



This document is scheduled to be published in the Federal Register on 12/12/2014 and available online at <http://federalregister.gov/a/2014-29237>, and on [FDsys.gov](http://FDsys.gov)

## **LIBRARY OF CONGRESS**

### **U.S. Copyright Office**

#### **37 CFR Part 201**

**[Docket No. 2014-07]**

### **Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies**

**AGENCY:** U.S. Copyright Office, Library of Congress.

**ACTION:** Notice of proposed rulemaking.

---

**SUMMARY:** The United States Copyright Office is conducting the sixth triennial rulemaking proceeding under the Digital Millennium Copyright Act (“DMCA”) concerning possible exemptions to the DMCA’s prohibition against circumvention of technological measures that control access to copyrighted works. On September 17, 2014, the Office published a Notice of Inquiry requesting petitions for proposed exemptions, and it has received forty-four petitions in response. With this Notice of Proposed Rulemaking, the Office is initiating three rounds of public comment on exemptions proposed in the petitions. Interested parties are invited to make full legal and evidentiary submissions in support of or opposition to the proposed exemptions, in accordance with the requirements set forth below. The Office is providing a “long comment” form for this purpose. The Office is also offering members of the public the opportunity to express general support for or opposition to any of the proposals via a “short comment” form. Commenters should carefully review the legal and evidentiary standards for the granting of exemptions under the DMCA, which are set forth in the September Notice of Inquiry. Commenters should also review the guidance provided in this document regarding

specific areas of legal and factual interest with respect to each proposed exemption or category of exemptions, and the types of evidence that commenters may wish to submit for the record. This document also provides information concerning the recommended format and content for submissions, including documentary and multimedia evidence.

**DATES:** Initial written comments (including documentary evidence) and multimedia evidence from proponents and other members of the public who support the adoption of a proposed exemption, as well as parties that neither support nor oppose an exemption but seek to share pertinent information about a proposal, are due February 6, 2015. Written response comments (including documentary evidence) and multimedia evidence from those who oppose the adoption of a proposed exemption are due March 27, 2015. Written reply comments from supporters of particular proposals and parties that neither support nor oppose a proposal are due May 1, 2015.

**ADDRESSES:** The Copyright Office strongly prefers that written comments be submitted electronically using the comment submission page on the Copyright Office website at <http://www.copyright.gov/1201/>. Commenters are required to provide separate submissions for each proposed class during each stage of the public comment period.

Although a single comment may not encompass more than one proposed class, the same party may submit comments on multiple classes.

As noted, the Office is providing two comment forms on its website: a long form for those who wish to provide a full legal and evidentiary basis for their position in support of or opposition to a proposed exemption, and a short form for those who wish briefly to express general support for or opposition to a proposed exemption. The formats and content of these forms are described in the **SUPPLEMENTARY INFORMATION**

section below. Long form comments should be submitted together with any documentary evidence. To meet accessibility standards, written comments and all associated documentary evidence (but not multimedia evidence, as discussed below) must be uploaded in a single file in either Portable Document File (PDF) format that contains searchable, accessible text (not an image); Microsoft Word; WordPerfect; Rich Text Format (RTF); or ASCII text file format (not a scanned document). The maximum file size is 6 megabytes (MB). The name of the submitter (and organization) should appear on both the submission form and the face of the comment.

Commenters submitting long form comments may also separately submit multimedia evidence, as further explained in the Supplementary Information section below. Commenters submitting multimedia evidence should so indicate on the first page of their written submission. Multimedia evidence should not be uploaded via the website; instead, it should be delivered to the Office, together with a hard copy of the written comment, on a CD-ROM, DVD-ROM, or flash drive in one of the acceptable file formats listed on the Copyright Office website at <http://copyright.gov/eco/help-file-types.html>. The disc or flash drive should be labeled with the name of the submitter and the number of the proposed class to which the evidence pertains. The file name of each file contained on the disc or flash drive should consist of the submitter's name, followed by the proposed class number and exhibit number, in the following format: "Jane Smith Class 1 Ex. 1." Multimedia evidence may be submitted either by U.S. mail addressed to Copyright Office, Office of General Counsel, P.O. Box 70400, Washington, D.C. 20024, or by hand delivery to Room LM-403 of the Copyright Office in the James Madison Memorial Building of the Library of Congress, 101 Independence Ave. SE, Washington,

D.C. 20540. In either case, to ensure proper delivery, the package should be clearly labeled “Attention: Office of General Counsel – Section 1201 Proceeding.”

All written comments and documentary evidence will be posted publicly on the Copyright Office website in the form in which they are received. Depending upon technological constraints and other factors, the Office may also post some or all multimedia evidence on its website, with the remainder made available for inspection and copying at the Office upon written email request to the Office of General Counsel using the contact information provided below. If a commenter cannot meet a particular submission requirement, the commenter should contact the Copyright Office using the contact information provided below.

**FOR FURTHER INFORMATION CONTACT:** Jacqueline C. Charlesworth, General Counsel and Associate Register of Copyrights, by email at [jcharlesworth@loc.gov](mailto:jcharlesworth@loc.gov) or by telephone at 202-707-8350; Sarang V. Damle, Special Advisor to the General Counsel, by email at [sdam@loc.gov](mailto:sdam@loc.gov) or by telephone at 202-707-8350; or Stephen Ruwe, Attorney-Advisor, by email at [sruwe@loc.gov](mailto:sruwe@loc.gov) or by telephone at 202-707-8350.

**SUPPLEMENTARY INFORMATION:**

On September 17, 2014, the Copyright Office published a Notice of Inquiry (“September Notice”) in the Federal Register to initiate the sixth triennial rulemaking proceeding under 17 U.S.C. 1201(a)(1) to determine whether there are any classes of copyrighted works for which noninfringing uses are, or in the next three years are likely to be, adversely affected by the prohibition on circumvention of technological protection measures (“TPMs”) that control access to copyrighted works (sometimes also referred to

as “access controls”).<sup>1</sup> The September Notice invited interested parties to submit petitions for proposed exemptions that set forth the essential elements of the exemption.<sup>2</sup>

The Office received forty-four petitions in response to the September Notice, which are posted on the Copyright Office website.<sup>3</sup> With this Notice of Proposed Rulemaking, the Office is initiating three rounds of public written comment regarding the proposed exemptions.

## **I. Written Comments**

Persons wishing to address proposed exemptions in written comments should carefully review the September Notice to familiarize themselves with the substantive legal and evidentiary standards for the granting of an exemption under section 1201(a)(1).<sup>4</sup> In addressing factual matters, commenters should be aware that the Office favors specific, “real-world” examples supported by evidence over speculative, hypothetical observations. For example, a proponent seeking to demonstrate that a TPM is having or is likely to have adverse effects should provide detailed evidence of actual noninfringing uses that are precluded by the TPM, rather than conclusory declarations or isolated harms. Likewise, an opponent seeking to establish, for instance, that alternative means of accessing the work obviate the need for an exemption should provide specific and detailed evidence of such alternatives rather than unsupported assertions.

Commenters’ legal analysis should explain why the proposal meets or fails to meet the criteria for an exemption under section 1201(a)(1), including, without limitation,

---

<sup>1</sup> 79 FR 55687 (Sept. 17, 2014).

<sup>2</sup> *Id.* at 55692-93.

<sup>3</sup> See <http://copyright.gov/1201/2014/petitions/>. References to these petitions in this document are by party name followed by “Pet.” Where a single party has filed multiple petitions, the reference will include the party name and a short description of the relevant proposal (*e.g.*, “EFF Jailbreaking Pet.”).

<sup>4</sup> 79 FR at 55689-91.

why the uses sought are or are not noninfringing as a matter of law. The legal analysis should also identify and discuss statutory or other legal provisions that could impact the necessity for or scope of the proposed exemption (for example, the Unlocking Consumer Choice and Wireless Competition Act (“Unlocking Act”),<sup>5</sup> or 17 U.S.C. 117). Legal assertions should be supported by statutory citations, relevant case law, and other pertinent authority.

The Office is accepting comments in two ways. First, commenters who wish to provide a legal and evidentiary basis for their position may submit comments in a long form format as set forth below. To assist participants, the Office has posted a recommended form for such longer submissions on its website at <http://copyright.gov/1201/>.

Second, for those commenters who wish only to briefly express general support for or opposition to a proposed exemption, the Office has provided a short form for single-page comments, also available at <http://copyright.gov/1201/>, which may be completed and uploaded to the Office’s website.

The deadlines for each round of submissions are set forth in the **DATES** section above. Commenting parties should be aware that rather than reserve time for potential extensions of time to file comments, the Office has already established what it believes to be the most generous possible deadlines consistent with the goal of concluding the triennial proceeding in a timely fashion.

To ensure a clear and definite record for each of the proposals, as explained in the September Notice, both long form and short form commenters are required to provide *a*

---

<sup>5</sup> Pub. L. 113–144, sec. 2(b)-(c), 128 Stat. 1751, 1751-52 (2014).

*separate submission for each proposed class* during each stage of the public comment period. Although a single comment may not address more than one proposed class, the same party may submit multiple written comments on different proposals. For example, a commenter may not submit a single comment addressing both Class 7 and Class 8, but may submit two comments addressing each separately. The Office acknowledges that the requirement of separate submissions may require commenters to repeat certain information across multiple submissions, but the Office believes that the administrative benefits for both participants and the Office of creating a self-contained, separate record for each proposal will be worth the modest amount of added effort.<sup>6</sup>

The *first round* of public comment is limited to submissions from the *proponents* (*i.e.*, those parties who proposed exemptions during the petition phase) and *other members of the public who support* the adoption of a proposed exemption, as well as *any members of the public who neither support nor oppose* an exemption but seek only to share pertinent information about a specific proposal.<sup>7</sup> Proponents of exemptions – as well as supporters – should present their complete affirmative case for an exemption during the initial round of public comment, including all legal and evidentiary support for the proposal. Those who neither support nor oppose an exemption but seek to offer relevant evidence in response to a proposal should also file comments in the initial round.

*Members of the public who oppose* an exemption should present the full legal and evidentiary basis for their opposition in the *second* round of public comment.

---

<sup>6</sup> See 79 FR at 55692.

<sup>7</sup> These submissions may suggest refinements to the proposed exemptions, but may not propose entirely new exemptions.

The *third* round of public comment will be limited to *proponents and supporters* of particular proposals, and *those who neither support nor oppose a proposal*, in either case who seek to *reply* to points made in the earlier rounds of comments. Reply comments should not raise new issues, but should instead be limited to addressing arguments and evidence presented by others.

Parties seeking to make submissions who believe they cannot adhere to the guidelines set forth in this notice should contact the Office, using the contact information above, to discuss their concern.

#### *Long Form Comment Guidelines*

Commenters who wish to submit long form comments are strongly encouraged to use the long comment form template available on the Office's website at <http://copyright.gov/1201/>. Long form comments should be limited to 25 pages in length (which may be single-spaced but should be in at least 12-point type), not including any documentary evidence attached to the comment.

Proponents' initial comments should, at a minimum, address the below points in separately labeled sections, as indicated below and set forth on the long comment form template. Others who wish to provide a legal and/or evidentiary submission in support of or in opposition to an exemption should follow the same format, as should those submitting reply comments. While, as noted, proponents should complete each portion of the long form in making their initial submission, other commenters (including reply commenters) may note "N/A" in any substantive section of the template that they do not wish to complete.

- *Commenter Information.* Identify the commenter, and, if desired, provide a means for others to contact the submitter or an authorized representative of the submitter by email and/or telephone. (Parties should keep in mind that any private, confidential, or personally identifiable information appearing in their submissions will be accessible to the public.)
- *Proposed Class Addressed.* Identify the proposed exemption the comment addresses by the number and name of the class set forth in this Notice of Proposed Rulemaking (e.g., “Proposed Class 7: Audiovisual works – noncommercial remix videos).
- *Overview.* Provide a brief, general explanation of the circumvention activity sought to be exempted or opposed and why.
- *Technological Protection Measure(s) and Method(s) of Circumvention.* Describe the TPM(s) that control access to the work and method(s) of circumvention. The description should provide sufficient information to allow the Office to understand the nature and basic operation of the relevant technologies, as well as how they are disabled or bypassed.
- *Asserted Noninfringing Use(s).* Explain the asserted noninfringing use(s) of copyrighted works said to be facilitated by the proposed exemption. Commenters should provide an evidentiary basis to support their arguments regarding noninfringing uses, including discussion or refutation of specific examples of such uses and, if available, relevant documentary and/or multimedia evidence. This section should identify all statutory provisions, case law, and/or other legal

authority the commenter wishes the Office to consider in connection with the analysis of whether the asserted uses are noninfringing.

