The Register of Copyrights
United States Copyright Office • Library of Congress • 101 Independence Avenue SE • Washington, DC 20559-6000

TO: James H. Billington
The Librarian of Congress

DATE: June 11, 2010

FROM: Marybeth Peters
Register of Copyrights

SUBJECT: Recommendation of the Register of Copyrights in RM 2008-8; Rulemaking on Exemptions from Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies

I am pleased to present my recommendation relating to the rulemaking on exemptions from the prohibition on circumvention of technological measures that control access to copyrighted works. This document constitutes my formal recommendation, as required pursuant to 17 U.S.C. § 1201(a)(1)(C).

Outline of the Recommendation

I. BACKGROUND

A. Legislative Requirements for Rulemaking Proceeding

B. Responsibilities of Register of Copyrights and Librarian of Congress

C. The Purpose and Focus of the Rulemaking

1. *Purpose of the Rulemaking*

2. *The Necessary Showing*

3. *Determination of "Class of Works"*

D. Consultation with the Assistant Secretary for Communications and Information

II. SOLICITATION OF PUBLIC COMMENTS AND HEARINGS

III. THE DESIGNATED CLASSES

A. Motion pictures on DVDs that are lawfully made and acquired and that are protected by the Content Scrambling System when circumvention is accomplished solely in order to accomplish the incorporation of short portions of motion pictures into new works for the purpose of criticism or comment, and where the person engaging in circumvention believes and has reasonable grounds for believing that circumvention is necessary to fulfill the purpose of the use in the following instances:

- **Educational uses by college and university professors and by college and university film and media studies students;**

- **Documentary filmmaking;**

- **Noncommercial videos**

B. Computer programs that enable wireless telephone handsets to execute software applications, where circumvention is accomplished for the sole purpose of enabling interoperability of such applications, when they have been lawfully obtained, with computer programs on the telephone handset.

C. Computer programs, in the form of firmware or software, that enable used wireless telephone handsets 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.

D. Video games accessible on personal computers and protected by technological protection measures that control access to lawfully obtained works, when circumvention is accomplished solely for the purpose of good faith testing for, investigating, or correcting security flaws or vulnerabilities, if:

- **The information derived from the security testing is used primarily to promote the security of the owner or operator of a computer, computer system, or computer network; and**

- **The information derived from the security testing is used or maintained in a manner that does not facilitate copyright infringement or a violation of applicable law**.

E. Computer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete. A dongle shall be considered obsolete if it is no longer manufactured or if a replacement or repair is no longer reasonably available in the commercial marketplace.

IV. OTHER CLASSES CONSIDERED, BUT NOT RECOMMENDED

A. Subscription based services that offer DRM-protected streaming video where the provider has only made available players for a limited number of platforms, effectively creating an access control that requires a specific

operating system version and/or set of hardware to view purchased material; and

Motion pictures protected by anti-access measures, such that access to the motion picture content requires use of a certain platform.

B. Lawfully purchased sound recordings, audiovisual works, and software programs distributed commercially in digital format by online music and media stores and protected by technological measures that depend on the continued availability of authenticating servers, when such authenticating servers cease functioning because the store fails or for other reasons; and

Lawfully purchased sound recordings, audiovisual works, and software programs distributed commercially in digital format by online music and media stores and protected by technological measures that depend on the continued availability of authenticating servers, prior to the failure of the servers for technologists and researchers studying and documenting how the authenticating servers that effectuate the technological measures function.

C. Software and information recorded, produced, stored, manipulated or delivered by the software, that a forensic investigator seeks to copy, activate, or reverse engineer in order to obtain evidence in a court proceeding.

D. Audiovisual works delivered by digital television ("DTV") transmission intended for free, over-the-air reception by anyone, which are marked with a "broadcast flag" indicator that prevents, restricts, or inhibits the ability of recipients to access the work at a time of the recipient's choosing and subsequent to the time of transmission, or using a machine owned by the recipient but which is not the same machine that originally acquired the transmission.

E. Audiovisual works embedded in a physical medium (such as Blu-Ray discs) which are marked for "down-conversion" or "down-resolutioning" (such as by the presence of an Image Constraint Token "ICT") when the work is to be conveyed through any of a playback machine's existing audio or visual output connectors, and therefore restricts the literal quantity of the embedded work available to the user (measured by visual resolution, temporal resolution, and color fidelity).

