely affected, as the use they seek to make is unwarranted and there are alternatives to circumvention.

The House Commerce Committee, which created the rulemaking during its consideration of the WIPO treaties, which, in part, became Section 1201, did not contemplate a regulatory proceeding that would result in broad waivers to the general circumvention prohibition, such as an exemption for any and all fair use under Section 107, or for any and every activity permitted under Section 110 (1) (the classroom exception). Instead, the Committee foresaw "selectively waiv[ing]

[3] Section 1201(a)(1).

[the prohibition against circumvention] for limited time periods, . . . for a particular category of copyrighted materials."[4]

Not only did the Committee envision any exemption to be selective and particular, but also that the exemption would be fully evaluated in the rulemaking (in keeping with the statutory requirement that the exemption be "pursuant to the rulemaking"). The Commerce Committee Report instructs that any exemption resulting from the rulemaking is to flow from the "development of a sufficient record as to how the implementation of these technologies is affecting the availability of works in the marketplace for lawful uses."[5] Most importantly, the Committee was quite clear that "the rulemaking proceeding should focus on distinct, verifiable and measurable impacts, [and] should not be based upon de minimis impacts . . . ."[6] This instruction alone would render the current request – if it intended to permit circumvention of any device that connects to a TV - impossible to grant, as the proposed exemption for any device that connects to a TV display is so broad and unbound that it is incompatible with the mandate for evidencing "distinct, verifiable and measurable impacts."

Congress' final direction was that a particular class of work should "be a narrow and focused subset of the broad categories of works of authorship than is identified in Section 102 of the Copyright Act (17 U.S.C. § 102)."[7] Clearly, the broad and unbounded class proposed by the proponents here cannot be considered "narrow and focused" as Congress demands.

---

[4] House Commerce Committee Report at 36.

[5] House Commerce Committee Report at 37.

[6] *Id.* at 37.

[7] *Id.* at 38.

1. Similar Proposed Classes Have Been Rejected

Whether the intended class is all devices that connect to a TV, or just "streaming devices", the proposed class is too broad. The scope of the class and the evidence supporting the class are fundamental to the rulemaking and were the basis of questions the Copyright Office raised in the NPRM, which "asked for regulatory language to define the types of devices that would be covered."[8] Proponents have proffered broad language for their proposed class of devices: "computer programs on devices that are primarily designed to display software applications on a screen, including applications that stream video delivered via the Internet, where such devices connect to but are not physically integrated into a display."[9] This language appears to implicate a DVD or Blu-ray player with streaming functionalities, and it certainly describes DVD and Blu-ray players that typically "connect to but are not integrated a display." This same description, which describes DVD and Blu-ray players, could also be applicable to DVRs, video game consoles, Kodi boxes, other casting devices, and even mobile phones. Proponents, however, only discuss Amazon Fire TV, the Apple TV, and the Roku, all very similar devices, and that discussion cannot form the factual basis to include a myriad of other television peripherals (*i.e.*, devices that connect to, but are not physically integrated into, a display). Consequently, the proposed class is overly broad.[10]

---

[8] Exemptions to Permit Circumvention of Access Controls on Copyrighted Works 85 Fed. Reg. 65293, 65396 (Oct. 15, 2020) (quotation omitted) (Notice of Proposed Rulemaking "NPRM").

[9] EFF Initial Comments at 2.

[10] Over-the-Top ("OTT") is also an elusive term, as it too refers to a broad and varied array of devices. Pixalate, the major advertising aggregator in the OTT market, describes OTT devices that its services presumably would extend to as "[a]ny device that is not desktop, laptop, or mobile but is used to consume OTT content. Examples include Smart TVs, Apple TVs, Chromecast, PlayStation, Xbox, Amazon Fire sticks, and other streaming devices." What is OTT and how is it different from video? Pixalate, Blog, available at https://blog.pixalate.com/what-is-ott-connected-tv-video.