- *Adverse Effects.* Explain whether the inability to circumvent the TPM(s) at issue has or is likely to have adverse effects on the asserted noninfringing use(s). The adverse effects can be current, or may be adverse effects that are likely to occur during the next three years, or both. Commenters should also address potential alternatives that permit users to engage in the asserted noninfringing use(s) without the need for circumvention. Commenters should provide an evidentiary basis to support their arguments regarding asserted adverse effects, including discussion or refutation of specific examples of such uses and, if available, relevant documentary or multimedia evidence. This section should identify all statutory provisions, case law, and/or other legal authority the commenter wishes the Office to consider in connection with the analysis of the claimed adverse effects.
- *Statutory Factors.* Evaluate the proposed exemption in light of each of the statutory factors set forth in 17 U.S.C. 1201(a)(1)(C): (i) The availability for use of copyrighted works; (ii) the availability for use of works for nonprofit archival, preservation, and educational purposes; (iii) the impact that the prohibition on the circumvention of TPMs applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research; (iv) the effect of circumvention of TPMs on the market for or value of copyrighted works; and (v) any other factor that may be appropriate for the Librarian to consider in evaluating the exemption. This section should identify all statutory provisions, case law, and/or other legal

authority the commenter wishes the Office to consider in connection with the analysis of these factors.

- *Documentary evidence.* Commenters are encouraged to submit documentary evidence to support or illustrate the information and arguments addressed in the written comments. As indicated in the **ADDRESSES** section above, such documentary evidence must be attached to the written comment (though it does not count towards the 25-page limit).
- *Multimedia evidence.* Commenters are also encouraged, when feasible, to submit multimedia evidence to support or illustrate relevant technologies or points made in written comments. Multimedia evidence must be submitted separately via mail or hand-delivered to the Office and must be contained on specified digital media, in an approved file format, and appropriately labeled, as described in the **ADDRESSES** section above. Where possible and permissible to post the multimedia submission on a publicly accessible website, commenters may wish to include a link to the materials in their comments (although providing such a link is not a substitute for the submission of a physical copy to the Office for inclusion in the official record). As noted above, the Office may post some or all multimedia evidence to its website, depending upon file types and sizes, overall volume, and other constraints. To the extent a multimedia submission is not made available on the Office's website, the Office will make it available for public inspection and copying at the Copyright Office upon written email request. Copying charges for multimedia files will be assessed at the applicable Office rate under 37 CFR 201.3 for copies of the relevant type. If there are unusual practical

or other constraints that preclude the submission of multimedia evidence with the initial written comment, the commenter should contact the Office *at least 21 days before the applicable submission deadline* to discuss whether it would be appropriate to provide a live demonstration at the public hearing and, if so, how any such demonstration would be captured for the official record.

#### *Short Form Comment Guidelines*

- Commenters who wish to submit a brief statement in support of or opposition to a particular proposed exemption are strongly encouraged to use the short comment form template available at <http://www.copyright.gov/1201/>. After supplying the Commenter Information and noting the Proposed Class Addressed as described above, the commenter may offer a general statement of support or opposition. Short form comment submissions should not exceed one single-spaced typed page (in at least 12-point type).

## **II. Review and Classification of Proposed Exemptions**

The Office has reviewed and classified the proposed exemptions set forth in the forty-four petitions received in response to its September Notice, in some cases combining overlapping or similar proposed exemptions, and in other cases subdividing proposals to allow for a more focused record, as detailed below.

At the outset, the Office observes that three of the petitions seek an exemption that cannot be granted as a matter of law, as each seeks to permit circumvention of any and all TPMs constituting “DRM”<sup>8</sup> with respect to unspecified types of copyrighted

---

<sup>8</sup> “DRM,” or digital rights management, is content protection software intended to prevent unauthorized redistribution of copyrighted material. *See, e.g., In re Sony BMG Audio Compact Disc Litig.*, 429 F. Supp. 2d 1378, 1380 (J.P.M.L. 2006).

works for the purpose of engaging in unidentified personal and/or consumer uses.<sup>9</sup> As the Office explained in its September Notice, the DMCA provides that any exemptions adopted as part of this rulemaking must be defined based on “a *particular class* of works.”<sup>10</sup> And, as legislative history elaborates, “the ‘particular class of copyrighted works’ [is intended to] be a *narrow and focused subset* of the broad categories of works . . . identified in Section 102 of the Copyright Act.”<sup>11</sup> That is because the purpose of the rulemaking is to “allow the enforceability of the prohibition against the act of circumvention to be *selectively* waived, for limited time periods, if necessary to prevent a diminution in the availability to individual users of a *particular category* of copyrighted materials.”<sup>12</sup>

In contrast, the three petitions at issue seek an exemption for all works in all media. Moreover, these broad petitions fail to identify “distinct” and “measurable” impacts on noninfringing uses as contemplated by the DMCA.<sup>13</sup> Because it is apparent that the Office may not adopt the sweeping type of exemption proposed by these three petitions consistent with the standards of section 1201(a)(1), the Office declines to put these proposals forward for public comment.<sup>14</sup>

The Office has studied the remaining forty-one proposals and categorized them into twenty-seven proposed classes of works. In some cases, overlapping proposals have

---

<sup>9</sup> See Eldridge Alexander Pet. at 1 (asking the Office to “add an exemption to the DMCA that allows for the removal of DRM for personal, legal uses.”); Ed Grossheim Pet. at 1 (“If I purchase a product it should be mine to do with as I choose without violating copyright.”); Jeremy Putnam Pet. at 1 (“I ask that legal exceptions be made for consumers to remove DRM from all digital content without repercussion.”).

<sup>10</sup> 17 U.S.C. 1201(a)(1)(B) (emphasis added); see also 79 FR at 55690-91.

<sup>11</sup> *Report of the H. Comm. on Commerce on the Digital Millennium Copyright Act of 1998*, H.R. Rep. No. 105-551, pt. 2, at 38 (1992) (emphasis added).

<sup>12</sup> *Id.* at 36 (emphases added).

<sup>13</sup> See *id.* at 37; see also 17 U.S.C. 1201(a)(1)(C).

<sup>14</sup> See 79 FR at 55693.

been merged into a single proposed class. In other cases, individual proposals that encompass multiple proposed uses have been subdivided. For administrative convenience, similar or related classes have also been grouped into overarching categories; the Office notes, however, that it will be considering exemptions on a class-by-class basis.

The Office further notes that it has not put forward precise regulatory language for the proposed classes, because any specific language for exemptions that the Register ultimately recommends to the Librarian will necessarily depend on the full record developed during this rulemaking.<sup>15</sup> Instead, each proposed class is briefly described in Part III below; additional information about the proposals can be found in the underlying petitions posted on the Office's website. As explained in the September Notice, the proposed classes as described here "represent only a starting point for further consideration in the rulemaking proceeding, and will be subject to further refinement based on the record."<sup>16</sup>

In addition, after examining the petitions, the Office has preliminarily identified some initial legal and factual areas of interest with respect to each proposed class. The Office, accordingly, offers guidance below concerning legal and factual issues that commenters may wish to address in connection with particular proposals, as well as particular types of evidence that they may wish to submit. The Office stresses, however, that this preliminary guidance is not exhaustive, and *commenters should consider and offer all legal argument and evidence they believe necessary* to create a complete record. In addition, the Office's early observations are offered without prejudice to the Office's ability to raise other questions or concerns at later stages of the proceeding.

---

<sup>15</sup> *Id.* at 55692.

<sup>16</sup> *Id.* at 55693.

### **III. The Proposed Classes**

#### **A. Audiovisual works on DVD, Blu-ray, and downloaded/streamed video**

Several petitions seek exemptions for circumvention of access controls protecting audiovisual works embodied on DVDs, on Blu-ray discs, and/or in downloaded or streamed videos in connection with three general categories of uses – educational uses; derivative uses; and format and space-shifting. These proposals raise some shared concerns, including the impact of TPMs on the alleged noninfringing uses of audiovisual works and whether alternative methods of accessing the content, such as screen-capture technology, could alleviate potential adverse impacts. Nonetheless, the evidentiary support for these proposed exemptions is likely to vary according to the specific formats and proposed uses. For example, a film studies professor may have a different need to access higher-resolution material than a teacher displaying an excerpt of a copyrighted work to a kindergarten class, and distribution standards for commercial documentary films may require use of higher-resolution material than required for use in noncommercial remix videos. Accordingly, the Office has further subdivided the three general categories of uses into more specific individual classes to permit proponents to better focus their submissions.

##### **1. *Audiovisual works – educational uses***

Multiple petitions seek exemptions for educational uses of audiovisual works. The Office notes that prior rulemakings have granted exemptions relating to uses of motion picture excerpts for commentary, criticism, and educational uses by college and

university faculty and staff and by kindergarten through twelfth-grade educators.<sup>17</sup> The current petitions generally seek to readopt those previously granted exemptions, and some also seek to expand an exemption to accommodate additional technologies, such as Blu-ray discs, or new users, such as museums, libraries, or students and faculty participating in Massive Open Online Courses (“MOOCs”).

The Office has identified some legal and factual issues that appear common to all of the proposed classes relating to educational uses of audiovisual works. In addition to other more specific areas of concern, for each of these proposals, the Office encourages commenters, in the course of detailing how the proposed exemption meets the legal and evidentiary requirements of section 1201(a)(1), to also address – including through the submission of relevant evidence – the following:

- Whether the proposed exemptions may be limited to “motion pictures” as defined under the Copyright Act<sup>18</sup> as opposed to all “audiovisual works”<sup>19</sup> (a broader category that encompasses, for example, video games).
- For each type of requested use, whether circumvention alternatives, such as licensing or screen-capture technology, obviate the need for an exemption.
- Specific examples illustrating the need for the exemption to extend beyond DVDs to other formats, such as Blu-ray discs and TPM-protected content distributed online.

---

<sup>17</sup> 37 CFR 201.40(b)(4)-(7) (2013). *See* 77 FR 65260, 65266-70 (Oct. 26, 2012) (discussing the most recent prior exemptions).

<sup>18</sup> “‘Motion pictures’ are audiovisual works consisting of a series of related images which, when shown in succession, impart an impression of motion, together with accompanying sounds, if any.” 17 U.S.C. 101.

<sup>19</sup> “‘Audiovisual works’ are works that consist of a series of related images which are intrinsically intended to be shown by the use of machines or devices such as projectors, viewers, or electronic equipment, together with accompanying sounds, if any, regardless of the nature of the material objects, such as films or tapes, in which the works are embodied.” *Id.*

*(a) Proposed Class 1: Audiovisual works – educational uses – colleges and universities*

**This proposed class would allow college and university faculty and students to circumvent access controls on lawfully made and acquired motion pictures and other audiovisual works for purposes of criticism and comment. This exemption has been requested for audiovisual material made available in all formats, including DVDs protected by the Content Scramble System (“CSS”), Blu-ray discs protected by the Advanced Access Content System (“AACCS”), and TPM-protected online distribution services.**

Professor Peter Decherney, the College Art Association, the International Communication Association, and the Society for Cinema and Media Studies (collectively referred to here as “Joint Educators”) have filed a petition seeking adoption of a revised version of the previously granted exemptions to permit circumvention of TPMs on DVDs, Blu-ray discs, and videos acquired via online distribution services, for purposes of facilitating educational uses of motion picture excerpts at the college and university level.<sup>20</sup>

The Office encourages commenters, in the course of detailing how the proposed exemption meets the requirements of section 1201(a)(1), to address – including through the submission of relevant evidence – the following:

- The proposed scope of the exemption, such as (a) whether it can be limited to uses requiring close analysis of the copyrighted work (such as in a film studies course), as opposed to general-purpose classroom uses, (b) whether it needs to extend to

---

<sup>20</sup> Joint Educators propose, in relevant part, the following regulatory language: “audiovisual works embodied in physical media (such as DVDs and Blu-Ray Discs) or obtained online (such as through online distribution services and streaming media) that are lawfully made and acquired and that are protected by various technological protection measures, where the circumvention is accomplished by college and university students or faculty (including teaching and research assistants).” Joint Educators Pet. at 1. *See* 37 CFR 201.40(b)(4)-(7) (2013); 77 FR at 65266-70.