F. Literary works distributed in ebook format when all existing ebook editions of the work (including digital text editions made available by authorized entities) contain access controls that prevent the enabling either of the book's read-aloud function or of screen readers that render the text into a specialized format.

I. BACKGROUND

A. Legislative Requirements for Rulemaking Proceeding

The Digital Millennium Copyright Act ("DMCA"), Pub. L. No. 105-304 (1998), was enacted to implement certain provisions of the WIPO Copyright Treaty ("WCT") and WIPO Performances and Phonograms Treaty ("WPPT"). It established "a wide range of rules that will govern not only copyright owners in the marketplace for electronic commerce, but also consumers, manufacturers, distributors, libraries, educators, and on-line service providers"; it "define[d] whether consumers and businesses may engage in certain conduct, or use certain devices, in the course of transacting electronic commerce."[1]

Title I of the Act, which added a new Chapter 12 to title 17 of the United States Code, prohibits circumvention of certain technological measures employed by or on behalf of copyright owners to protect their works (*i.e*. "access controls"). Specifically, Section 1201(a)(1)(A)[2] provides, in part, that "[n]o person shall circumvent a technological measure that effectively controls access to a work protected under this title." In order to ensure that the public will have continued ability to engage in noninfringing uses of copyrighted works, such as fair use,[3] subparagraph (B) limits this prohibition. It provides that the prohibition against circumvention "shall not apply to persons who are users of a copyrighted work which is in a particular class of works, if such persons are, or are likely to be in the succeeding three-year period, adversely affected by virtue of such prohibition in their ability to make noninfringing uses of that particular class of works under this title" as determined in a rulemaking proceeding. The rulemaking proceeding is conducted by the Register of Copyrights, who is to provide notice of the rulemaking, seek comments from the public, consult with the Assistant Secretary for Communications and Information of the Department of Commerce, and recommend final regulations to the Librarian of Congress.[4] The regulations, to be issued by the Librarian of Congress, announce "any class of copyrighted works for which the Librarian has determined,

---

[1] Report of the House Committee on Commerce on the Digital Millennium Copyright Act of 1998, H.R. Rep. No. 105-551, pt. 2, at 22 (1998) ("Commerce Comm. Report").

[2] Unless otherwise stated, all statutory references hereinafter are to sections of title 17, United States Code.

[3] *See* Commerce Comm. Report at 25-26, 35.

[4] Report of the Committee of Conference on the Digital Millennium Copyright Act, H.R. Conf. Rep. No. 105-796, at 64 (1998) ("Conf. Report"). In addition, a number of statutory exceptions are codified at Section 1201(d)-(j).

pursuant to the rulemaking conducted under subparagraph (C), that noninfringing uses by persons who are users of a copyrighted work are, or are likely to be, adversely affected, and the prohibition contained in subparagraph (A) shall not apply to such users with respect to such class of works for the ensuing 3-year period."[5]

This is the fourth Section 1201 rulemaking. The first rulemaking culminated in the Librarian's issuance of a regulation on October 27, 2000, announcing that noninfringing users of two classes of works would not be subject to the prohibition against circumvention of access controls.[6] The second rulemaking resulted in the Librarian's decision on October 28, 2003, that the prohibition against circumvention would not apply to persons who engage in noninfringing uses of four classes of copyrighted works.[7] In the third rulemaking, the Librarian announced on November 27, 2006, that noninfringing users of the following six classes of works would not be subject to the prohibition on circumvention:

> 1. Audiovisual works included in the educational library of a college or university's film or media studies department, when circumvention is accomplished for the purpose of making compilations of portions of those works for educational use in the classroom by media studies or film professors.
>
> 2. Computer programs and video games distributed in formats that have become obsolete and that require the original media or hardware as a condition of access, when circumvention is accomplished for the purpose of preservation or archival reproduction of published digital works by a library or archive. A format shall be considered obsolete if the machine or system necessary to render perceptible a work stored in that format is no longer manufactured or is no longer reasonably available in the commercial marketplace.
>
> 3. Computer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete. A dongle shall be considered obsolete if it is no longer manufactured or if a replacement or repair is no longer reasonably available in the commercial marketplace.
>
> 4. Literary works distributed in ebook format when all existing ebook editions of

---

[5] *See* Section 1201(a)(1)(D).