When a class is overly broad, such as the instant proposed class is, the question becomes whether a permissible class may nonetheless be refined from the record. In the 2018 rulemaking, which expanded the 2015 repair exemption for motor vehicles to several other categories of devices, the Acting Register searched the record evidence to come forward with unifying elements to establish the class. She explained:

> it is not clear whether "devices," generally, share enough commonalities for the Acting Register to evaluate whether access controls are, in practice, adversely affecting noninfringing uses. The rulemaking record lacks a minimum quantity of evidence for a broad panoply of the devices that proponents' reference, let alone those which are not introduced but would fall under the proposed exemption. Outside of the vehicle context, the information provided is sparse regarding specific types of devices where TPMs inhibit repair or modification activities, with initial comments providing only cursory notice of devices considered by proponents as "relevant" to the exemption. [Notwithstanding] lengthy lists of specific devices that "could be configured to include technological protection measures that would prevent independent maintenance and repair," for many categories, it is still unclear whether TPMs are typically applied to these devices.[11]

In light of the shortcomings in the record, the Register "refine[d] the class based on the types of devices for which there is a cognizable record."[12]

In the instant case, there is no additional information, let alone a cognizable record, as to how the class may extend beyond the specific examples, and certainly not to the proposed class, which may implicate a far wider array of television peripherals. The lack of additional information becomes more problematic with the absence of information about particular TPMs and an explanation as to how circumvention facilitates any noninfringing use.

Identifying the device and the particular TPM utilized is more than a ministerial element of the rulemaking. It goes to the heart of whether circumvention is required or prohibited under Section 1201, and, ultimately, whether any prohibition is adversely affecting a noninfringing use.

---

[11] 2018 Recommendation at 191-92.

[12] *Id.*

For example, in *Lexmark v. Static Control Components*,[13] the Sixth Circuit reversed the District Court on the question of whether, in fact, circumvention had occurred:

> It is not Lexmark's authentication sequence that "controls access" to the Printer Engine Program. See 17 U.S.C. § 1201(a)(2). It is the purchase of a Lexmark printer that allows "access" to the program. Anyone who buys a Lexmark printer may read the literal code of the Printer Engine Program directly from the printer memory, with or without the benefit of the authentication sequence, and the data from the program may be translated into readable source code after which copies may be freely distributed.[14]

Lexmark demonstrates that the possible implementation of a TPM does not automatically mean every alleged act of circumventing a TPM is prohibited under the DMCA. Thus, the rulemaking has been fundamentally correct in requiring some information and detail as to the device, the TPM in use, and how circumvention would occur. Absent that information, there is no basis to conclude that the circumvention prohibition is adversely affecting any noninfringing use.

2. No Evidence is Offered for a Class to Include DVD and Blu-ray Products

Furthermore, proponents have not introduced any information sufficient to include DVD or Blu-ray playback devices in the proposed class. Thus, even if a determination is made that a class is warranted, the class should explicitly exclude DVD and Blu-ray players.

[13] *Lexmark Intern. v. Static Control Components*, 387 F.3d 522 (6th Cir. 2004).

[14] *Lexmark*, 387 F.3d at 546-47.

III. *The Proposed Use Is Not Permissible Under Fair Use.*

A. Modification Implicates the Derivative Right of Software, and Reverse Engineering Case Law Is Insufficient

In the 2018 Recommendation, the Acting Register distinguished between "lawful modification of a vehicle function" and unqualified modification (*i.e.*, "any modification") to conclude that the latter is likely an infringing use:

> In some cases, where a user seeks to modify only a functional element of a device for a personal, noncommercial use, that activity may well qualify as a fair use. In other cases, however, a modification under the proposed exemption may result in an infringing derivative work. Indeed, the statutory definition of "derivative work" requires an underlying work to "be recast, transformed, or adapted," and at the hearings proponents appeared to acknowledge that at least some of the modifications they describe in their comments could implicate that right.[15]

As for the idea that fair use makes infringement of the derivative work right tolerable, the Register summarily dismissed that argument. Modification proponents, in support of reverse engineering as a means to achieve interoperability, argued that *Sega v. Accolade*[16] and *Sony v. Connectix*[17] supported their position that "enabling interoperability and increasing the utility of hardware are fair uses."[18] The Register reasoned the "two cases [do not] go so far as to support the broader range of activities envisioned"[19] and would "not conclude that modification of a function of a device as a general category is likely to be noninfringing."[20] Thus, in light of the dearth of information about modification, and more importantly, the lack of details about how DVD and Blu-ray players (including their software components) or similar devices may be

---

[15] 2018 Recommendation at 211.