Blu-ray in addition to other formats, and (c) whether the exemption should be extended to students in addition to materials prepared by faculty.

- Any changed circumstances in the need for an exemption over the last three years, including whether any viable alternatives to circumvention have emerged or evolved during this period.
- Whether the previously granted exemption has had an adverse effect on the marketplace for the accessed copyrighted works.

**(b) Proposed Class 2: Audiovisual works – educational uses – primary and secondary schools (K-12)**

**This proposed class would allow kindergarten through twelfth-grade educators and students to circumvent access controls on lawfully made and acquired motion pictures and other audiovisual works for educational purposes. This exemption has been requested for audiovisual material made available in all formats, including DVDs protected by CSS, Blu-ray discs protected by AACS, and TPM-protected online distribution services.**

Two submitters – Professor Renee Hobbs and the Library Copyright Alliance (“LCA”) – filed petitions seeking adoption of a revised version of the previously granted exemption to permit circumvention of TPMs on DVDs, Blu-ray discs, and videos acquired via online distribution services, for purposes of facilitating educational uses of motion picture excerpts by kindergarten through twelfth grade educators and students.<sup>21</sup>

---

<sup>21</sup> Hobbs proposes “an exemption that enables educators and students in grades K-12 . . . to ‘rip’ encrypted or copy-protected lawfully accessed audiovisual works used for educational purposes.” Hobbs Pet. at 1. LCA requests “renewal of the exemption granted in the 2012 rulemaking for motion picture excerpts. The exemption should be broadened to apply to all storage media, including Blu-Ray. Further, the exemption for educational purposes should be expanded to apply to students in kindergarten through twelfth grade. LCA also seeks simplification of the exemption so that it could be readily understood by the authors, filmmakers, students, and educators it is intended to benefit.” LCA Motion Picture Pet. at 1. *See* 37 CFR 201.40(b)(4)-(7) (2013); 77 FR at 65266-70.

The Office encourages commenters, in the course of detailing how the proposed exemption meets the requirements of section 1201(a)(1), to address – including through the submission of relevant evidence – the following:

- The proposed scope of the exemption, such as (a) whether it can be limited to uses requiring close analysis of the copyrighted work, as opposed to general-purpose classroom uses, (b) whether it needs to extend to Blu-ray in addition to other formats, and (c) whether it can be limited to materials prepared by faculty.
- Any changed circumstances in the need for an exemption over the last three years, including whether any viable alternatives to circumvention have emerged or evolved during this period.
- Whether the previously granted exemption has had an adverse effect on the marketplace for the accessed copyrighted works.

**(c) *Proposed Class 3: Audiovisual works – educational uses – massive open online courses (“MOOCs”)***

**This proposed class would allow students and faculty participating in Massive Open Online Courses (“MOOCs”) to circumvent access controls on lawfully made and acquired motion pictures and other audiovisual works for purposes of criticism and comment. This exemption has been requested for audiovisual material made available in all formats, including DVDs protected by CSS, Blu-ray discs protected by AACS, and TPM-protected online distribution services.**

The Joint Educators petition requests that any exemption for college and university faculty and staff include those participating in MOOCs, a type of distance education which has become increasingly popular over the last few years.<sup>22</sup>

---

<sup>22</sup> Joint Educators, in relevant part, propose the following regulatory language: “audiovisual works embodied in physical media (such as DVDs and Blu-Ray Discs) or obtained online (such as through online distribution services and streaming media) that are lawfully made and acquired and that are protected by various technological protection measures, where the circumvention is accomplished by . . . students and

The Office encourages commenters, in the course of detailing how the proposed exemption meets the requirements of section 1201(a)(1), to address – including through the submission of relevant evidence – the following:

- The definition of a “MOOC” for purpose of the proposed exemption, with reference to the various distinctions among MOOCs in relation to the proposed exemption, including but not limited to (a) courses offered with free and open content versus courses that require course materials to be licensed by users, (b) courses requiring registration and/or identity verification versus courses without such requirements, (c) courses offered for free versus paid courses, and (d) whether the provider is a nonprofit or for-profit entity.
- How the proposed exemption might affect the market for or value of the accessed copyrighted works, including how access to materials resulting from circumvention of TPMs could be limited to the intended audience.
- Whether or how the exception in 17 U.S.C. 110(2) for distance education is relevant the proposed exemption.
- The proposed scope of the exemption (in light of the proposed definition of MOOC), including (a) whether the exemption can be limited to lower-resolution content, (b) whether it can be limited to uses requiring close analysis of the copyrighted work, and (c) whether it can be limited to materials prepared by faculty.

---

faculty participating in Massive Open Online Courses (MOOCs) for the purpose of criticism or comment.”  
Joint Educators Pet. at 1.

***(d) Proposed Class 4: Audiovisual works – educational uses – educational programs operated by museums, libraries, or nonprofits***

**This proposed class would allow educators and learners in libraries, museums and nonprofit organizations to circumvent access controls on lawfully made and acquired motion pictures and other audiovisual works for educational purposes. This exemption has been requested for audiovisual material made available in all formats, including DVDs protected by CSS, Blu-ray discs protected by AACS, and TPM-protected online distribution services.**

Professor Hobbs has proposed that any exemption for kindergarten through twelfth-grade educators and students include “educators and learners” in libraries, museums, and nonprofit organizations.<sup>23</sup>

The Office encourages commenters, in the course of detailing how the proposed exemption meets the requirements of section 1201(a)(1), to address – including through the submission of relevant evidence – the following:

- The proposed scope of the exemption, such as (a) whether the exemption can be limited to video production, film, and media studies and/or other close analysis of copyrighted works, (b) whether it can be limited to lower-resolution media, (c) the people who would be entitled to use the exemption, including an explanation of who would be included in the proposed categories of “educators” and “learners,” (d) whether the exemption can be limited to prepared presentations by museums, libraries and non-profit entities, and (e) whether the exemption can be limited to use and display within physical spaces as opposed to online use and display.

---

<sup>23</sup> Hobbs proposes that the Register recommend “an exemption that enables . . . educators and learners in libraries, museum and nonprofit organizations to ‘rip’ encrypted or copy-protected lawfully accessed audiovisual works used for educational purposes.” Hobbs Pet. at 1.

- How the proposed exemption might affect the market for or value of the accessed copyrighted works, including how access to materials resulting from circumvention of TPMs could be limited to the intended users and intended uses.

## **2. *Audiovisual works – derivative uses***

Multiple petitions seek exemptions for derivative uses of audiovisual works, including for use in multimedia e-books, in filmmaking, and in non-commercial remix videos. The Office notes that prior rulemakings have granted exemptions relating to uses of motion picture excerpts in noncommercial videos, documentary films, and nonfiction multimedia e-books offering film analysis.<sup>24</sup> The current petitions generally seek to readopt the most recent previously granted exemption while expanding its contours to encompass additional technologies or types of uses.

The Office has identified some legal and factual issues that appear common to all of the proposed classes relating to derivative uses of audiovisual works. In addition to other more specific areas of concern, for each of these proposals, the Office encourages commenters, in the course of detailing how the proposed exemption meets the requirements of section 1201(a)(1), to address – including through the submission of relevant evidence – the following:

- Whether circumvention alternatives, such as licensing or screen-capture technology, would be suitable for each type of requested use.
- Specific examples illustrating the need for the exemption to extend beyond DVDs to other formats, such as Blu-ray discs and TPM-protected content distributed online.

---

<sup>24</sup> See 37 CFR 201.40(b)(4)-(7) (2013); 77 FR at 65266-70.

**(a) Proposed Class 5: Audiovisual works – derivative uses – multimedia e-books**

**This proposed class would allow circumvention of access controls on lawfully made and acquired motion pictures used in connection with multimedia e-book authorship. This exemption has been requested for audiovisual material made available in all formats, including DVDs protected by CSS, Blu-ray discs protected by AACS, and TPM-protected online distribution services.**

Authors Alliance and Professor Bobette Buster (collectively referred to here as “Authors Alliance”) seek adoption of a revised version of the previously granted exemption for multimedia e-books, to permit circumvention of TPMs on DVDs, Blu-ray discs, and videos acquired via online distribution services, for purposes of facilitating uses of motion picture excerpts in nonfiction multimedia e-books offering film analysis.<sup>25</sup>

The Office encourages commenters, in the course of detailing how the proposed exemption meets the requirements of section 1201(a)(1), to address – including through the submission of relevant evidence – the following:

- Whether the exemption should be limited to multimedia e-books containing film analysis or whether a broader exemption is warranted.
- Whether and how the need for an exemption has increased over the last three years due to “new authorship tools, sophisticated digital distribution networks, and widespread consumer adoption of e-book readers.”<sup>26</sup>

---

<sup>25</sup> Authors Alliance requests an exemption “that permits authors of multimedia e-books to circumvent Content Scramble System (“CSS”) on DVDs, Advanced Access Content System (“AACS”) on Blu-ray discs, and encryption and authentication protocols on digitally transmitted video in order to make fair use of motion picture content in their e-books.” Authors Alliance Pet. at 2. See 37 CFR 201.40(b)(4)-(7) (2013); 77 FR at 65266-70.

<sup>26</sup> See Authors Alliance Pet. at 2.

- Any changed circumstances in the need for an exemption over the last three years, including whether any viable alternatives to circumvention have emerged or evolved during this period.
- Whether the previously granted exemption has had an adverse effect on the marketplace for the accessed copyrighted works.

**(b) Proposed Class 6: Audiovisual works – derivative uses – filmmaking uses**

**This proposed class would allow circumvention of access controls on lawfully made and acquired motion pictures for filmmaking purposes. This exemption has been requested for audiovisual material made available in all formats, including DVDs protected by CSS, Blu-ray discs protected by AACS, and TPM-protected online distribution services.**

International Documentary Association, Film Independent, Kartemquin Educational Films, Inc., and National Alliance for Media Arts and Culture (collectively referred to here as “IDA”) seek adoption of a revised version of the previously granted exemption to permit circumvention of TPMs on DVDs, Blu-ray discs, and videos acquired via online distribution services, for purposes of facilitating uses of motion picture excerpts in documentary films.<sup>27</sup>

The Office encourages commenters, in the course of detailing how the proposed exemption meets the requirements of section 1201(a)(1), to address – including through the submission of relevant evidence – the following:

---

<sup>27</sup> IDA requests an exemption for filmmakers who seek to make fair use in their filmmaking of copyrighted motion pictures protected by TPMs on DVDs, Blu-Ray discs, and digitally transmitted video, such as streaming video, digital downloads, or transmissions captured on digital video recorders. IDA Pet. at 2-3. See 37 CFR 201.40(b)(4)-(7) (2013); 77 FR at 65266-70.

- Whether the proposed exemption should extend to commercial uses in fictional (*i.e.*, nondocumentary) films, including whether such uses could supplant derivative markets for the copyrighted works used.
- Whether the exemption can be limited to use of only short portions or clips of motion pictures or, if not, the basis for a broader exemption.
- Specific examples of whether access to Blu-ray content or other high-resolution content is necessary to meet applicable distribution standards for documentary and/or fictional filmmaking.
- Any changed circumstances in the need for an exemption over the last three years, including whether any viable alternatives to circumvention have emerged or evolved during this period.
- Whether the previously granted exemption has had an adverse effect on the marketplace for the accessed copyrighted works.