[6] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Recommendation of the Register of Copyrights, 65 Fed. Reg. 64,555 (Oct. 27, 2000) ("2000 Recommendation of the Register of Copyrights").

[7] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 68 Fed. Reg. 62,011 (Oct. 31, 2003).

the work (including digital text editions made available by authorized entities) contain access controls that prevent the enabling either of the book's read-aloud function or of screen readers that render the text into a specialized format.

5. Computer programs in the form of firmware that enable wireless telephone handsets to connect to a wireless telephone communication network, when circumvention is accomplished for the sole purpose of lawfully connecting to a wireless telephone communication network.

6. Sound recordings, and audiovisual works associated with those sound recordings, distributed in compact disc format and protected by technological protection measures that control access to lawfully purchased works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities.[8]

B. Responsibilities of Register of Copyrights and Librarian of Congress

As noted above, the prohibition against circumvention is subject to triennial review by the Register of Copyrights and the Librarian of Congress in order to permit a determination whether users of particular classes of copyrighted works are, or in the next three years are likely to be, adversely affected by the prohibition in their ability to make noninfringing uses of copyrighted works. The primary responsibility of the Register and the Librarian in this rulemaking proceeding is to assess whether the implementation of access control measures is diminishing the ability of individuals to use copyrighted works in ways that are not infringing.[9] As examples of technological protection measures in effect today, the House Commerce Committee offered the use of "password codes" to control authorized access to computer programs and encryption or scrambling of cable

---

[8] *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 71 Fed. Reg. 68,472 (Nov. 27, 2006).

[9] Commerce Comm. Report at 37. The Commerce Committee Report referred to "whether the prevalence of these technological protections, with respect to particular categories of copyrighted materials, is diminishing the ability of individuals to use those works in ways that are otherwise lawful." However, in the draft of the DMCA under consideration at the time, the provision that eventually would become Section 1201 was worded somewhat differently, placing the responsibility for the rulemaking with the Secretary of Commerce, who was to determine "whether users of copyrighted works have been, or are likely to be in the succeeding 2-year period, adversely affected by the implementation of technological protection measures that effectively control access to works protected under title 17, United States Code, in their ability to *make lawful uses* under title 17, United States Code, of copyrighted works." (Emphasis added.) Thus, the subsequent amendment changing "lawful" to "noninfringing" clarifies that the focus of the rulemaking is on whether access controls have adversely affected the ability of users to make noninfringing uses, a somewhat narrower focus than might have been the case if the original proposed statutory text – "lawful uses" – had been retained. Note, however, that even the original proposed text referred to "lawful uses under title 17."

programming, videocassettes, and CD-ROMs.[10] Congress intended that the Register solicit input that would enable consideration of a broad range of current or likely future adverse impacts. The statute directs that in conducting the rulemaking, the Register and the Librarian shall examine:

> (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 technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research;
> (iv) The effect of circumvention of technological measures on the market for or value of copyrighted works; and
> (v) Such other factors as the Librarian considers appropriate.

These factors to be considered in the rulemaking process require the Register to carefully balance the availability of works for use, the effect of the prohibition on particular uses, and the effect of circumvention on copyrighted works.[11]

C. The Purpose and Focus of the Rulemaking

1. *Purpose of the Rulemaking*

As originally drafted, Section 1201(a)(1) consisted of only one sentence--what is now the first sentence of Section 1201(a)(1): "No person shall circumvent a technological protection measure that effectively controls access to a work protected under this title."[12] Section 1201(a)(2), like the provision finally enacted, would prohibit the manufacture, importation, offering to the public, providing or otherwise trafficking in any technology, product, service, device, or component to circumvent access control measures. Section 1201(a) thus addressed "access control" measures, prohibiting both the conduct of circumventing access control measures and making or trafficking in products, services and devices that circumvent access control measures. In addition to these measures relating to circumvention of access control measures, Section 1201 also addressed circumvention of a different type of technological measure. As originally drafted and as finally enacted, Section 1201(b) prohibits the manufacture, importation,

---

[10] *Id.*

[11] Section 1201(a)(1)(C)(i)-(v).