[16] *Sega Enters. Ltd. v. Accolade, Inc,* 977 F.2d 1510, 1522–23 (9th Cir. 2000) as amended (Jan. 6, 1993)).

[17] *Computer Entm't, Inc. v. Connectix Corp.*, 203 F.3d 596, 607–08 (9th Cir. 2000).

[18] 2018 Recommendation at 210.

[19] 2018 Recommendation at 211.

[20] *Id.*

modified, the precedent of this rulemaking clearly provides that such activities are not even eligible to be considered as fair use.

B. Modification of Players Is Not Fair Use

The precedent concerning the repair of video game consoles further illustrates that fair use does not authorize repair or modification of DVD and Blu-ray players and similar devices that would play back, display, or perform motion pictures. That precedent establishes both that: (i) modification is outside the permitted uses of the current repair exemption, and (ii) circumvention for authorized repair activities is still not permitted for video game consoles. Since DVD and Blu-ray players are to motion pictures as video game consoles are to video games – both players and video game consoles are intended to make use of expressive works — the video game console precedent is instructive to the analysis of permitting circumvention for the purpose of repairing or modifying DVD and Blu-ray players or other devices that play back, display, or perform motion pictures.

In the 2018 Recommendation, when the Acting Register considered the current repair exemption, the Register concluded that the current exemption permitting the repair of software-enabled devices could not extend to video game consoles.

> In multiple past rulemakings, the Office has rejected proposed jailbreaking exemptions for video game consoles — including passing suggestions of the need to repair these consoles — because of the potential harm to the market. For example, in 2012, the Register stated that:
>
> [O]pponents have provided compelling, uncontradicted evidence that circumvention of access controls to permit interoperability of video game consoles — regardless of purpose — has the effect of diminishing the value of, and impairing the market for, the affected code, because the compromised code can no longer serve as a secure platform for the development and distribution of legitimate content.
>
> This rulemaking reflects similar console-specific concerns about potential market harm. Proponents have not provided a persuasive legal or factual analysis why the

> Acting Register should reach a different conclusion than in 2012 or 2015, and so she does not.[21]

In Class 12 of this proceeding, proponents once again filed petitions that would permit circumvention for the purpose of repair of video game consoles. While acknowledging receipt of the petitions, the NPRM asked petitioners to explain what has changed since the last decision, noting that:

> in prior rulemakings [the Copyright Office] has declined to recommend exemptions for jailbreaking and repair of video game consoles in light of evidence that circumvention of TPMs in such devices may adversely affect the value of the affected software, as well as a lack of evidence of adverse effects on noninfringing uses. The Office invites comment on whether, in the past three years, there has been any change in the legal or factual circumstances bearing upon these issues.[22]

In their initial comments following the NPRM, proponents did not accept the invitation to explain what changes occurred in the last three years – either factually or legally – that would alter the conclusion that circumvention adversely affects the value of the affected software. As for new evidence regarding the adverse effect the prohibition has on noninfringing uses, the proponents state that Microsoft has stopped providing repair on pre-2016 video game consoles, thus game console owners must now, they claim, engage in more acts of circumvention if they want to repair their video game consoles.[23] There are multiple online repair shops that offer mail-in repair for both the Xbox 360 (initially released in 2006) and the Xbox One (initially released in 2013). The fact that Microsoft no longer directly performs repairs on consoles initially released 15 and 8 years

[21] 2018 Recommendation at 206.

[22] NPRM, *supra* note 7 at 65307.

[23] Public Knowledge and iFixit Initial Comments at 4.

ago is *de minimis*, particularly when there are repair shops that still provide repair services.[24] In light of these shortcoming, proponents have not advanced a case for the Register to reconsider the precedent.