(c) *Proposed Class 7: Audiovisual works – derivative uses – noncommercial remix videos*

**This proposed class would allow circumvention of access controls on lawfully made and acquired audiovisual works for the sole purpose of extracting clips for inclusion in noncommercial videos that do not infringe copyright. This exemption has been requested for audiovisual material made available on DVDs protected by CSS, Blu-ray discs protected by AACS, and TPM-protected online distribution services.**

Electronic Frontier Foundation (“EFF”) and Organization for Transformative Works (“OTW”) jointly seek adoption of a revised version of the previously granted exemption to permit circumvention of TPMs on DVDs, Blu-ray discs, or videos acquired

via online distribution services, for purposes of facilitating uses of motion picture excerpts in noncommercial remix videos.<sup>28</sup>

The Office encourages commenters, in the course of detailing how the proposed exemption meets the requirements of section 1201(a)(1), to address – including through the submission of relevant evidence – the following:

- The proposed scope of the exemption, including whether the exemption can be limited to: (a) “motion pictures” as defined under the Copyright Act rather than extending to all “audiovisual works,” (b) uses of short portions or clips of motion pictures or audiovisual works, (c) uses for purposes of criticism, comment, or education, as opposed to other “noninfringing” or “fair” uses, (d) “noncommercial videos” as opposed to “primarily noncommercial videos,” (e) with respect to works distributed online, those works that are not readily available on DVD and/or Blu-ray disc, and (f) with respect to Blu-ray discs, those works or content that are not readily available on DVD.
- Any changed circumstances in the need for an exemption over the last three years, including whether any viable alternatives to circumvention have emerged or evolved during this period.
- Whether the previously granted exemption has had an adverse effect on the marketplace for the accessed copyrighted works.

---

<sup>28</sup> EFF/OTW filed two petitions which relate to this class; one for DVD and Blu-ray discs, and one for online content. The respective petitions seek exemptions for “[a]udiovisual works on DVDs and Blu-Ray discs that are lawfully made and acquired and that are protected by Digital Rights Management schemes, where circumvention is undertaken for the sole purpose of extracting clips for inclusion in noncommercial videos that do not infringe copyright” and “[a]udiovisual works that are lawfully made and acquired via online distribution services, where circumvention is undertaken solely for the purpose of extracting clips for inclusion in noncommercial videos that do not infringe copyright.” *See* EFF/OTW Disc Remix Pet. at 1; EFF/OTW Online Remix Pet. at 1. *See* 37 CFR 201.40(b)(4)-(7) (2013); 77 FR at 65266-70.

### 3. *Proposed Class 8: Audiovisual works – space-shifting and format-shifting*

**This proposed class would allow circumvention of access controls on lawfully made and acquired audiovisual works for the purpose of noncommercial space-shifting or format-shifting. This exemption has been requested for audiovisual material made available on DVDs protected by CSS, Blu-ray discs protected by AACS, and TPM-protected online distribution services.**

Public Knowledge filed a petition seeking an exemption permitting circumvention of TPMs on DVDs, Blu-ray discs, and videos acquired via online distribution services for space-shifting or format-shifting for personal use.<sup>29</sup> The Office notes that in the 2006 and 2012 triennial rulemakings, the Librarian rejected proposed exemptions for space-shifting or format-shifting, finding that the proponents had failed to establish under applicable law that space-shifting is a noninfringing use.<sup>30</sup>

The Office encourages commenters, in the course of detailing how the proposed exemption meets the requirements of section 1201(a)(1), to address – including through the submission of relevant evidence – the following:

- Legal and factual bases that establish that space-shifting and format-shifting are noninfringing fair uses.
- The potential adverse effects likely to be suffered over the next three years in the absence of the requested exemption.

---

<sup>29</sup> Public Knowledge proposes “an exemption for digital rights management-encrypted motion pictures and other audiovisual works on lawfully made and lawfully acquired DVDs, Blu-ray discs (‘BDs’), and downloaded files, when circumvention is accomplished for the purpose of noncommercial space shifting of the contained audiovisual content.” Public Knowledge Space-Shifting Pet. at 1. Relatedly, in addition, in the context of a general objection to digital rights management technology, Alpheus Madsen has requested an exemption to allow circumvention of CSS for purposes of playing DVDs on the Linux Operating System. *See* Madsen Pet. at 1.

<sup>30</sup> *See* 77 FR at 65276-77; 71 FR 68472, 68478 (Nov. 27, 2006). The Librarian also previously declined to adopt an exemption to allow motion pictures on DVDs to be played on the Linux operating system. *See* 68 FR 62011, 62017 (Oct. 31, 2003).

- Evidentiary support for the contention that the DVD is becoming obsolete and incompatible with currently produced computing devices, and any contention that the same concern also applies to Blu-ray discs or downloaded video files.
- The specific TPMs sought to be circumvented, including whether they are access or copy controls.
- Whether the proposed exemption can be limited to “motion pictures” as defined under the Copyright Act rather than extending to all “audiovisual works.”
- Whether viable alternatives to circumvention exist, such as screen-capture technology, external drives, alternative playback devices, online subscription services, etc.

## **B. Literary works distributed electronically**

### **1. *Proposed Class 9: Literary works distributed electronically – assistive technologies***

**This proposed class would allow circumvention of access controls on lawfully made and acquired literary works distributed electronically for purposes of accessibility for persons who are print disabled. This exemption has been requested for literary works distributed electronically, including e-books, digital textbooks, and PDF articles.**

The American Foundation for the Blind (“AFB”) and the American Council of the Blind (“ACB”) have jointly requested renewal of an exemption allowing accessibility for persons who are print disabled.<sup>31</sup> The AFB/ACB petition notes that granting such an exemption has historically been relatively uncontroversial and that no one appeared at the 2012 triennial rulemaking hearing to oppose this exemption.<sup>32</sup>

---

<sup>31</sup> AFB/ACB request an exemption to allow “people who are blind, visually impaired, or print disabled, as well as the authorized entities that serve them, to circumvent technological protection measures . . . that prevent or interfere with the use of assistive technologies with electronically distributed literary works.” AFB/ACB Pet. at 2. *See* 37 CFR 201.40 (2013); 77 FR at 65262-63.

<sup>32</sup> AFB/ACB Pet. at 5.

The Office encourages commenters, in the course of detailing how the proposed exemption meets the requirements of section 1201(a)(1), to address – including through the submission of relevant evidence – the following:

- Specific evidence relating to whether and the extent to which the prohibition on circumvention has or is likely to have an adverse effect on the ability of persons who are blind, visually impaired, or print disabled to engage in noninfringing uses, such as by providing a significant representative sample of titles across various e-book formats that are otherwise inaccessible.
- Any changed circumstances in the need for an exemption over the last three years, including whether previous similar exemptions have improved accessibility for persons who are blind, visually impaired, or print disabled.
- Whether the previously granted exemption has had an adverse effect on the marketplace for the accessed copyrighted works and whether the market has evolved to enhance accessibility.
- How accessibility software interacts with TPMs and e-book technology to improve accessibility for persons who are blind, visually impaired, or print disabled.
- To what extent the “anti-copying encryptions” mentioned in the petition can be described as access controls within the meaning of 1201(a)(1).

**2. *Proposed Class 10: Literary works distributed electronically – space-shifting and format-shifting***

**This proposed class would allow circumvention of access controls on lawfully made and acquired literary works distributed electronically for the purpose of noncommercial space-shifting or format-shifting.**

**This exemption has been requested for literary works distributed electronically in e-books.**

Christopher Meadows has requested an exemption to allow space-shifting and format-shifting of lawfully purchased e-books.<sup>33</sup> As noted above, in previous rulemakings, upon recommendation by the Register, the Librarian declined to adopt an exemption for purposes of space-shifting and format-shifting due to the lack of legal precedent establishing that space-shifting and format-shifting are noninfringing uses.<sup>34</sup>

The Office encourages commenters, in the course of detailing how the proposed exemption meets the requirements of section 1201(a)(1), to address – including through the submission of relevant evidence – the following:

- Legal and factual bases that establish that space-shifting and format-shifting are noninfringing fair uses.
- Existing alternatives in the market, if any, that may ameliorate potential adverse effects, such as the extent to which people can purchase material in DRM-free formats.
- Evidentiary support for the concern that e-books distributed by vendors that have gone out of business will become, or have become, unreadable due to TPMs.
- Whether allowing an exemption could harm the market for e-books, including e-book subscription and lending services.

---

<sup>33</sup> Meadows proposes that “[c]onsumers should be legally permitted to remove DRM from electronic books that they have purchased in order to back them up, read them on other e-book platforms, or otherwise make section 107 fair use of the material.” Meadows Pet. at 1.

<sup>34</sup> See 77 FR at 65276-77; 68 FR at 62015-17; 71 FR at 68478. The Register also declined to recommend, and the Librarian declined to adopt, an exemption for creating back-up copies. See 71 FR at 68479.

**C. Software/firmware that enable devices to connect to a wireless network that offers telecommunications and/or information services (“unlocking”)**

The Office has received several petitions seeking exemptions permitting the circumvention of access controls on computer programs that enable wireless telephone handsets (*i.e.*, cellphones) and other wireless devices to connect to a mobile wireless communications network, for purpose of allowing the device to connect to an alternate network. This process is commonly known as “unlocking.” Consistent with the Unlocking Act,<sup>35</sup> the Office will be considering whether to grant an exemption for wireless telephone handsets and whether to “extend” any exemption for wireless telephone handsets to “any other category of wireless devices.”<sup>36</sup>

A few petitions address multiple types of wireless devices. As the Office indicated in its September Notice, however, “[t]he evaluation of whether an exemption would be appropriate under section 1201(a)(1)(C) is likely to be different for different types of wireless devices, requiring distinct legal and evidentiary showings.”<sup>37</sup> For instance, in past rulemakings, determining the existence of a noninfringing use has involved asking whether the software is owned or licensed by the owner of the wireless device.<sup>38</sup> The answer to that question may vary for different types of devices. In addition, the marketplace for cellphones and that for, *e.g.*, tablet computing devices may be quite different with respect to carrier subsidies, service commitments, availability of unlocked devices, and other factors. These differences necessarily will impact the factual and legal analysis. Accordingly, the Office has categorized the petitions into the five proposed

---

<sup>35</sup> Pub. L. 113–144, sec. 2(b), 128 Stat. at 1751; *see also* 79 FR at 55688 (explaining the Unlocking Act).

<sup>36</sup> 70 FR at 55689.

<sup>37</sup> *Id.*

<sup>38</sup> *See, e.g.*, 77 FR at 65265.

classes below, with Proposed Classes 11 through 13 each covering a specific type of device, Proposed Class 14 generally covering “wearable” wireless devices, and Proposed Class 15 representing a broad exemption for all “consumer machines.” While Proposed Classes 14 and 15 appear challenging because of the wide range of devices they purport to cover, the Office hopes to encourage the creation of an adequate administrative record for as many types of devices as possible within the unlocking category.

The Office has identified some legal and factual issues that appear common to all of the proposed classes relating to unlocking. In addition to other more specific areas of concern, for each of these proposals, the Office encourages commenters, in the course of detailing how the proposed exemption meets the requirements of section 1201(a)(1), to also address – including through the submission of relevant evidence – the following:

- Whether an owner of a device at issue in the class also owns the firmware and/or software that runs the device for purposes of 17 U.S.C. 117, which gives software owners certain rights to copy and adapt such programs. In addition, the Office is interested in the relevance, if any, to the section 117 analysis of section 2(c)(2) of the Unlocking Act, which provides that the current cellphone unlocking exemption and any future unlocking exemptions may be initiated “by the *owner of any such handset or other device*.”<sup>39</sup>
- The technical details of how each type of locking mechanism operates – *e.g.*, service provider code locks, system operator code locks, band order locks, and subscriber identity module locks – and how those locks are circumvented. In particular, the Office is interested in determining with precision the instances in

---

<sup>39</sup> Pub. L. 113–144, sec. 2(c)(2), 128 Stat. at 1752 (emphasis added); *see also* 37 CFR 201.40(c).

which unlocking merely involves changing underlying variables relied upon by the device firmware, and those in which unlocking requires copying or rewriting the firmware itself.

- The Office understands that the unlocking exemption is aimed at permitting a device to connect to an alternative mobile wireless telecommunications or data network, such as CDMA, GSM, HSPA+, LTE, or other similar networks.<sup>40</sup> The petitions use differing terminology to refer to these networks, including “wireless communications networks,” “wireless telecommunications networks,” “wireless networks that offer telecommunications and/or information services.” The Office invites discussion on what terminology most accurately describes the networks to which the proposed unlocking exemptions would apply.

