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 16 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 16: Computer Programs—Copyright License Investigation

ITEM C. OVERVIEW

DVD CCA and AACS LA object to the proposed class as the purpose of investigating possible FOSS licensing terms does not warrant the risk posed to the overall content protection system employed to protect copies of motion pictures distributed on DVD and Blu-ray discs.

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 1

A. Robustness and Compliance Rules Are Integral to A Secure Digital Ecosystem 2

II. The Proposed Class Does Not Constitute A Proper Class 4

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 4

1. Similar Proposed Classes Have Been Rejected 5

2. No Evidence for A Class to Include DVD and Blu-ray Products is Proffered 9

III. The Circumvention Prohibition Is Not Causing Proponents' Harm 9

A. Proponents Have Not Shown the Circumvention Prohibition Has Interfered with Their Ability to Obtain Judicial Relief 9

B. Legal System Provides Alternative to Circumvention 10

IV. Statutory Factors Weigh Against the Creation of the Class 11

A. Availability for Use of Copyrighted Works 12

B. The Effect of Circumvention of Technological Measures on The Market for or The Value of Copyrighted Works 13

1. The Concerns for the Value (or Market for the Work) for Players Approximate Concerns Identified in the Fair Use Analysis for Video Game Consoles 13

a) Piracy Is Still a Consequence of a Compromised Digital Ecosystem 14

b) Hacked DVD and Blu-Ray Discs Remain a Source for Piracy 15

c) Piracy and Its Harms 17

C. Fourth Statuary Factor Does Not Favor the Creation of the Exemption 18

V. Conclusion 19

I. *Introduction*

DVD CCA and AACS LA object to an exemption that would permit circumvention of technical protection measures ("TPMs") for the purpose of investigating products that may violate the terms of "free and open source software" (FOSS) licenses.[1] Bizarrely, the proposal would provide a new enforcement mechanism to the opensource movement that far exceeds the tools currently available to rightsholders in the traditional copyright industries. Rightsholder, who have made a far greater financial investment in the exploitation of their works than providers of opensource software have, simply do not have this tool in their enforcement arsenal. Indeed, the proponents' request presents a curious paradox that, if the exemption is granted, free and open-source interest would have a greater ability to enforce their copyrights than those rightsholders in the copyright industries currently have. Nevertheless, as explained below, proponents should not be afforded such an invasive tool, particularly when, were that tool applied clumsily, or even precisely, the result could be an unwarranted disruption of DVD and Blu-ray players manufacturers' efforts to comply with the robustness and compliance rules which they are obligated to implement in their devices.

---

[1] Proponents also advance a second circumstance that allegedly may warrant circumvention for copying, redistributing, and updating free and open-source software. It is not clear what real world activity proponents seek to address. If proponents are seeking to "copy, redistribute and update" the native open-source software (i.e., not the software as it may be implemented by a licensee), then DVD CCA and AACS LA do not understand what TPM, if any, may be at issue. If, however, proponents are seeking to "copy, redistribute and update" a licensee's implementation of the software, then DVD CCA and AACS LA do not understand how proponents propose that could be achieved in practical terms. While the license may permit such activities, the possible enforcement of those terms would make FOSS adoption and implementation very unattractive as licensees would effectively surrender all control over their product to the FOSS licensor. DVD CCA and AACS LA are not aware of any updating activity occurring without the cooperation of the licensee. Thus, in the absence of more information, DVD CCA and AACS LA object to the second circumstance as being too hypothetical or speculative.

DVD CCA and AACS LA object to the proposal to permit circumvention for purpose of investigating possible violations of FOSS terms. The proposed class is impermissibly broad as proposals to circumvent software-enabled devices for repair/modification have been or currently are in Class 12. But even if the class were limited, then an exemption still is not warranted because there are indeed alternatives to circumvention. Finally, analyzing the application of the proposed exemption on DVD or Blu-ray playback devices shows that the statutory factors do not support the creation of the exemption. Consequently, the proposed class should be denied, but if the Register finds the exemption is nonetheless warranted for other reasons, then the Register should refine the exemption to exclude these products and other products intended for the lawful access to copyrighted expressive works.