[12] *See* Report of the Senate Committee on the Judiciary on the Digital Millennium Copyright Act of 1998, S. Rep. No. 195-190 (1998) ("Senate Report").

offering to the public, providing or otherwise trafficking in any technology, product, service, device, or component to circumvent protection afforded by a technological measure that effectively protects a right of a copyright owner under title 17 in a copyrighted work. The type of technological measure addressed in Section 1201(b) includes copy-control measures and other measures that control uses of works that would infringe the exclusive rights of the copyright owner. They will frequently be referred to herein as copy controls. But unlike Section 1201(a), which prohibits both the conduct of circumvention and devices that circumvent, Section 1201(b) does not prohibit the conduct of circumventing copy control measures. The prohibition in Section 1201(b) extends only to devices that circumvent copy control measures. The decision not to prohibit the conduct of circumventing copy controls was made, in part, because it would penalize some noninfringing conduct such as fair use.

In the House of Representatives, the DMCA was sequentially referred to the Committee on Commerce after it was reported out of the Judiciary Committee. The Commerce Committee was concerned that Section 1201, in its original form, might undermine Congress's commitment to fair use.[13] The Committee acknowledged that the growth and development of the Internet has had a significant positive impact on the access of students, researchers, consumers, and the public to information. It also recognized that a plethora of information, most of it embodied in materials subject to copyright protection, was available to individuals, often for free, that in the past could only have been located and acquired only through the expenditure of considerable time, resources, and money.[14] The Committee expressed concern that marketplace realities may someday dictate a different outcome, resulting in less access, rather than more, to copyrighted materials that are important to education, scholarship, and other socially vital endeavors.[15] It noted that possible measures that might lead to such an outcome included the elimination of print or other hard-copy versions, permanent encryption of all electronic copies and adoption of business models that restrict distribution and availability of works. The Committee concluded that "[i]n this scenario, it could be appropriate to modify the flat prohibition against the circumvention of effective technological measures that control access to copyrighted materials, in order to ensure that access for lawful purposes is not unjustifiably diminished."[16] In order to address such possible developments, the Commerce Committee proposed a modification of

---

[13] Commerce Comm. Report at 35.

[14] *Id.*

[15] *Id.* at 36.

[16] *Id.*

Section 1201 which it characterized as a "fail-safe mechanism."[17] In the words of the Committee Report, this mechanism would monitor developments in the marketplace for copyrighted materials, and 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.[18] The "fail-safe" mechanism is this rulemaking. In its final form as enacted by Congress, slightly modified from the mechanism that appeared in the version of the DMCA reported out of the Commerce Committee, the Register is to conduct a rulemaking proceeding and, after consulting with the Assistant Secretary for Communications and Information of the Department of Commerce, recommend to the Librarian whether he should conclude that persons who are users of a copyrighted work are, or are likely to be in the succeeding 3-year period, adversely affected by the prohibition under Section 1201(a)(1) in their ability to make noninfringing uses under title 17 of a particular class of copyrighted works.[19] "The Librarian shall publish any class of copyrighted works for which the Librarian has determined, pursuant to the rulemaking conducted under subparagraph (C), that noninfringing uses by persons who are users of a copyrighted work are, or are likely to be, adversely affected, and the prohibition contained in subparagraph (A) shall not apply to such users with respect to such class of works for the ensuing 3-year period."[20] The Commerce Committee offered additional guidance as to the task of the Register and the Librarian in this rulemaking: "The goal of the proceeding is to assess whether the implementation of technological protection measures that effectively control access to copyrighted works is adversely affecting the ability of individual users to make lawful uses of copyrighted works . . . . The primary goal of the rulemaking proceeding is to assess whether the prevalence of these technological protections, with respect to particular categories of copyrighted materials, is diminishing the ability of individuals to use these works in ways that are otherwise lawful."[21] Thus, the task of this rulemaking is to determine whether the availability and use of access control measures has already diminished or is about to diminish the ability of the public to engage in noninfringing uses of copyrighted works similar or analogous to those that the public had

---

[17] *Id.*

[18] *Id.*

[19] 17 U.S.C. § 1201(a)(1)(C)..

[20] 17 U.S.C. § 1201(a)(1)(D).