### ***1. Proposed Class 11: Unlocking – wireless telephone handsets***

**This proposed class would allow the unlocking of wireless telephone handsets. “Wireless telephone handsets” includes all mobile telephones including feature phones, smart phones, and “phablets” that are used for two-way voice communications.**

Five parties – Consumers Union,<sup>41</sup> the Competitive Carriers Association (“CCA”),<sup>42</sup> the Institute of Scrap Recycling Industries (“ISRI”),<sup>43</sup> Pymatuning

---

<sup>40</sup> The Office does not understand the concept of “unlocking” to be relevant to other types of wireless communications, such as those using the IEEE 802.11 standard employed in Wi-Fi routers, the Bluetooth standard, or the ANT wireless network technology, though it invites comment on that issue to the extent the Office may misunderstand the proposals.

<sup>41</sup> Consumers Union’s proposed regulatory language reads as follows: “Computer programs, in the form of firmware or software, that enable a mobile wireless communications device to connect to a wireless communications network, when circumvention is initiated by – (1) the owner of the device, (2) another person at the direction of the owner, (3) a provider of a commercial mobile radio service or a commercial mobile data service at the direction of such owner or other person, solely in order to enable the device to connect to other wireless communications networks, subject to the connection to any such other wireless communications network being authorized by the operator of such network. The term ‘mobile wireless communications device’ means (1) a wireless telephone handset, or (2) a hand-held mobile wireless device used for any of the same wireless communications functions, and using equivalent technology, as a wireless telephone handset.” Consumers Union Pet. at 3.

Communications (“Pymatuning”),<sup>44</sup> and the Rural Wireless Association (“RWA”)<sup>45</sup> – seek, in essence, renewal of the unlocking exemption for wireless telephone handsets (as reinstated by the Unlocking Act) for another three-year period. Two of the petitions vary in their particulars, however. Pymatuning’s proposal is limited to “used” handsets, but does not define that term. ISRI asks that the exemption specifically allow both “individual and bulk circumvention.”

The Office encourages commenters, in the course of detailing how the proposed exemption meets the requirements of section 1201(a)(1), to address – including through the submission of relevant evidence – the following:

- The current cellphone unlocking policies for all significant wireless carriers, including (a) whether those carriers are adhering to mobile wireless device unlocking guidelines issued by CTIA-The Wireless Association, (b) whether,

---

<sup>42</sup> CCA’s proposed regulatory language reads as follows: “Computer programs, in the form of firmware, software, or data used by firmware or software, that enable wireless handsets to connect to a wireless network that offers telecommunications and/or information services, when circumvention is initiated by the owner of the device, or by another person at the direction of the owner of the device, in order to connect to a wireless network that offers telecommunications and/or information services, and access to the network is authorized by the operator of the network.” CCA Cellphone Unlocking Pet. at 1-2.

<sup>43</sup> ISRI’s proposed regulatory language reads as follows: “Computer programs, in the form of firmware or software, that enable wireless telephone handsets to connect to a wireless telecommunications network, when circumvention, including individual and bulk circumvention for used devices, is initiated by the owner of any such handset, by another person at the direction of the owner, or by a provider of a commercial mobile radio service or a commercial mobile data service at the direction of such owner or other person, solely in order to enable such owner, family member of such owner, or subsequent owner or purchaser of such handset to connect to a wireless telecommunications network when such connection is authorized by the operator of such network.” ISRI Cellphone Unlocking Pet. at 1.

<sup>44</sup> Pymatuning’s proposed regulatory language reads as follows: “Computer programs, in the form of firmware or software, that enable used wireless telephone handsets and other used wireless telecommunications devices to connect to a wireless telecommunications network, when circumvention is initiated by the owner of the copy of the computer program solely in order to connect to a wireless telecommunications network and access to the network is authorized by the operator of the network.” Pymatuning Pet. at 2.

<sup>45</sup> RWA’s proposal would “allow for the circumvention of the technological measures that control access to Wireless Telephone Handset software and firmware to allow the owner of a lawfully acquired handset, or a person designated by the owner of the lawfully acquired handset, to modify the device’s software and firmware so that the wireless device may be used on a technologically compatible wireless network of the customer’s choosing when the connection to the network is authorized by the operator of the network.” *See* RWA Cellphone Unlocking Pet. at 1-2.

under those policies, a consumer's completion of the term of a service contract, or payment of early termination fees, affects his or her ability to unlock a cellphone, and (c) the extent to which those policies obviate the need for an exemption.

- The extent to which unlocked mobile phones are available for purchase, and whether the availability of such phones is a viable alternative to circumvention.
- Whether the exemption should be limited to "used" handsets, and what would qualify a handset as "used."
- The practice and market effects of "bulk circumvention" (or unlocking), and whether the exemption should address "bulk circumvention."
- Any changed circumstances in the need for an exemption over the last three years, including whether any viable alternatives to circumvention have emerged or evolved during this period.
- Whether the previously granted exemption has had an adverse effect on the marketplace for the accessed copyrighted works.

## ***2. Proposed Class 12: Unlocking – all-purpose tablet computers***

**This proposed class would allow the unlocking of all-purpose tablet computers. This class would encompass devices such as the Apple iPad, Microsoft Surface, Amazon Kindle Fire, and Samsung Galaxy Tab, but would exclude specialized devices such as dedicated e-book readers and dedicated handheld gaming devices.**

The Office received several petitions – from CCA,<sup>46</sup> ISRI,<sup>47</sup> and RWA<sup>48</sup> – that specifically seek an exemption to allow the unlocking of all-purpose tablet computers.

---

<sup>46</sup> CCA's proposed regulatory language reads as follows: "Computer programs, in the form of firmware or software, or data used by firmware or software, that enable all-purpose tablet computers to connect to a wireless network that offers telecommunications and/or information services, when circumvention is initiated by the owner of the device, or by another person at the direction of the owner of the device, in

Two other petitions – from Consumers Union<sup>49</sup> and Pymatuning<sup>50</sup> – seek tablet exemptions as part of their cellphone unlocking petitions. Again, Pymatuning’s proposal is limited to “used” tablets, but does not define that term, and ISRI asks that the exemption specifically allow both “individual and bulk circumvention.”

The Office encourages commenters, in the course of detailing how the proposed exemption meets the requirements of section 1201(a)(1), to address – including through the submission of relevant evidence – the following:

- The definition of “all-purpose tablet computer” that would govern the proposed exemption.
- The marketplace for tablets with mobile data connections, including (a) any relevant differences between the marketplace for cellphones and that for tablets, (b) the extent to which wireless carriers subsidize consumer purchases of tablets,

---

order to connect to a wireless network that offers telecommunications and/or information services, and access to the network is authorized by the operator of the network.” CCA Tablet Unlocking Pet. at 1-2.

<sup>47</sup> ISRI’s proposed regulatory language reads as follows: “Computer programs, in the form of firmware or software, that enable all-purpose tablet computers to connect to a wireless telecommunications network, when circumvention, including individual and bulk circumvention for used devices, is initiated by the owner of any such tablet, by another person at the direction of the owner, or by a provider of a commercial mobile radio service or a commercial mobile data service at the direction of such owner or other person, solely in order to enable such owner, family member of such owner, or subsequent owner or purchaser of such tablet to connect to a wireless telecommunications network when such connection is authorized by the operator of such network.” ISRI Tablet Unlocking Pet. at 1.

<sup>48</sup> RWA’s proposal would “allow for the circumvention of the technological measures that control access to all purpose tablet computer (‘Tablet’) software and firmware to allow the owner of a lawfully acquired Tablet, or a person designated by the owner of the lawfully acquired Tablet, to modify the device’s software and firmware so that the wireless device may be used on a technologically compatible wireless network of the customer’s choosing, and when the connection to the network is authorized by the operator of the network.” See RWA Tablet Unlocking Pet. at 1-2.

<sup>49</sup> Consumers Union Pet. at 2-3 (“Consumers Union’s proposed exemption accordingly includes all hand-held mobile wireless devices that are used for essentially the same functions and in the same manner as wireless telephone handsets, including tablets.”).

<sup>50</sup> Pymatuning Pet. at 2 (stating that because “the justifications underlying the [Unlocking] Act also apply to all portable computers, tablets and other types of devices that communicate via wireless telecommunications networks, and that are often locked much the same as wireless telephone handsets, Pymatuning requests that the scope of ‘handsets’ be clarified to include all such wireless telecommunications devices.”).

and require service commitments in return, and (c) the tablet unlocking policies for all significant wireless carriers, including the extent to which those policies obviate the need for an exemption.

- The extent to which unlocked tablets are available for purchase, and whether the availability of such tablets is a viable alternative to circumvention.
- Whether the exemption should be limited to “used” tablets, and what would qualify a tablet as “used.”
- The practice and market effects of “bulk circumvention” (or unlocking), and whether the exemption for tablets should address “bulk circumvention.”

### ***3. Proposed Class 13: Unlocking – mobile connectivity devices***

**This proposed class would allow the unlocking of mobile connectivity devices. “Mobile connectivity devices” are devices that allow users to connect to a mobile data network through either a direct connection or the creation of a local Wi-Fi network created by the device. The category includes mobile hotspots and removable wireless broadband modems.**

Two petitions – from CCA<sup>51</sup> and RWA<sup>52</sup> – seek an exemption to allow the unlocking of mobile connectivity devices such as mobile hotspots and aircards.

---

<sup>51</sup> CCA’s proposed regulatory language reads as follows: “Computer programs, in the form of firmware or software, or data used by firmware or software, that enable mobile hotspots and MiFi devices to connect to a wireless network that offers telecommunications and/or information services, when circumvention is initiated by the owner of the device, or by another person at the direction of the owner of the device, in order to connect to a wireless network that offers telecommunications and/or information services, and access to the network is authorized by the operator of the network.” CCA Mobile Hotspot and MiFi Device Unlocking Pet., at 2.

<sup>52</sup> RWA filed two petitions, one addressed to mobile broadband wireless modems, and the other addressed to mobile hotspots. *See* RWA Mobile Broadband Wireless Unlocking Pet. at 1-2 (seeking exemption “to allow for the circumvention of the technological measures that control access to the software and firmware of mobile broadband wireless modems, which are also known as wireless air cards (‘Air Card’), to allow the owner of a lawfully acquired Air Card, or a person designated by the owner of the lawfully acquired Air Card, to modify the Air Card’s software and firmware so that the device may be used on a technologically compatible wireless network of the customer’s choosing, and when the connection to the network is authorized by the operator of the network”); RWA Mobile Hotspot Unlocking Pet. at 1-2 (same, except that

The Office encourages commenters, in the course of detailing how the proposed exemption meets the requirements of section 1201(a)(1), to address – including through the submission of relevant evidence – the following:

- The marketplace for mobile connectivity devices, including (a) any relevant differences between the marketplace for cellphones and that for mobile connectivity devices, (b) the extent to which wireless carriers subsidize consumer purchases of such devices, and require service commitments in return, and (c) the unlocking policies for all significant wireless carriers with respect to mobile connectivity devices.
- The extent to which unlocked mobile connectivity devices are available for purchase, and whether the availability of such mobile connectivity devices is a viable alternative to circumvention.

#### ***4. Proposed Class 14: Unlocking – wearable computing devices***

**This proposed class would allow the unlocking of wearable wireless devices. “Wearable wireless devices” include all wireless devices that are designed to be worn on the body, including smart watches, fitness devices, and health monitoring devices.**

CCA<sup>53</sup> and RWA<sup>54</sup> both propose an exemption to permit unlocking of wearable mobile wireless devices, a broad category that would include smart watches, fitness devices, health monitoring devices, and perhaps devices such as Google Glass.

---

it seeks to circumvent access controls on “Mobile Wireless Personal Hotspot (‘Mobile Hotspot’) software and firmware”).

<sup>53</sup> CCA addressed what it called “consumer wearables” in the course of its broad catch-all proposal, the remainder of which is addressed in Proposed Class 15. *See* CCA Connected Wearables and Consumer Machines Unlocking Pet. at 1-2.