A. Robustness and Compliance Rules Are Integral to A Secure Digital Ecosystem

DVD and Blu-ray players 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". Just like circumvention of TPMs for the purpose of repair or modification of these devices could harm the security of the DVD and Blu-ray players, so too can circumvention for the purpose of investigation undo those manufacturer design elements, developed in compliance with the robustness rules, leaving the technological protection measure 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 other offerings rights holders intend to exploit. 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 might 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 is 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.

While circumvention for the purpose of investigation may not readily appear to jeopardize the products as circumvention for repair or modification would, any circumvention of DVD or Blu-ray players poses the identical risk such as exposing player keys or compromising some other element intended to comply with the applicable robustness or compliance rules. Circumvention for investigative purposes results in no less risk because it similarly upsets the careful licensing arrangement between rights holders and manufacturers, it introduces the possibility that keys will be discovered, or other elements compromised, and ultimately threatens the digital ecosystem. Therefore, DVD CCA and AACS LA object to the proposed class as being impermissibly broad.

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 where 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 . . . ."[2] The statute thus limits the rulemaking to exempt certain uses from the general prohibition against circumventing TPMs based on a determination resulting directly 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 an 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] [the prohibition against circumvention] for limited time periods, . . . for a particular category of copyrighted materials."[3]

---

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

[3] House Commerce Committee Report at 36.

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."[4] 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 . . . ." [5] This instruction alone would render the current request impossible to grant, as this rulemaking could never handle the quantum of evidence that would be necessary to support an unbound exemption for investigative purposes as contemplated by proponents.

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)."[6] Clearly, the broad and unbounded class proposed by the proponents here cannot be considered "narrow and focused" as Congress demands.

1. Similar Proposed Classes Have Been Rejected

The scope of the proposed class is identical to the proposed class for software-enabled devices, which, as originally proposed, has been found impermissibly broad. These concerns are fundamental to the rulemaking and were the bases of questions the Copyright Office raised in the NPRM. Ignoring the precedent of this rulemaking and failing to propose legal reasons to justify the broad class, the proponents, nevertheless, insist that their circumstances warrant an exemption.

[4] House Commerce Committee Report at 37.

[5] *Id*. at 37.

[6] *Id*. at 38.

> [S]oftware is everywhere, both programs used on traditional computers – server, desktop, laptop and mobile – and on an increasing kind and number of the devices that are part of our everyday lives. Conservancy is impaired in its ability to investigate all of these uses because of TPMs. The exemption is therefore sought for any device that is capable of running a software program, because these devices are all likely to be using FOSS.[7]

While that may all be true, these circumstances do not satisfy the requirements that a class be narrow, as Congress instructed. Thus, the question becomes whether a permissible class may 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.[8]

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."[9]

Information as to how the class may be refined here is essentially impossible to discern from proponents' assertions. Proponents state that they are "frequently investigating special-purpose devices driven by software" which may result from the growth of "mobile computing,

---

[7] Software Freedom Conservancy, Initial Comments at 6.

[8] 2018 Recommendation at 191-92.

[9] 2018 Recommendation at 191-92.

'smart' electronics and the 'Internet of Things[.]'"[10] They provide a laundry-list of devices that may contain FOSS and violate FOSS licensing terms, including but not limited; to servers, laptops, android phones, speakers and other audiovisual equipment, cars, aerial drones, thermostats, doorbells, and even watches. Apparently, they also investigate software more generally (*i.e.*, "software applications intended for use on general purpose computer, server, mobile device, or virtual machine").

Defining the class as being FOSS-dependent devices, however, is insufficient, because apparently, not even proponents know which devices include FOSS. Proponents explain, "[t]he other part of the exemption, investigating infringement, will often require the reverse engineering of software code to ascertain whether it is using FOSS code but not meeting all the conditions of the licenses, thusly an infringing use."[11] Proponents thus seek an exemption to be able to confirm their suspicion that a particular body of code is subject to a FOSS license; so they could then seek to enforce the license while avoiding the potential expense of discovery that would normally be a part of a litigated dispute.[12]

The lack of commonality as a class is further exacerbated by the dearth of information about the TPMs at issue, including whether all the devices employ TPMs, and the lack of an explanation as to how circumvention facilitates the noninfringing use. The proponents suggest that the simplest TPM is password protection, while the most difficult is end-to-end encryption. But in no way do proponents draw a nexus between any TPM and any particular device.