[21] Commerce Comm. Report at 37. *Accord* Section-By-Section Analysis of H.R. 2281 as passed by the United States House of Representatives on August 4, 1998. House Comm. on the Judiciary, 105th Cong., (Comm. Print 1998) at 6 ("House Manager's Report"). *See*, *supra*, regarding the change from "lawful" to "noninfringing" in the text of what became Section 1201.

traditionally been able to make prior to the enactment of the DMCA. As the Commerce Committee Report stated, in examining the factors set forth in Section 1201(a)(1)(C), the focus must be on "whether the implementation of technological protection measures (such as encryption or scrambling) has caused adverse impact on the ability of users to make lawful uses."[22]

2. *The Necessary Showing*

In the first Section 1201 rulemaking, the Register concluded, based on a review of the statutory text and the legislative history, that a determination to designate a class of works in this rulemaking must be based on a showing that the prohibition has or is likely to have a substantial adverse effect on noninfringing uses of a particular class of works.[23] The required showing of a "substantial" adverse effect is drawn from the legislative history, where the requirement is variously stated as substantial adverse impact, distinct, verifiable, and measurable impacts, and "more than de minimis impacts."[24] Similarly, for proof of "likely" adverse effects on noninfringing uses, the Register found that a proponent must prove by a preponderance of the evidence that the harm alleged is more likely than not; a proponent may not rely on speculation alone to sustain a prima facie case of likely adverse effects on noninfringing uses.[25] If the evidence is based on likely adverse effects on noninfringing uses, and the proponent demonstrates that such an effect is more likely than not in the ensuing three-year period, the proponent must demonstrate that the adverse impact is substantial (*i.e.*, more than de minimis), and distinct (*i.e.*, more than a vague or generalized claim unrelated to a particular class). The Register also emphasized the requirement of showing a causal nexus between the prohibition on circumvention and the alleged harm. Adverse impacts that are the result of factors other than the prohibition are not within the scope of this rulemaking.[26]

The demonstration of a present or likely adverse effect is only part of the requisite threshold showing. Proponents of designating a particular class of works must also provide sufficient facts and legal analysis to demonstrate that the underlying use affected by the prohibition is a noninfringing use. In the current proceeding, some proponents of certain classes

---

[22] Commerce Comm. Report at 37.

[23] 2000 Recommendation of the Register of Copyrights, 65 Fed. Reg. at 64,558.

[24] *See* Notice of Inquiry, 70 Fed. Reg. 57,526, 57,528 (Oct. 3, 2005).

[25] *See id.*

[26] 2000 Recommendation of the Register of Copyrights, 65 Fed. Reg. at 64,559.

of works asserted that where it is unclear whether a particular use is a fair use, the Register and Librarian should give the benefit of the doubt to the proponent of designating the class.[27] They argued that this process would provide courts with the opportunity to assess the underlying use and render a determination whether the uses are infringing or noninfringing. If the court found that the use was noninfringing, there would be no liability for circumvention under Section 1201(a)(1). On the other hand, if the court found that the underlying use was infringing, then the designation of the class would not shield them from liability under Section 1201(a)(1). Proponents of this approach argued that it would allow for a development of copyright law, particularly as it relates to fair use, and that failing to take such an approach would effectively foreclose the courts from "breaking new ground" on fair use because "if a proposed exemption involved an activity supported by a fair use argument that has yet to be addressed by the courts, and the exemption were denied, a court may never have the opportunity to rule on the question because a defendant may be unable to raise the fair use defense against a Section 1201(a)(1) claim."[28]

More specifically, that proponent suggested that "[i]f the Librarian is satisfied that the activity in question might plausibly be a fair use or be protected by any other statutory exception, but has some doubt on the question, then the Librarian should narrow the proposed exemption to apply only so long as the activity in question is noninfringing."[29]

The Register declines to incorporate such a rule of doubt in this proceeding. While someone who must circumvent an access control in order to engage in what she believes to be a fair use might be deterred from doing so due to the knowledge that she would have no defense to a claim that she had violated Section 1201(a)(1), that does not lead to the conclusion that a class should be designated whenever a proponent has offered a plausible but ultimately unpersuasive argument that a particular use is fair or otherwise noninfringing. The statute requires that the Register recommend, and the Librarian designate, a class based on a finding that users of works in that class "are, or are likely to be in the succeeding 3-year period, adversely affected by virtue of such prohibition in their ability to make noninfringing uses of that particular class of works."[30]

---

[27] C11A (EFF) at 2-4.