<sup>54</sup> RWA’s proposed exemption would “allow for the circumvention of the technological measures that control access to wearable mobile wireless device (‘Wearable Wireless Device’) software and firmware to allow the owner of a lawfully acquired Wearable Wireless Device, or a person designated by the owner of the lawfully acquired Wearable Wireless Device, to modify the device’s software and firmware so that the

The Office encourages commenters, in the course of detailing how the proposed exemption meets the requirements of section 1201(a)(1), to address – including through the submission of relevant evidence – the following:

- The specific types of devices that would fall under the proposed exemption.
- The Office’s understanding is that most smart watches, and most if not all fitness and health monitoring devices, do not employ mobile telecommunications or data networks (*e.g.*, HSPA+ or LTE networks) for wireless connections, but instead use either Wi-Fi to connect to a local wireless network, or Bluetooth or ANT technologies to connect to a smartphone or computer. The Office is interested in the extent to which there are wearable wireless devices that directly connect with mobile telecommunications or data networks – and what those devices are – or whether the exemption seeks to permit circumvention of access controls on devices that use Wi-Fi, Bluetooth, or ANT technologies.
- The marketplace for wearable computing devices, including (a) the extent to which wireless carriers subsidize consumer purchases of such devices, and require service commitments in return, and (b) the unlocking policies for all significant wireless carriers with respect to wearable computing devices.
- The extent to which unlocked devices are available for purchase, and whether the availability of such devices is a viable alternative to circumvention.

---

Wearable Wireless Device may be used on a technologically compatible wireless network of the customer’s choosing, and when the connection to the network is authorized by the operator of the network.” RWA Wearable Wireless Device Unlocking Pet. at 1-2. RWA explains that “[a] Wearable Wireless Device is a wearable Internet-connected, voice and touch screen enabled, mobile wireless computing device that is designed to be worn on the body, including but not limited to a smart watch.” *Id.* at 2 n.3.

## 5. *Proposed Class 15: Unlocking – consumer machines*

**This proposed class would allow the unlocking of all wireless “consumer machines,” including smart meters, appliances, and precision-guided commercial equipment.**

CCA has proposed a broad, open-ended exemption for all “consumer machines” – or “the ‘Internet of Things’” – which would encompass a diverse range of devices and equipment.<sup>55</sup> At least as currently framed, it appears that it may be difficult to build an adequate administrative record for this exemption in light of the fact-bound analysis required by section 1201(a)(1). For example, CCA’s proposal refers to “precision-guided commercial equipment” but provides no explanation as to the kind of equipment to which it refers. The Office invites commenters to provide targeted argument and evidence that would allow the Office to narrow this category appropriately.

The Office encourages commenters, in the course of detailing how the proposed exemption meets the requirements of section 1201(a)(1), to address – including through the submission of relevant evidence – the following:

- The extent to which devices understood to be in this class use mobile telecommunications or data networks (*e.g.*, HSPA+ or LTE networks) for wireless connections, rather than Wi-Fi or Bluetooth, or some other technology, and whether parties are seeking to circumvent access controls on devices that use such other technologies.

---

<sup>55</sup> In relevant part, CCA proposes the following regulatory language: “Computer programs, in the form of firmware or software, or data used by firmware or software, that enable . . . consumer machines to connect to a wireless network that offers telecommunications and/or information services, when circumvention is initiated by the owner of the device, or by another person at the direction of the owner of the device, in order to connect to a wireless network that offers telecommunications and/or information services, and access to the network is authorized by the operator of the network.” CCA Connected Wearables and Consumer Machines Unlocking Pet. at 2. CCA states that the “consumer machines” category encompasses “smart meters, connected appliances, connected precision-guided commercial equipment, among others.” *Id.* at 1.

- The extent to which consumers, rather than the device manufacturer or some other entity, select and/or pay for the mobile wireless connection for a smart meter, an appliance, or a piece of precision-guided commercial equipment.
- Specific examples demonstrating adverse effects stemming from a consumer’s inability to choose the mobile wireless communications provider used by a smart meter, an appliance, or a piece of precision-guided commercial equipment.

**D. Software that restricts the use of lawfully obtained software (“jailbreaking”)**

The Office received several petitions for exemptions to allow users to circumvent TPMs protecting computer programs in devices such as cellphones, all-purpose tablets, and smart TVs and that prevent users from running certain software on, or removing preinstalled software from, these devices. This type of circumvention is commonly referred to as the “jailbreaking” or “rooting” of a device, and has been the subject of proposed classes in the last triennial rulemaking and earlier proceedings.<sup>56</sup> The Office has categorized the proposals into Proposed Classes 16 through 20, with each class covering a different type of device.

The Office has identified some legal and factual issues that appear common to all of the proposed classes relating to jailbreaking. In addition to other more specific areas of concern, for each of these proposals, the Office encourages commenters, in the course of detailing how the proposed exemption meets the requirements of section 1201(a)(1), to also address – including through the submission of relevant evidence – the following:

---

<sup>56</sup> See, e.g., 77 FR at 65263-64 (wireless telephone handsets); *id.* at 65272-76 (video game consoles); *id.* at 65274-75 (personal computing devices).

- The extent to which consumers may legally purchase devices that do not contain the complained-of access controls, and whether the availability of such devices eliminates the need for an exemption.
- Whether jailbreaking the device facilitates infringing uses, including access to or consumption of infringing content. The Office is particularly interested in specific examples of noninfringing versus infringing uses, and any available evidence regarding the relative volume of lawful versus pirated content installed on or consumed via jailbroken devices, as well as whether there is a practical way to segregate lawful from unlawful uses.

**1. Proposed Class 16: Jailbreaking – wireless telephone handsets**

**This proposed class would permit the jailbreaking of wireless telephone handsets to allow the devices to run lawfully acquired software that is otherwise prevented from running, or to remove unwanted preinstalled software from the device.**

EFF seeks readoption of an existing exemption allowing the jailbreaking of wireless telephone handsets to allow those devices to interoperate with lawfully obtained software and to allow users to remove unwanted preinstalled software from the device.<sup>57</sup>

The Office encourages commenters, in the course of detailing how the proposed exemption meets the requirements of section 1201(a)(1), to address – including through the submission of relevant evidence – the following:

---

<sup>57</sup> EFF's petition encompassed wireless telephone handsets and other all-purpose mobile computing devices. *See* EFF Jailbreaking Pet. at 1 (suggesting an exemption for “[c]omputer programs that enable mobile computing devices, such as telephone handsets and tablets, to execute lawfully obtained software, where circumvention is accomplished for the sole purposes of enabling interoperability of such software with computer programs of the device, or removing software from the device”). Proposed Class 16 encompasses EFF's proposal with respect to wireless telephone handsets, and Proposed Class 17 encompasses the remainder of EFF's proposal. *See* 37 CFR 201.40(b)(2) (2013); *see also* 77 FR at 65263-64.

- Whether the previously granted exemption has had an adverse effect on the marketplace for wireless telephone handsets or the applications that run on them.
- Specific examples of the following: (a) The manner in which access controls are being used to prevent installation of software that competes with software offered by the device manufacturer, and (b) “unwanted software installed by the manufacturer” that “consumes energy, shortens the device’s battery life, or sends personal information to advertisers” that cannot be uninstalled.<sup>58</sup>

## 2. *Proposed Class 17: Jailbreaking – all-purpose mobile computing devices*

**This proposed class would permit the jailbreaking of all-purpose mobile computing devices to allow the devices to run lawfully acquired software that is otherwise prevented from running, or to remove unwanted preinstalled software from the device. The category “all-purpose mobile computing device” includes all-purpose non-phone devices (such as the Apple iPod touch) and all-purpose tablets (such as the Apple iPad or the Google Nexus). The category does not include specialized devices such as e-book readers or handheld gaming devices, or laptop or desktop computers.**

EFF<sup>59</sup> and Maneesh Pangasa<sup>60</sup> seek to extend any exemption allowing the jailbreaking of wireless telephone handsets<sup>61</sup> to other all-purpose mobile computing devices, including non-phone handheld devices and all-purpose tablets. In the 2012 triennial rulemaking, the Librarian rejected a jailbreaking exemption for tablets because

---

<sup>58</sup> EFF Jailbreaking Pet. at 4.

<sup>59</sup> EFF’s petition seeks, in relevant part, the following proposed class: “Computer programs that enable mobile computing devices, such as . . . tablets, to execute lawfully obtained software, where circumvention is accomplished for the sole purposes of enabling interoperability of such software with computer programs on the device, or removing software from the device.” EFF Jailbreaking Pet. at 1.

<sup>60</sup> Mr. Pangasa’s tablet jailbreaking petition encompasses two distinct proposals. Pangasa Tablet Jailbreaking Pet. at 1-4. The Office has consolidated the portion of Mr. Pangasa’s petition addressing jailbreaking of general purpose tablets with the EFF’s proposal in Proposed Class 17. *See id.* at 1 (“I would like to request an exemption to the Digital Millennium Copyright Act for jail-breaking or rooting tablets like the Apple iPad Air & iPad Mini, Amazon’s Kindle Fire HD, Microsoft Surface line of tablets (particularly the RT version to install hacks that permit running desktop applications on RT devices.”). Mr. Pangasa’s proposal with respect to e-book readers is made part of Proposed Class 18.

<sup>61</sup> *See* 37 CFR 201.40(b)(2) (2013).

“the record lacked a sufficient basis to develop an appropriate definition for the ‘tablet’ category of devices, a necessary predicate to extending the exemption beyond smartphones.”<sup>62</sup> The Librarian acknowledged, however, that “[i]n future rulemakings, as mobile computing technology evolves, such a definition may be more attainable.”<sup>63</sup>

The Office encourages commenters, in the course of detailing how the proposed exemption meets the requirements of section 1201(a)(1), to address – including through the submission of relevant evidence – the following:

- The specific types of devices that would be encompassed by the exemption.
- Whether there are any relevant differences between wireless telephone handsets and other all-purpose computing devices, such as non-phone handheld computing devices and tablets, for purposes of analyzing the proposed exemption.
- Although the EFF’s proposed exemption encompasses all-purpose mobile computing devices, it specifically excludes laptop and desktop computers.<sup>64</sup> The Office is interested in the rationale for that exclusion, and how any exemption would distinguish between those devices that would fall within the exemption and those that would fall outside it.
- Specific examples of the following: (a) The manner in which access controls are being used to prevent installation of software that competes with software offered by the device manufacturer, and (b) “unwanted software installed by the

---

<sup>62</sup> See 77 FR at 65264.

<sup>63</sup> *Id.*

<sup>64</sup> See EFF Jailbreaking Pet. at 2.

manufacturer” that “consumes energy, shortens the device’s battery life, or sends personal information to advertisers” that cannot be uninstalled.<sup>65</sup>

### **3. Proposed Class 18: Jailbreaking – dedicated e-book readers**

**This proposed class would permit the jailbreaking of dedicated e-book readers to allow those devices to run lawfully acquired software that is otherwise prevented from running.**

Maneesh Pangasa filed a petition that, in relevant part, seeks an exemption to allow jailbreaking of dedicated e-book readers such as Amazon’s Kindle Paperwhite and Barnes and Noble’s Nook.<sup>66</sup> Mr. Pangasa provided only a limited explanation of the noninfringing uses that would be facilitated by jailbreaking e-book readers, or of the adverse effects caused by the relevant access controls. In part, it appears his concern may be related to the inability to format-shift or space-shift e-books, a topic that is addressed in Proposed Class 10. Mr. Pangasa also makes a passing reference to enabling “universal access functionality”; the Office notes that e-book accessibility concerns are addressed in Proposed Class 9. Reading the petition generously, Mr. Pangasa does appear to raise a concern that dedicated e-readers may not be able to run lawfully acquired third-party applications. Accordingly, the Office has elected to put forward this proposed class for further comment.

The Office encourages commenters, in the course of detailing how the proposed exemption meets the requirements of section 1201(a)(1), to address – including through the submission of relevant evidence – the following:

---

<sup>65</sup> *Id.* at 4.

<sup>66</sup> *See* Pangasa Tablet Jailbreaking Pet. at 2-4 (“I therefore request an exemption to the Digital Millennium Copyright Act be granted extending the protections for (class #5) mobile phones to include . . . dedicated e-readers like the Amazon Kindle.”).

- The TPMs that are included with dedicated e-book readers, and how they prevent access to the e-book reader’s firmware or software.
- Specific examples of noninfringing uses that are facilitated by the jailbreaking of a dedicated e-book reader, other than enabling accessibility for persons who are print disabled.
- Whether allowing an exemption could harm the market for e-books, including e-book subscription and lending services.