[10] Software Freedom Conservancy Initial Comments at 4.

[11] Moreover, the term FOSS in itself may be illusory, as the open source movement does not recognize a single authority or prescribe a single paradigm for implementation. The rules of the licenses often vary as to what constitutes either free software or open source licenses.

[12] Such a result would be inconsistent with our current legal system in which the potential expense of litigation helps to guard against excess and encourages parties to compromise.

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 the prohibition is adversely affecting a noninfringing use. 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 that 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 on the referenced device, and how circumvention of that specific TPM would occur. Absent that information, there is no basis to conclude that the circumvention prohibition is adversely affecting any noninfringing use. As for the proposed class, if there is no basis to conclude that a TPM is adversely affecting any particular FOSS-dependent devices, then there is certainly no basis to conclude more generally that TPMs, of any kind, are adversely affecting the panoply of devices that the proponents seek to include in the proposed class.

---

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

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

2. No Evidence for A Class to Include DVD and Blu-ray Products is Proffered

Proponents have not introduced any information sufficient to include DVD or Blu-ray playback devices (or any other device that would play back or otherwise display/perform motion pictures) in a class.

III. *The Circumvention Prohibition Is Not Causing Proponents' Harm*

A. Proponents Have Not Shown the Circumvention Prohibition Has Interfered with Their Ability to Obtain Judicial Relief

Proponents erroneously assert that Section 1201 is adversely affecting them. In short, proponents argue they are harmed by the possibility that any defendant, having been sued for violating the FOSS license terms applicable to a device they have circumvented, could raise a counterclaim under the DMCA.

> However, Conservancy is fully aware that if it circumvented TPMs to investigate the infringement claim, without an exemption it will be at risk of a counterclaim under Section 1201. Any counterclaim will turn what may be a simple, clear-cut infringement case into a legally complicated, fact-intensive suit at significantly higher cost, one that a charitable non-profit or hobbyist FOSS developer can ill afford.[15]

At the outset, no rule or legal principle in the U.S. legal system suggests an aggrieved party – even with a "simple, clear-cut infringement case" is entitled to a conveniently quick, cost-effective resolution of the grievance, especially when their claim is not unchallenged.[16] Thus, the alleged harm is general in nature and has little to do with the prohibition against circumvention.

---

[15] Initial Comments at 10.

[16] See, e.g., *FD Rich Co. v. United States ex rel. Industrial Lumber Co.*, 417 US 116, 128-29 (1974) (explaining that the American Rule, the default position that litigants pay their own attorney fees, may result in a prevailing party being made less than whole, but other countervailing considerations are at play as well).

A closer examination of the specific argument also suggests that the proponents have not accurately weighed the risk of harm, because a favorable resolution on their hypothetical infringement claim makes it less likely that a Section 1201 counterclaim is available to the defendant infringer. While the circumvention prohibition against access controls protects all works under Title 17, a violation is dependent on whether circumvention is done without the authority of the copyright owner. Thus, if the defendant has been found to infringe proponents' work then the defendant may have no copyright in the remainder of the work to protect under a Section 1201 counterclaim.[17] But, even if defendants do have some other elements of the work protected by copyright, proponents have not offered any jurisprudence that suggests equitable defenses such as "clean hands" are not available to proponents. Thus, the alleged harm is speculative[18].

B. Legal System Provides Alternative to Circumvention

Proponents do not need to circumvent in order to pursue their claim of copyright infringement. The legal system provides an arsenal of tools to pursue a copyright infringement claim. Proponents are not in the dark as to whether infringement has occurred. The Conservancy describes "receiv[ing] credible reports that the device contains FOSS but the license requirements have not been met", and the Free Software Foundation states that it receives "186 reports each year

[17] Cf *Lexmark Intern*, 387 F.3d at 550. The Lexmark Court had found that "the Toner Loading Program is not copyrightable." Lexmark, 387 F.3d at 544. The court explained, "[t]o the extent the Toner Loading Program is not a 'work protected under the copyright statute,' which the district court will consider on remand, the DMCA necessarily would not protect it." *Id.* at 550.