C. Jailbreaking Precedent Is Distinguishable

Proponents overstate past precedent to conclude that the proposed activity here is noninfringing as well. In the 2018 Recommendation, when approving the jailbreaking exemption for voice assistant devices, the Acting Register explained that the difference between the jailbreaking precedent and the video game console is that the firmware at issue in the jailbreaking exemption did not purport to control access to the copyrighted work (*i.e.*, access to the copyrighted works were controlled by different TPMs). Reviewing the record for voice assistant devices, she reasoned:

> opponents did not dispute that subscription streaming services typically control access to their content with TPMs separate from those protecting the firmware. Mr. Bell stated that such services "would typically use multiple measures to prevent unauthorized access," including requiring "a customer log-in and password to verify that a subscription has been obtained" and "encrypt[ing] streams as they are delivered to the consumer." The current record does not support a finding that jailbreaking undermines the effectiveness of those separate TPMs.[25]

In fact, as the Register explained in the footnote to that conclusion, she was relying on the same reasoning that permitted jailbreaking of Smart TVs and explained how that jailbreaking was consistent with the precedent of denying an exemption for the repair of video game consoles:

---

[24] *See, e.g.,* VideoGame911 ("Video Game 911 specializes in Xbox 360 Repair", "Video Game 911 specializes in Xbox One Repair.") available at https://videogame911.com/xbox-360-repair/#1483403056908-5a4afd25-87d5; GamersRepair available at https://www.gamersrepair.com/game-console-repair/xbox-one-repair/. Both business provide service through mail. VideoGame911 provides "FREE return shipping on all completed orders.," GamersRepair provides "FREE SHIPPING ON ALL ORERS."

[25] 2018 Recommendation at 184.

> proponents of jailbreaking exemption for smart TVs 'explained that access to copyrighted programming . . . from services like Hulu and Netflix 'is controlled by separate TPMs' from those used to protect the smart TV firmware, and Joint Creators do not rebut this claim") (citation omitted). In this regard, the record evidence distinguishes the access controls protecting the firmware in voice assistant devices from the access controls in video game consoles. The Register has repeatedly concluded that "'**access controls on gaming consoles protect not only the console firmware, but the video games and applications that run on the console as well**,' many of which are owned by the console manufacturers."[26]

Playback device firmware is part of the overall content protection system for DVD and Blu-ray players, since that firmware and other design decisions safeguard the CSS and AACS encryption technologies as well as the "in the clear" copyrighted content after the player lawfully decrypts the content from the disc and passes it through the player to a display screen. Consequently, the jailbreaking precedent is inapplicable in the case of DVD and Blu-ray players. Just as is the case with video game consoles, the DVD and Blu-ray player manufacturer firmware, as well as other design elements, serve the overall purpose of providing a secure playback platform and protecting expressive copyrighted works. The applicable manufacturers' firmware and design elements are fundamental to the overall protection of motion picture entrusted to the device just as much as the "access controls on gaming consoles protect not only the console firmware, but the video games and applications that run on the console as well[.]" Consequently, as the jailbreaking precedent is simply inapplicable to the way content is protected on DVD and Blu-ray players, the Register should give effect to the video game console precedent, as the same fair use analysis is readily applicable to DVD and Blu-ray players.

D. The Concerns for the Value (or Market for the Work) Are Identical or Similar to the Concerns Identified in the Case of Video Game Consoles

In considering jailbreaking a video game console under fair use, the Register found that the fourth factor, the market or value for the code that protected the game console would be

[26] 2018 Recommendation at 184 n.1121 (citing 2015 Recommendation at 215) (emphasis added).

diminished, and with that factor "weigh[ing] somewhat strongly against a finding of fair use"[27] there could not be any persuasive basis to establish that jailbreaking a game console was noninfringing. The Register reasoned that, once jailbroken, "the compromised code can no longer serve as a secure platform for the development and distribution of legitimate content."[28] The Register also concluded that the evidence supported the finding that circumvention was inextricably linked to piracy.[29]

That same reasoning applies in the case of DVD players and Blu-ray players. Copies of motion pictures on optical discs that employ CSS and AACS content protection technologies are also dependent on code that manufacturers put in place to protect DVD and Blu-ray players from attacks that would expose the cryptographic keys necessary for the player to successfully play back copies of motion pictures distributed on CSS or AACS–protected discs. This code is not part of the CSS or AACS technologies themselves, and varies among CSS or AACS-licensed manufacturers as they each implement the AACS and CSS technical specifications, robustness rules, and compliance rules in their own way. Nevertheless, even though implemented in multiple ways, the code is fundamental to protecting the integrity of the player ecosystem, which the Register recognized in the context of video game consoles as a "secure platform for the development and distribution of legitimate content." Just as a "secure platform" is necessary for the development and distribution of legitimate content in the video game context, so it is in the motion picture context.