#### **4. Proposed Class 19: Jailbreaking – video game consoles**

**This proposed class would permit the jailbreaking of home video game consoles. Asserted noninfringing uses include installing alternative operating systems, running lawfully acquired applications, preventing the reporting of personal usage information to the manufacturer, and removing region locks. The requested exemption would apply both to older and currently marketed game consoles.**

Maneesh Pangasa has proposed an exemption to permit circumvention of home video game consoles for an assortment of asserted noninfringing uses, including installing alternative operating systems and removing region locks.<sup>67</sup> In the 2012 triennial rulemaking, the Librarian rejected a proposed class seeking an exemption for jailbreaking of video game consoles.<sup>68</sup> Among other things, the Librarian concluded based on the evidentiary record that the jailbreaking of video game consoles “leads to a higher level of infringing activity.”<sup>69</sup> At the same time, the Librarian determined that there was insufficient evidence of adverse impacts on noninfringing uses, because the asserted

---

<sup>67</sup> Mr. Panagasa seeks an exemption “for jail-breaking or rooting home video game consoles like Nintendo’s Wii U, Sony’s Play Station 4, Microsoft’s Xbox One and home media devices like Apple TV which may in future gain the ability to natively play video games.” Pangasa Video Game Console Jailbreaking Pet. at 1.

<sup>68</sup> 77 FR at 65272-74.

<sup>69</sup> *Id.* at 65274.

noninfringing uses were not substantial, and there were alternative devices that allowed users to engage in those uses.<sup>70</sup>

Particularly in light of those earlier conclusions, the Office encourages commenters, in the course of detailing how the proposed exemption meets the requirements of section 1201(a)(1), to address – including through the submission of relevant evidence – the following:

- The nature of the specific TPMs at issue and how they operate, and the particular acts of circumvention required for the jailbreaking of video game consoles as sought in the proposal (including any significant differences among platforms).
- The relationship between the ability to jailbreak consoles and the dissemination and consumption of pirated content, including any practical means to limit the exemption to facilitate noninfringing rather than infringing conduct.
- Specific evidence regarding the adverse impact of access controls in video game consoles on noninfringing uses, including an explanation of why it is necessary to employ the console for particular uses rather than an alternative device such as a general-purpose computer.
- Whether allowing an exemption could harm the market for video game consoles or video games.
- Whether the Librarian’s analysis should distinguish between current-generation game consoles and older game consoles and, if so, how.

---

<sup>70</sup> *Id.*

## 5. *Proposed Class 20: Jailbreaking – smart TVs*

**This proposed class would permit the jailbreaking of computer-embedded televisions (“smart TVs”). Asserted noninfringing uses include accessing lawfully acquired media on external devices, installing user-supplied licensed applications, enabling the operating system to interoperate with local networks and external peripherals, and enabling interoperability with external devices, and improving the TV’s accessibility features (e.g., for hearing-impaired viewers). The TPMs at issue include firmware encryption and administrative access controls that prevent access to the TV’s operating system.**

The Software Freedom Conservancy (“SFC”) has proposed an exemption to permit circumvention of TPMs that protect access to firmware and software on “smart TVs.”<sup>71</sup> It asserts that although modern smart TVs are “full-featured computers,” manufacturers limit their capabilities in a number of ways. For instance, SFC asserts that while smart TVs are internet enabled, they are “limited to accessing only services chosen by the manufacturer.”<sup>72</sup> In addition, SFC asserts that many TVs have USB ports that “can only be used to install manufacturer-supplied updates and connect to manufacturer-sanctioned devices.”<sup>73</sup>

The Office encourages commenters, in the course of detailing how the proposed exemption meets the requirements of section 1201(a)(1), to address – including through the submission of relevant evidence – the following:

- The specific TPMs on smart TVs, how they operate, and methods of circumventing such access controls.

---

<sup>71</sup> SFC’s proposal would “permit owners of computer-embedded televisions (‘Smart TVs’) to circumvent firmware encryption and administrative access controls that control access to the TVs’ operating systems, for the purpose of accessing lawfully-acquired media, installing licensed applications, and enabling interoperability with external devices.” SFC Pet. at 1.

<sup>72</sup> *Id.* at 3.

<sup>73</sup> *Id.*

- Specific examples of noninfringing uses that would be facilitated by circumvention.
- What users seek to do with jailbroken smart TVs, including specific examples of the following: (a) user-supplied software that users wish to install, (b) external hardware users are prevented from connecting absent circumvention, (c) improvements to accessibility for hearing-impaired users that would be facilitated by jailbreaking, and (d) external storage devices through which users seek to access media.
- The reasons smart TV manufacturers limit end users' ability to install third-party applications and/or restrict interoperability with external devices.
- The role of any licensing arrangements between smart TV manufacturers and content or application providers and the extent to which the TPMs at issue protect open-source software.

#### **E. Vehicle software**

Several petitions seek exemptions to permit circumvention of TPMs on software that is embedded in vehicles. The Office has initially consolidated these proposals into the two classes below based on the asserted noninfringing uses and may further refine the two proposed classes based on the record as it develops.

The Office has identified certain areas of inquiry that appear to be common to both of these proposed classes. In addition to other more specific areas of concern, for each of these proposals, the Office encourages commenters, in the course of detailing how the proposed exemption meets the requirements of section 1201(a)(1), to also address – including through the submission of relevant evidence – the following:

- The computers and TPMs used in connection with different types of vehicles, including personal automobiles, commercial motor vehicles, and agricultural machinery, and how they operate.
- Whether the proposed exemption is warranted for all types of motorized land vehicles – including personal automobiles, commercial motor vehicles, and agricultural machinery – and whether and how the analysis may differ for each type of vehicle.

**1. Proposed Class 21: Vehicle software – diagnosis, repair, or modification**

**This proposed class would allow circumvention of TPMs protecting computer programs that control the functioning of a motorized land vehicle, including personal automobiles, commercial motor vehicles, and agricultural machinery, for purposes of lawful diagnosis and repair, or aftermarket personalization, modification, or other improvement. Under the exemption as proposed, circumvention would be allowed when undertaken by or on behalf of the lawful owner of the vehicle.**

EFF has proposed an exemption to allow the circumvention of TPMs on computer programs that are embedded in vehicles for purposes of personalization, modification, or other improvement and would apply to all motorized land vehicles.<sup>74</sup> The Intellectual Property & Technology Law Clinic of the University of Southern California Gould School of Law (“USC Law”) has proposed a similar exemption for agricultural machinery specifically.<sup>75</sup> EFF explains that “[v]ehicle owners expect to be able to repair

---

<sup>74</sup> EFF’s proposed regulatory language reads as follows: “Lawfully-obtained computer programs that control or are intended to control the functioning of a motorized land vehicle, including firmware and firmware updates, where circumvention is undertaken by or on behalf of the lawful owner of such a vehicle for the purpose of lawful aftermarket personalization, improvement, or repair.” EFF Vehicle Software Repair Pet. at 1.

<sup>75</sup> USC Law filed two petitions relating agricultural machinery software. The first seeks an exemption to “allow[] farmers to circumvent . . . TPMs for the purpose of modifying their own agricultural machinery to improve efficiency and/or functionality.” USC Law Vehicle Software Modification Pet. at 1. The second seeks an exemption to “allow[] farmers to circumvent . . . TPMs for the purpose of diagnosing and/or

and tinker with their vehicles[,]” but TPMs on vehicle software “block such legitimate activities, forcing vehicle owners to choose between breaking the law or tinkering and repairing their vehicles.”<sup>76</sup> USC Law similarly observes that farmers specifically require unfettered access to this vehicle software “to make any significant modifications to the efficiency and/or functionality of . . . their increasingly sophisticated agricultural machinery”<sup>77</sup> and to “obtain vital diagnostic information.”<sup>78</sup>

The Office encourages commenters, in the course of detailing how the proposed exemption meets the requirements of section 1201(a)(1), to address – including through the submission of relevant evidence – the following:

- Specific examples of the adverse effects of the TPMs, including how they prevent vehicle owners or others from engaging in lawful diagnosis, repair, or modification activities.
- With respect to *each* of the proposed uses – diagnosis, repair, and modification – (a) the extent to which any of the asserted noninfringing activities merely requires examination or changing of variables or codes relied upon by the vehicle software, or instead requires copying or rewriting of the vehicle software, and (b) whether vehicle owners can properly be considered “owners” of the vehicle software.
- The applicability (or not) of the statutory exemption for reverse engineering in 17 U.S.C. 1201(f) to the proposed uses.

---

repairing their own agricultural machinery.” USC Law Vehicle Software Repair Pet. at 1. At least at this stage of the rulemaking, the Office believes that the two petitions are similar enough that they may be addressed as part of the same proposed class.

<sup>76</sup> EFF Vehicle Software Repair Pet. at 5.

<sup>77</sup> USC Law Vehicle Software Modification Pet. at 2.

<sup>78</sup> USC Law Vehicle Software Repair Pet. at 1.

- Whether a third party – rather than the owner of the vehicle – may lawfully offer or engage in the proposed circumvention activities with respect to that vehicle pursuant to an exemption granted under 17 U.S.C. 1201(a)(1).

## ***2. Proposed Class 22: Vehicle software – security and safety research***

**This proposed class would allow circumvention of TPMs protecting computer programs that control the functioning of a motorized land vehicle for the purpose of researching the security or safety of such vehicles. Under the exemption as proposed, circumvention would be allowed when undertaken by or on behalf of the lawful owner of the vehicle.**

EFF seeks an exemption that would permit circumvention of TPMs on computer programs that are embedded in vehicles for purposes of researching the security or safety of that vehicle.<sup>79</sup> According to EFF, TPMs on vehicle software prevent researchers from “discover[ing] programming errors that endanger passengers” or “errors that would allow a remote attacker to take control of a vehicle’s functions.”<sup>80</sup> Thus, separate and apart from Proposed Class 21, EFF seeks a specific exemption to permit vehicle safety and security research.

The Office encourages commenters, in the course of detailing how the proposed exemption meets the requirements of section 1201(a)(1), to address – including through the submission of relevant evidence – the following:

---

<sup>79</sup> EFF’s proposed regulatory language reads as follows: “Lawfully-obtained computer programs that control or are intended to control the functioning of a motorized land vehicle, including firmware and firmware updates, where circumvention is undertaken by or on behalf of the lawful owner of such a vehicle for the purpose of researching the security or safety of such vehicles.” EFF Vehicle Software Security Pet. at 1.

<sup>80</sup> EFF Vehicle Software Security Pet. at 2.

- Specific examples of the adverse effects of the TPMs, including how they prevent vehicle owners or others from engaging in lawful safety and security research activities.
- With respect to the proposed uses, (a) the extent to which any of the asserted noninfringing activities merely requires examination or changing of variables or codes relied upon by the vehicle software, or instead requires copying or rewriting of the vehicle software, and (b) whether vehicle owners can properly be considered “owners” of the vehicle software.
- Whether granting the exemption could have negative repercussions with respect to the safety or security of vehicles, for example, by making it easier for wrongdoers to access a vehicle’s software.
- The applicability (or not) of the statutory exemptions for reverse engineering in 17 U.S.C. 1201(f) and encryption research in 17 U.S.C. 1201(g) to the proposed uses.
- Whether a third party – rather than the owner of the vehicle – may lawfully offer or engage in the proposed circumvention activities with respect to that vehicle pursuant to an exemption granted under 17 U.S.C. 1201(a)(1).