[18] While fair use advocates regularly invoke the chilling effect of 1201 as an alleged harm none of them have presented a record of actual harm. Most recently in the 2018 Recommendation, in reviewing claims of the chilling effect on computer research, the Acting Register said "[she] is not convinced that this provision risks chilling good-faith research. There is no indication in the record that any disputes of the type described by proponents have arisen, and speculation alone is insufficient to demonstrate a likely adverse effect." 2018 Recommendation at 303.

of copyright violations on free software programs."[19] Proponents do not equivocate on whether infringement is occurring. Any copyright owner including these "copyleft" interests understand the value of a cease-and-desist letter (CAD). CADs usually bring the parties into negotiations. If defendants ignore the CAD, they do so at their own peril, as the law provides increased damages for willful infringement. The availability of these statutory damages encourages negotiation, as calculating the damages as part of litigation can prove challenging. Finally, the same statutory damages also encourage contingency relationships, where an experienced attorney will take on a simple, clear-cut infringement case as proponents suggest they have.[20] In fact proponents clearly must understand these tools, because they assert that they have been pursuing these cases for years. Moreover, they have not proffered examples where the law was unable to resolve the alleged infringement or where the DMCA counterclaim was actually an issue. Consequently, as there are alternatives to circumvention such as continuing to avail themselves of the current well-known legal tools, there is no basis to create an exemption for proposed class.

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

The analysis of the statutory factors is inapposite to the reasoning the Register provided for the preservation of computer programs or even video games.

---

[19] Free Software Foundation, Initial Comments at 2.

[20] *See, e.g.,* Joe Rothman, *6 Factors We Consider for Copyright Infringement Contingency Litigation*, SRipLaw available at https://www.sriplaw.com/6-factors-considered-copyright-infringement-contingency-litigation/ (last visited Feb. 1, 2021). Rothman explains:

> When an experienced copyright infringement lawyer agrees to take your case on a contingent fee basis, it means that the lawyer believes in the strength of your case. Unlike hourly-billing cases, contingency cases must have a strong chance of winning and recovering for a contingent fee to make sense.

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.[21]

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[.]"[22]

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 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

[21] 2012 Recommendation at 51.

[22] *Id.*

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 those players that playback CSS or AACS-protected discs.

B. The Effect of Circumvention of Technological Measures on The Market for or The Value of Copyrighted Works

This fourth statutory factor does not favor an exemption for DVD and Blu-ray players. Frequently, this factor is intertwined with the fourth factor of the fair use analysis (the effect of the market for the copyrighted work) as it, too, seeks to ascertain the effect of circumvention of access controls on the market for or value of copyrighted works. Thus, DVD CCA and AACS LA provides a discussion of the fourth factor of fair use analysis before addressing the statutory factor.

1. The Concerns for the Value (or Market for the Work) for Players Approximate Concerns Identified in the Fair Use Analysis for Video Game Consoles

The Register should rely on the analogy that a DVD or Blu-ray player is to motion pictures what video game consoles are to video games and consider her prior analysis of jailbreaking video games as instructive to a review of the fourth factor of the fair use analysis in the context of players. In considering jailbreaking a video game console under fair use, the Register found that under the fourth factor, the market or value for the code that protected the video game console would be diminished, and with that factor "weigh[ing] somewhat strongly against a finding of fair use"[23] there could not be any persuasive basis to establish that jailbreaking a video 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."[24] The

[23] 2012 Recommendation at 44.

[24] 2012 Recommendation at 44.

Register also concluded that the evidence supported the finding that circumvention was inextricably linked to piracy.[25]

Copies of motion pictures that employ CSS and AACS content protection technologies are dependent on code similar to that which 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, 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."

a) 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, the chain of events unquestionably leads to piracy. In promoting its own proprietary copy protection services, Smart Protection explains that

[25] 2012 Recommendation at 43.