[28] *Id.* at 3.

[29] *Id.* at 3-4.

[30] *See* 17 U.S.C. § 1201(a)(1)(B).

That language requires a conclusion that the use *is* or *is likely to be* noninfringing, not merely that the use could plausibly be considered noninfringing.[31] And the burden of proving that a particular use is noninfringing belongs to the proponent of a class of works.[32]

That does not mean that unless there is a controlling precedent directly on point, the Register and the Librarian must conclude that a particular use is an infringing use. If, for example, based on a review and application of the statutory factors set forth in Section 107 and a review and analysis of judicial precedents, the Register and Librarian conclude that a particular use, although never before adjudicated in the courts, is a fair use, the Librarian may designate a class of works based upon the conclusion that the use in question is fair if all the other requirements for designating the class have been satisfied. But it is not sufficient to conclude that a use *could conceivably* be fair. The burden of persuasion is on the proponent of the class.

With respect to the claim that a failure in such a case to designate a class might forever deprive the courts of the ability to consider whether a particular use is noninfringing, the Register considers that scenario unlikely. If, for example, the Register had recommended against designating the proposed class of "audiovisual works released on DVD, where circumvention is undertaken solely for the purpose of extracting clips for inclusion in noncommercial videos that do not infringe copyright,"[33] the courts would not have been effectively prevented from determining whether the extraction of film clips for inclusion in noncommercial videos constitute fair use. It is not, as a general rule, necessary to circumvent access controls on DVDs in order to make copies of film clips for inclusion in noncommercial videos, although it has been asserted and the Register has acknowledged that in *some* cases it is preferable, and perhaps even necessary, to circumvent in order effectively to make one's point.[34] A person wishing to adjudicate whether inclusion of film clips in noncommercial videos can be a fair use may do so by using one of the other means discussed below without circumventing any access controls.

---

[31] The meaning of "likely" was addressed in the first Section 1201 rulemaking. "'Likely'—the term used in section 1201 to describe the showing of future harm that must be made— means 'probable,' 'in all probability,' or 'having a better chance of existing or occurring than not.' Black's Law Dictionary 638 (Abridged 6th ed. 1991)." *See* 65 Fed. Reg. at 64,562.

[32] *See* Recommendation of the Register of Copyrights in RM 2002-4E, Rulemaking on Exemptions from Prohibition on Circumvention of Copyright Protection Systems for Access Control, Oct. 31, 2003, at 25 (hereinafter "2003 Recommendation of the Register of Copyrights").

[33] The Register is not recommending designation of that precise class, but is recommending designation of a similar class. *See* discussion *infra* at p. 22

[34] *See* discussion *infra* at p. 59, regarding the DVDs and alternatives to circumvention.

The Register also declines to create a *per se* rule in an evidentiary vacuum. Proposals to designate classes of works in this proceeding are evaluated on the totality of the evidence, including market alternatives to circumvention that enable noninfringing uses. Thus, a proponent must demonstrate, in addition to noninfringing nature of the underlying use, that the prohibition is adversely affecting the use of works in a particular class of works. In some cases, this may be demonstrated by showing that the work is only available in copies protected by access controls. In other cases, a proponent may prove that the protected copy is needed to achieve the intended use. In all cases, the proponent must be able to demonstrate that circumvention of access controls is necessary in order to engage in the desired noninfringing use.

Another threshold consideration is whether the prohibition is causally related to the adverse effect on noninfringing uses. In order for the prohibition to apply to a work, the technological protection measure must control *access* to a copyrighted work. A factual record that establishes how a technological protection measure controls access to a work is essential to the analysis.[35]

If these threshold showings are met, the Register will continue the analysis in relation to the statutory factors that the Librarian must consider before designating a class of works. The Register will, when appropriate, assess the alternatives that exist to accomplish the noninfringing use; such evidence is relevant to the inquiry regarding whether the prohibition is adversely affecting the noninfringing use of the class of works. This assessment also includes consideration of any other statutory exemptions to the prohibition that may be applicable to the use. If a statutory exemption applies, there may be no need for the Librarian to designate a class. On the other hand, if Congress has enacted a statutory exemption for certain types of activity that includes requirements that proponents of a class cannot meet, that may be evidence of legislative intent not to permit circumvention when those requirements have not been met.