## **F. Abandoned software**

### **1. *Proposed Class 23: Abandoned software – video games requiring server communication***

**This proposed class would allow circumvention of TPMs on lawfully acquired video games consisting of communication with a developer-operated server for the purpose of either authentication or to enable multiplayer matchmaking, where developer support for those server communications has ended. This exception would not apply to video games whose audiovisual content is primarily stored on the**

**developer’s server, such as massive multiplayer online role-playing games.**

EFF has proposed an exemption to permit circumvention of TPMs on video games that require communication with a server to “enable core functionality” – that is, either “single-player or multiplayer play” – where the developer no longer supports the requisite server or services.<sup>81</sup> EFF claims that an exemption allowing video game owners to circumvent relevant authentication and multiplayer TPMs is necessary to “serve player communities that wish to continue playing their purchased games, as well as archivists, historians, and other academic researchers who preserve and study videogames.”<sup>82</sup>

The Office encourages commenters, in the course of detailing how the proposed exemption meets the requirements of section 1201(a)(1), to address – including through the submission of relevant evidence – the following:

- Specific descriptions of the TPMs and methods of circumvention involved.
- Specific examples of video games that would be covered by this proposed class, including games that can no longer be played at all and games for which single-player play remains possible but cannot be played in multiplayer mode.
- Whether the exemption would threaten the current market for video games (a) by allowing users of unlawfully acquired video games to similarly bypass server checks, (b) by contributing to the circumvention of client-server protocols for

---

<sup>81</sup> EFF’s proposed regulatory language reads as follows: “Literary works in the form of computer programs, where circumvention is undertaken for the purpose of restoring access to single-player or multiplayer video gaming on consoles, personal computers or personal handheld gaming devices when the developer and its agents have ceased to support such gaming.” EFF Abandoned Video Games Pet. at 1.

<sup>82</sup> *Id.* at 1-2.

non-abandoned video games, or (c) by threatening the market for older video games or discouraging the market for backward compatibility of video games.

- The standard for determining when developer support has ended, including whether that standard should have a notice or grace period for developers before the exemption can be used.
- The proposed scope of an exemption, including (a) whether the exemption should differ with respect to games that cannot be played at all because developer support has ended, and those for which only multiplayer support has ended, (b) whether it should exclude video games that are hosted on or played through a remote server, and (c) whether it should be limited to libraries, archivists, historians, or other academic researchers who preserve or study video games.
- Whether the exemption should differ with respect to video games that are made for personal computers, those made for consoles, and those made for handheld devices.

## ***2. Proposed Class 24: Abandoned software – music recording software***

**This proposed class would allow circumvention of access controls consisting of the PACE content protection system, which restricts access to the full functionality of lawfully acquired Ensoniq PARIS music recording software.**

In three similar petitions, Richard Kelley, James McCloskey, and Michael Yanoska have proposed an exemption to permit circumvention of a TPM called PACE that protects access to a specific hardware and software system used for music production

called Ensoniq PARIS.<sup>83</sup> The petitions explain that, when PARIS is installed on a new computer or the hosting computer is modified in some way, the PACE access control requires the user to enter a response code, but these codes soon will no longer be available. Petitioners assert that an exemption will allow for both continued use of the PARIS system and access to existing sound recording files saved using that system, which would otherwise be unrecoverable.

The Office encourages commenters, in the course of detailing how the proposed exemption meets the requirements of section 1201(a)(1), to address – including through the submission of relevant evidence – the following:

- Specific evidence that response codes will no longer be provided to Ensoniq PARIS owners.
- The applicability (or not) of 17 U.S.C. 117 to the maintenance or repair of the hardware and software comprising Ensoniq PARIS or the PACE protection system.
- Whether any portions of the Ensoniq PARIS hardware or software will remain functional without the ability to circumvent the PACE access control.

---

<sup>83</sup> Mr. Kelley alone proposed specific regulatory language as follows: “1) Obsolete software/hardware combinations protected by a software based copy protection mechanism (software dongle) when the manufacturer is unable (because of no longer being in business) or unwilling to provide access via this system to those who are otherwise entitled access; 2) Obsolete software/hardware combinations protected by a software based copy protection mechanism (software dongle) that prevents the hardware and software from running on current operating systems or current hardware by those otherwise entitled to access to the software and hardware.” Kelley Pet. at 1; *see also* McCloskey Pet. at 1 (seeking “a minor broadening of a previous exemption, namely ‘Computer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete’”); Yanoska Pet. at 1 (seeking exemption to allow “[e]limination of the PACE control on recording software that was created and sold over 15 years ago (which is no longer sold or supported by the creating company)”).

- Whether the proposed circumvention could impact others, if any, who use the PACE protection system, including federal agencies and state and local law enforcement personnel who apparently rely upon services from Intelligent Devices, the current proprietor of the PACE access control system.

## **G. Miscellaneous**

### **1. *Proposed Class 25: Software – security research***

**This proposed class would allow researchers to circumvent access controls in relation to computer programs, databases, and devices for purposes of good-faith testing, identifying, disclosing, and fixing of malfunctions, security flaws, or vulnerabilities.**

Two submissions – by Professor Matthew D. Green,<sup>84</sup> and by a group of academic security researchers comprising Professors Steven M. Bellovin, Matt Blaze, Edward W. Felten, J. Alex Halderman, and Nadia Heninger (“Security Researchers”)<sup>85</sup> – seek exemptions for researchers performing good-faith security research. According to the submissions, an exemption is needed to identify, disclose, and fix malfunctions, security flaws, and/or vulnerabilities across a wide range of systems and devices. Petitioners seek to circumvent TPMs in medical devices; car components; supervisory control and data

---

<sup>84</sup> Professor Green’s proposed regulatory language reads as follows: “Computer programs and software, a subcategory of literary works, accessible on personal computers and personal devices and protected by technological protection measures (‘TPMs’) that control access to lawfully obtained works when circumvention is accomplished for the purposes of good faith testing, investigating, or correcting security flaws and vulnerabilities, commentary, criticism, scholarship, or teaching.” Green Pet. at 1.

<sup>85</sup> Security Researchers’ proposed regulatory language reads as follows: “Literary works, including computer programs and databases, protected by access control mechanisms that potentially expose the public to risk of harm due to malfunction, security flaws or vulnerabilities when (a) circumvention is accomplished for the purposes of good faith testing for, investigating, or correcting such malfunction, security flaws or vulnerabilities in a technological protection measures or the underlying work it protects; OR (b) circumvention was part of the testing or investigation into a malfunction, security flaw or vulnerability that resulted in the public dissemination of security research when (1) a copyright holder fails to comply with the standards set forth in ISO 29147 and 30111; or (2) the finder of the malfunction, security flaw or vulnerability reports the malfunction, security flaw or vulnerability to the copyright holder by providing the information set forth in Form A\* in advance of or concurrently with public dissemination of the security research.” Security Researchers Pet. at 1.

acquisition (“SCADA”) systems; and other critical infrastructure, such as the computer code that controls nuclear power plants, smartgrids, and industrial control systems; smartphones that operate critical applications, such as pacemaker applications; internet-enabled consumer goods in the home; and transit systems.<sup>86</sup> According to petitioners, the exemptions codified in subsection (f) of 17 U.S.C. 1201 for reverse engineering, subsection (g) for encryption research, subsection (i) for protection of personally identifying information, and subsection (j) for security testing do not sufficiently capture the breadth of the research they seek to facilitate, and suffer from “ambiguities ... and burdensome requirements to qualify for those exemptions.”<sup>87</sup> As a result, the petitioners say that they have “chosen not to perform specific acts of security research that they believe would have prevented harms to and benefited [the] safety of human persons.”<sup>88</sup>

The Office encourages commenters, in the course of detailing how the proposed exemption meets the requirements of section 1201(a)(1), to address – including through the submission of relevant evidence – the following:

- Specific examples of the types of noninfringing uses that are, or in the next three years, are likely to be adversely affected by a prohibition on circumvention, including the security risks sought to be avoided.
- The specific TPMs sought to be circumvented in connection with particular classes of works and the methods for circumventing those access controls,

---

<sup>86</sup> See Security Researchers Pet. at 2.

<sup>87</sup> Green Pet. at 4; *see also* Security Researchers Pet. at 2.

<sup>88</sup> Security Researchers Pet. at 3. The Office notes that prior exemptions granted in 2006 and 2010 addressed circumvention for investigation or security purposes for the more limited categories of compact discs or video games accessible on personal computers. *See* 37 CFR 201.40(b)(6) (2007) (compact discs); 37 CFR 201.40(b)(4) (2011) (video games); 71 FR at 68477; 75 FR 43825, 43832 (July 27, 2010).

including the environment (academic or otherwise) in which the circumvention would be accomplished.

- Specific examples of acts of security research that have been foregone or delayed due to the current lack of the proposed exemption.
- Whether granting the exemption could have negative repercussions with respect to the safety or security of the works that are subject to research, for example, by making it easier for wrongdoers to access sensitive applications or databases.
- Any industry standards that the Office should consider in evaluating this request, such as the ISO 29147 and ISO 30111 security guidelines, including an explanation of how these standards may relate to the proposed exemption.

## ***2. Proposed Class 26: Software – 3D printers***

**This proposed class would allow circumvention of TPMs on firmware or software in 3D printers to allow use of non-manufacturer-approved feedstock in the printer.**

Public Knowledge seeks an exemption to circumvent TPMs on computer programs used in 3D printers to allow use of non-manufacturer-approved feedstock in such printers.<sup>89</sup>

The Office encourages commenters, in the course of detailing how the proposed exemption meets the requirements of section 1201(a)(1), to address – including through the submission of relevant evidence – the following:

---

<sup>89</sup> Public Knowledge “seeks an exemption for users of 3D printers that are protected by control technologies when circumvention is accomplishe[d] solely for the purpose of using non-manufacturer approved feedstock in the printer.” Public Knowledge 3D Printer Pet. at 2.

- Specific examples of 3D printers that include the complained-of access controls, including a description of the applicable TPMs, how they operate, and methods of circumvention.
- The extent to which there are available for purchase 3D printers that do not include such access controls, and whether the existence of such printers obviates the need for an exemption.

### 3. *Proposed Class 27: Software – networked medical devices*

**The proposed class would allow circumvention of TPMs protecting computer programs in medical devices designed for attachment to or implantation in patients and in their corresponding monitoring devices, as well as the outputs generated through those programs. As proposed, the exemption would be limited to cases where circumvention is at the direction of a patient seeking access to information generated by his or her own device, or at the direction of those conducting research into the safety, security, and effectiveness of such devices. The proposal would cover devices such as pacemakers, implantable cardioverter defibrillators, insulin pumps, and continuous glucose monitors.**

This proposal, filed by a coalition of medical device patients and researchers (“Medical Device Research Coalition”), seeks an exemption to allow circumvention of TPMs in the firmware or software of medical devices and their corresponding monitoring systems at patient direction or for purposes of safety, security, or effectiveness research.<sup>90</sup> According to the petition, “[m]any medical device manufacturers use measures to control access” to medical device software, including password systems and encryption of

---

<sup>90</sup> The Medical Device Research Coalition’s proposed regulatory language reads as follows: “Computer programs, in the form of firmware or software, including the outputs generated by those programs, that are contained within or generated by medical devices and their corresponding monitoring systems, when such devices are designed for attachment to or implantation in patients, and where such circumvention is at the direction of a patient seeking access to information generated by his or her own device or at the direction of those conducting research into the safety, security, and effectiveness of such devices.” Medical Device Research Coalition Pet. at 1-2.

outputs.<sup>91</sup> The Office encourages commenters, in the course of detailing how the proposed exemption meets the requirements of section 1201(a)(1), to address – including through the submission of relevant evidence – the following:

- Specific examples demonstrating the noninfringing uses and adverse effects of the TPMs, including how patients seeking access to information generated by their own devices, and/or those seeking to conduct research into the safety, security, and effectiveness of such devices, are prevented from engaging in lawful activities because of the TPMs.
- Whether the exemption should distinguish among different users (researchers, patients, healthcare providers at the direction of the device-user patient, etc.) and/or the proposed use (examining output of devices, research into safety, security, and effectiveness of devices, etc.).
- Whether the outputs generated by the medical device programs constitute copyright-protected materials.
- Whether granting the exemption could have negative repercussions with respect to the safety or security of the relevant medical devices, for example, by making it easier for wrongdoers to access such medical devices' software or outputs.
- The relevance of the statutory exemptions for reverse engineering in 17 U.S.C. 1201(f) and for encryption research in 17 U.S.C. 1201(g) to the proposed uses.

---

<sup>91</sup> *Id.* at 2.

- Whether a third party – rather than the owner of the device – may lawfully offer or engage in the proposed circumvention activities with respect to that device pursuant to an exemption granted under 17 U.S.C. 1201(a)(1).

Dated: December 9, 2014.

**Jacqueline C. Charlesworth,**  
*General Counsel and  
Associate Register of Copyrights.*

**BILLING CODE 1410-30-P**

**[FR Doc. 2014-29237 Filed 12/11/2014 at 8:45 am; Publication Date: 12/12/2014]**