[27] 2012 Recommendation at 44.

[28] 2012 Recommendation at 44.

[29] 2012 Recommendation at 43.

1. Piracy Is Still a Consequence of a Compromised Digital Ecosystem

Piracy takes advantage of weaknesses in the digital ecosystem. The first widely publicized hack of CSS, DeCSS, demonstrates this to be true, as DeCSS resulted from a single manufacturer's failure to protect against the discovery and theft of a single cryptographic player key. Once a key is discovered and exposed, the chain of events inevitably leads to piracy. In promoting its own proprietary copy protection services, Smart Protection explains that:

> the first step in digital piracy is securing an illegal copy of a movie or TV show, [and one of four] "methods pirates use to obtain an illegal copy" is
>
> . . .
>
> DVD or Blu-ray Originals. To make this type of copy, pirates circumvent the digital rights security measures (DRMs) implemented on both DVDs and Blu-ray discs, which allows them to copy their content using digital recording software and/or hardware.[30]

2. Hacked TPMs for DVD and Blu-Ray Discs Remain a Source for Piracy

Using software enabled by stolen decryption keys to "read" DVD and Blu-ray discs and then obtain the digital content in the clear (often referred to as "ripping") is still a significant source for piracy. Quite recently, the Department of Justice announced the indictment of members of the "Sparks Group", who misrepresented themselves over a ten-year period to obtain advance distribution copes of motion pictures distributed on DVD and Blu-ray discs intended for retail

[30] *How does online piracy of moves and TV series Actually work?,* Smart Protection Blog available at https://smartprotection.com/en/media/how-does-film-series-online-piracy-work/ (last visited Jan. 29, 2021). Piracy resulting from hacked DVDs or Blu-ray discs is widely recognized in all forms. *See, e.g., Blu-ray Working Great, For Pirates*, TechDirt (Nov. 18, 2008) (describing how pirates "rip Blu-ray movies, then burn them onto DVDs" "create[s] fat profit margins on the $7 bootleg [DVDs]") available at https://www.techdirt.com/articles/20081117/1721382856.shtml. (last visited Jan. 29. 2021).

sale.[31] According to the release, the accused pirates then ripped the discs and disseminated the film and TV content via the Internet prior to the retail release date." The release described the activity as follows:

> Sparks Group members then used computers with specialized software to compromise the copyright protections on the discs, a process referred to as "cracking" or "ripping," and to reproduce and encode the content in a format that could be easily copied and disseminated over the Internet. They thereafter uploaded copies of the copyrighted content onto servers controlled by the Sparks Group, where other members further reproduced and disseminated the content on streaming websites, peer-to-peer networks, torrent networks, and other servers accessible to the public. The Sparks Group identified its reproductions by encoding the filenames of reproduced copyrighted content with distinctive tags, and also uploaded photographs of the discs in their original packaging to demonstrate that the reproduced content originated from authentic DVDs and Blu-Ray discs.[32]