At this stage of the analysis, a balancing of the interests of users and copyright owners is critical. If an exemption is warranted by the evidentiary record, the proper tailoring of the scope of the class is also an important consideration.

However, if a proponent of a class does not make a threshold showing in the record,

---

[35] The proponent of a class of works does not necessarily have to provide a technical analysis of how the access control operates, but she must provide sufficient information to enable the decisionmaker to understand how, as a practical matter (*e.g.*, from the point of view of the user of the copy of the work), access is controlled.

mainly that the use is noninfringing or that the prohibition is causing the effect on noninfringing uses, the evaluation of the statutory factors will not be warranted. Only when a proponent demonstrates a *prima facie* case for designating a class will the Register engage in the further balancing of the respective interests called for in the statutory factors.

In each rulemaking proceeding, proposed classes are reviewed *de novo*. The fact that a class was previously designated by the Librarian creates no presumption that redesignation is appropriate, but rather the proponent of such a class must make a prima facie case in each three-year period.[36] However, when a class has been designated for the preceding three-year period, evidence relating to the costs or benefits ensuing from that designation are generally relevant to the assessment of whether the existing class (or some variation thereof) should be redesignated.

3. *Determination of "Class of Works"*

A major focus of the first rulemaking proceeding was how a "class" of works is to be defined. The Register determined that the statutory language requires that the Librarian identify a "class of works" based upon attributes of the works themselves, and not by reference to some external criteria such as the intended use or users of the works. The Register also found that the legislative history appears to leave no other alternative than to interpret the statute as requiring a "class" to be defined primarily, if not exclusively, by reference to attributes of the works themselves. The Commerce Committee Report addressed the issue of determining a class of works:

> The issue of defining the scope or boundaries of a "particular class" of copyrighted works as to which the implementation of technological protection measures has been shown to have had an adverse impact is an important one to be determined during the rulemaking proceedings. In assessing whether users of copyrighted works have been, or are likely to be adversely affected, the Secretary shall assess users' ability to make lawful uses of works "within each particular class of copyrighted works specified in the rulemaking." The Committee intends that the "particular class of copyrighted works" be a narrow and focused subset of the broad categories of works of authorship than [sic] is identified in section

[36] 2000 Recommendation of the Register of Copyrights, 65 Fed. Reg. at 64,563.

102 of the Copyright Act (17 U.S.C. § 102).[37]

Because the term "category" of works has a well-understood meaning in the copyright law, referring to the categories set forth in Section 102, the Register concluded that the starting point for any definition of a "particular class" of works in this rulemaking must be one of the section 102 categories. The illustrative list of categories appearing in Section 102 of Title 17 is only a starting point for this decision and a "class" will generally constitute some subset of a Section 102 category. Crafting the appropriate scope of a "class" is one of the major functions of the rulemaking proceeding. The scope of any class will necessarily be determined by the evidence of the present or likely adverse effects on noninfringing uses. The determination of the appropriate scope of a "class of works" recommended for exemption will also take into account the adverse effects that designation of the class may have on the market for, or value of, copyrighted works. While starting with a Section 102 category of works, or a subcategory thereof, the description of a "particular class" of works ordinarily should be further refined by reference to other factors that assist in ensuring that the scope of the class addresses the scope of the harm to noninfringing uses. For example, the class might be defined in part by reference to the medium on which the works are distributed, or even to the access control measures applied to them. But tailoring a class solely by reference to the medium on which the work appears, or the access control measures applied to the work, would be beyond the scope of what a "particular class of work" is intended to be.[38]

In previous rulemakings, the Register also rejected proposals to classify works by reference to the type of user or use (*e.g.*, libraries, or scholarly research).[39] This conclusion was consistent with the records in those rulemakings. However, in the 2006 proceeding the Register concluded, based upon the record before her, that in appropriate circumstances a "class of works" that is defined initially by reference to a Section 102 category of works or a subcategory thereof, may additionally be refined not only by reference to the medium on which the works are distributed or the access control measures applied to them, but also by reference to the particular type of use and/or user to which the exemption shall be applicable. Tailoring a class solely by reference to the use and/or user would be beyond the scope of what "particular class of work" is

---

[37] Commerce Comm. Report at 38.