> 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.[26]

b) Hacked DVD and Blu-Ray Discs Remain Source for Piracy

Using software enabled by stolen decryption keys to read DVD and Blu-ray discs and then obtaining 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 meant for retail.[27] 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

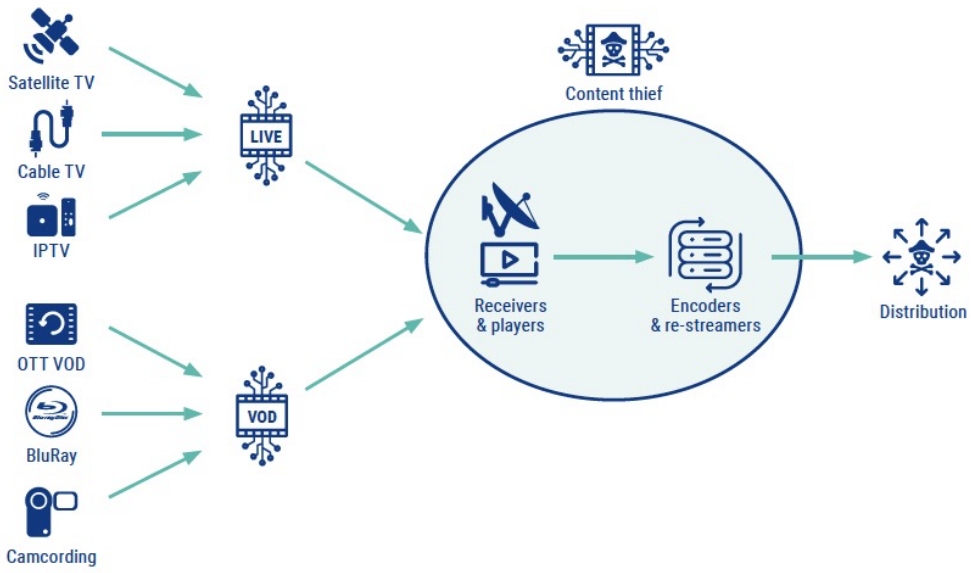
[26] *How does online piracy of moves and TV series Actually work?,* Smart Protection Blog available at https://smartprotection.com/en/media/how-does-film-series-online-piracy-work/ (last visited Jan. 29, 2021). Piracy resulting from hacked DVDs or Blu-ray discs is widely recognized in all forms. *See, 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).

[27] 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).

> 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.[28]

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.[29]

Figure 7 – Content theft



[28] *Id.*

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

c) Piracy and Its Harms

This piracy undoubtedly leads to significant 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 Alliances Report, largely intended to show 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."[30]

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 the video piracy that remained after Megaupload, total losses to rightsholders from piracy in the home market could be quite substantial."[31]

Since the resulting piracy of film and television content flows in part from the circumvention of CSS and AACS-protected discs, rights holders can ill afford permitting any circumvention that may interfere with or disrupt the integrity of the carefully considered content protection ecosystem. Technologies like CSS and AACS are more than transactional licensee 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

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

[31] 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).

acts can jeopardize the integrity of content protection ecosystem. 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 players manufacturers intend. Consequently, the exemptions are not warranted, and a review of the statutory factors make that conclusion even more evident.

C. 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.[32]

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 serve as an implementation of the robustness and/or compliance rules. The statutory factor weights against the creation of an exemption for the purpose of FOSS investigation because – even unintentionally – certain acts can disrupt the manufacturers' implementation of the robustness and compliance rules – and thereby

[32] 2012 Recommendation at 52.

compromise the integrity of the overall content protection scheme – leaving bad actors to take advantage of these newly created vulnerabilities. Proponents' alleged speculative harm certainly does not outweigh the proven harm piracy has caused rightsholders.

V. *Conclusion*

For the reasons stated above, an exemption to circumvent TPMs in order to investigate FOSS-dependent devices would be just as harmful as an exemption that permitted circumvention for repair or modification. Thus, the exemption simply is not warranted.

///