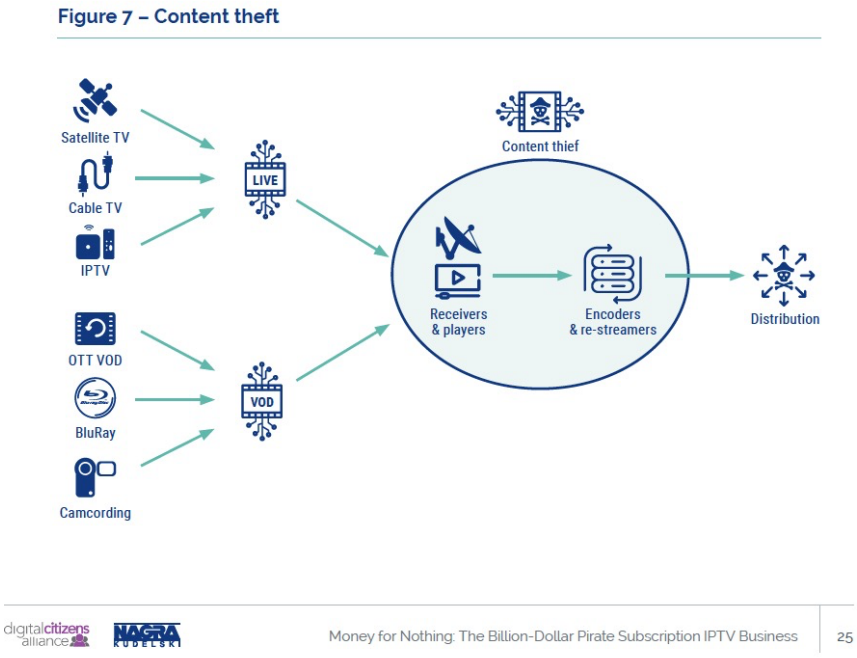
Just as the indictments against the Sparks Group show that they relied on ripped consumer market discs, online streaming piracy is generally well understood to be fueled by content ripped from discs using software implementing circumvention tools. For example, the Digital Citizens Alliance August 2020 Report, *Money for Nothing: The Billion-Dollar Pirate Subscription IPTV Business,* points to ripped Blu-ray Discs as a source for this piracy.[33]

---

[31] Acting U.S. Attorney Announces Federal Charges and International Operation to Dismantle Online Piracy Group, Press Release, Department of Justice (Aug. 26, 2020) available at https://www.justice.gov/usao-sdny/pr/acting-us-attorney-announces-federal-charges-and-international-operation-dismantle-0 (last visited Jan. 29, 2021).

[32] *Id.*

[33] Digital Citizens Alliance and NAGRA, Money for Nothing: The Billion-Dollar Pirate Subscription IPTV Business.



3. Piracy and Its Harms

This piracy leads to extraordinary harm. In the above case of indictments against the Sparks Group, the DOJ stated that "Sparks Group has caused tens of millions of dollars in losses to film production studios." The Digital Citizens Alliance Report, largely intended to illustrate the billion-dollar industry that online streaming piracy has become, cites to other reports that have quantified the loss to the "U.S. economy [to be] at least $29.2 billion in lost revenue each year."[34]

These recent accounts are consistent with what has been known about the effects of piracy for some time. A study prepared for the U.S. Patent Trademark Office, providing a systematic review of the literature, pointed out that "if the shutdown of one popular piracy site — Megaupload.com — caused a 6.5-8.5 percent increase in digital movie revenues in spite of all of

[34] Digital Citizen Alliance Report at 1 n.4 (citing DIGITAL VIDEO PIRACY: Impacts of Digital Piracy on the U.S. Economy (GIPC, June 2019)).

the video piracy that remained after Megaupload, total losses to rightsholders from piracy in the home market could be quite substantial."[35]

Since the piracy of film and television content flows in part from the circumvention of CSS and AACS-protected discs, rightsholders can ill afford permitting any circumvention that may interfere with or disrupt the integrity of a carefully considered and implemented content protection ecosystem. Technologies like CSS and AACS are more than transactional licenses to decrypt the content on discs. Instead, they are composed of multilayer commitments requiring careful manufacturer design elements and deliberate device functionality, as the robustness and compliance rules may prescribe. As in the chain of events leading to DeCSS, even unintentional acts can jeopardize the integrity of a content protection ecosystem. Likewise, even well-intentioned exemptions can unintentionally impose undue stress on the system by encouraging activities that leave a key to be discovered or compromised that then effectively strips the copyrighted content of its TPM technical and license obligation protections. This then ultimately reduces the effectiveness of the system to a fraction of what both the rights holders expect and the licensed player manufacturers intend. Consequently, the exemptions are not warranted, and a review of the statutory factors make that conclusion even more evident.

IV. *Statutory Factors Weigh Against the Creation of the Class*

The analysis of the proposed exemption to jailbreak video game consoles is instructive to the application of the statutory factors to an exemption that would permit the jailbreaking of DVD and Blu-ray players. As proponents do not argue that the second and third factors are particularly relevant to the proposed exemption, the discussion of the statutory factors is limited to the first and

[35] Brett Danaher, Michael D. Smith, and Rahul Telang, Piracy Landscape Study: Analysis of Existing and Emerging Research Relevant to Intellectual Property Rights (IPR) Enforcement of Commercial-Scale Piracy at 27 (March 20, 2020) (Prepared for the U.S. Patent and Trademark Office).

fourth factors, which are of fundamental importance to the potential effects the proposed exemption may have on the market for motion pictures and the secure successful distribution platform that DVD and Blu-ray players have proven to be.

A. Availability for Use of Copyrighted Works

An exemption permitting the circumvention of players would not make more works available or increase the use of copyrighted works. In the 2012 Recommendation, the Register considered the proposed exemption to jailbreak video game consoles in the context of the first statutory factor and concluded that a jailbreaking exemption for video game consoles would not result in the availability and use of more copyrighted works:

> [C]onsole access controls encourage the development and dissemination of highly creative copyrighted works by facilitating secure platforms for the development and distribution of video games and other applications. In addition to artwork, graphics and sound effects, a sophisticated video game may include storyline, character development, voiceovers, music and other expressive elements. Such a work is far more challenging and expensive to create than the typical smartphone application, for example, like a motion picture, it involves a team of creators and may require funding in the millions of dollars. It is difficult to imagine that one would choose to make such an investment without some hope that it could be recouped by offering the resulting product through channels that provide some measure of protection against unauthorized copying and distribution.[36]

The Register's analysis looks past the copyright in the code, and more fully considers the copyrights that the code is ultimately intended to protect – the video games. She notes that video games are more akin to movies, which require a "team of creators" and "funding in the millions of dollars[.]"[37]

More importantly, the Register's reasoning reveals that motion pictures are, in fact, the quintessential works warranting the full weight of the prohibition against circumvention. The application of this rationale to motion pictures distributed on CSS- and AACS-protected discs has

---

[36] 2012 Recommendation at 51.

[37] *Id.*

been fundamental to the rulemaking since its inception, as no other types of copyrighted works have been as regularly and intensely subject to evaluation than those copies of motion pictures distributed on CSS and AACS-protected discs. Consequently, the reasoning that weighed the first factor against the creation of an exemption to circumvent video game consoles should weigh as much, if not more, against creating an exemption to circumvent players that playback CSS or AACS-protected discs.

B. Fourth Statuary Factor Does Not Favor the Creation of the Exemption

The Register in the 2012 Recommendation explained why this factor did not favor the creation of a repair exemption for video game consoles:

> As discussed above . . . , due to the particular characteristics of the video game marketplace, the circumvention of access controls protecting a console computer program so that it can be copied and modified for the purpose of enabling unauthorized applications has the effect of decreasing the market for, and value of, that program, as it can no longer serve to facilitate a secure gaming platform. Further, by enabling the ability to obtain and play pirated games and other unauthorized content, the dismantling of console access controls undermines the value of legitimate copyrighted works in the marketplace, many of which require a substantial investment of creative and financial resources to create.[38]

The Register again was concerned about the integrity of the overall content protection ecosystem, as she noted that the code "can no longer serve a secure gaming platform." Similarly, as explained earlier, any repair exemption that permits the circumvention of independent code protecting the player threatens to disrupt the digital ecosystem as this code serves as an implementation of the robustness and/or compliance rules. And, as explained earlier, even unintentional acts can lead to circumstances that enable widespread piracy. Consequently, this factor, too, weighs against the creation of an exemption to permit circumvention of TPMs for the purpose of repair or modification of a DVD or Blu ray player (or other devices that display/perform motion pictures).

[38] 2012 Recommendation at 52.

Finally, if the proposed class purports to include DVD and Blu-ray players, then the statuary factors weigh against the creation of an exemption permitting the jailbreaking of this proposed class. Indeed, jailbreaking is nothing more than repair or modification of the device. As the jailbreaking video game precedent for the purpose of repair demonstrated that the statutory factors do not favor the creation of the exemption, so too, for identical reasons, the Register should find that the video game console precedent applies equally to video streaming devices.

V. *Conclusion*

For the reasons stated above, if the class for video streaming devices purports to include DVD or Blu-ray players, then an exemption permitting jailbreaking for the underlying purpose of repair or modification of video streaming devices is not warranted.

///