[38] *See* 2003 Recommendation of the Register of Copyrights at 11-13.

[39] *See id.*

intended to be.[40] As the Register stated in 2000, a class of works must always begin with a category (or categories) of works, or some subset thereof, and may then be refined by other factors, such as the medium, the technological protection measure, the use, and/or the user. These examples of the ways in which a class can be refined are illustrative and are representative of the types of refinements that the Register has recommended in the past. The only general requirement applicable to any class is that it begin with some subset of a category or categories of works. In some factual situations, that subset classification may be the ending point for a class. However, the records in this and prior rulemaking proceedings have demonstrated that in many cases, such a subset of a category of works should be further tailored in accordance with the evidence in the record. Beyond the requirement for a starting point, the Register finds no basis in the statute or the legislative history to delineate the contours of a "class of works" in a factual vacuum.[41] The contours of a "class" will depend on the unique factual circumstances established in the

---

[40] *See* 2003 Recommendation of the Register of Copyrights at 84 ("Another group of proposals defined the class of works primarily by reference to the type of use of works or the nature of the users, *e.g.*, fair use works. A 'use-based' or 'user-based' classification was rejected by the Register in the last rulemaking, because the statutory language and the legislative history did not provide support for classification on this basis. Defining a class in such a manner would make it applicable to all works and would not provide any distinctions between varying types of works or the measures protecting them. If an exemption encompassing all works is to be granted, it is more appropriately a matter for Congressional action.") (Footnote omitted.)

[41] In a letter to the Librarian of Congress and the Register of Copyrights made part of the *ex parte* file in this proceeding, and appended to the Post-Hearing Response of the Motion Picture Association of America to Copyright Office Questions relating to DVDs of August 21, 2009, at pp. 8-13, there was an objection to the Copyright Office's Notice of Inquiry in this proceeding. Among other things, five organizations representing copyright owners alleged that they were precluded from presenting arguments on the proper scope of a class of works at the initial written comment phase of the proceeding. In the Register's view, the purpose of the initial comment phase is to provide the opportunity to propose classes of works for consideration in the rulemaking. If no proposals are forthcoming in a particular three-year period, this initial comment period would be an indication that the market for access-protected digital works is functioning in a satisfactory manner and that no further information is required for the Register's recommendation. Opening the initial comment period to all legal arguments would not only fragment and dilute the process, but also foster an unproductive hypothetical legal debate in a factual vacuum. The goal of the rulemaking is to solicit information on adverse effects on noninfringing uses that are caused by the prohibition on circumvention and to recommend classes of works to effectuate an appropriate remedy during the ensuing three-year period for any adverse effects demonstrated in the record. The starting point for determining the proper scope of a class is to examine the case made by proponents of a class. Once the proponents have made their case, opponents are invited to express their views, presenting facts and offering legal arguments to the Register. If opponents believe the proposed class is too broad in scope, they may (among other things) challenge the breadth of the proposed class and offer their arguments as to the proper scope of a class. Deferring such submissions until after the initial proposals have been made helps ensure that all arguments as to scope are grounded in a factual record and, in any event, is a reasonable procedural measure that provides for an orderly and, it is hoped, focused presentation of the cases for and against the designation of the proposed classes. As the initial Notice of Inquiry in this proceeding clearly stated, the Register will entertain all arguments and facts related to the proper tailoring of a class. *See* Notice of Inquiry, *Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies*, 73 Fed. Reg. 58,073, 58,076 (Oct. 6, 2008) (Hereinafter "Notice of Inquiry" or "NOI").

rulemaking record on a case-by-case basis.[42] Moreover, those factual circumstances must be considered in the context of the market for copyrighted works in any given three-year period.[43] Aside from designating a starting point for a "class of works," Congress's only real guidance as to the scope of any particular class is that such a class should neither be too broad nor too narrow.[44] In determining the proper contours of a class in any particular case, the Register will look to the factual record to assess the proper scope of a class for the ensuing three-year period.

D. Consultation with the Assistant Secretary for Communications and Information

Section 1201(a)(1)(C) requires the Register of Copyrights to consult with the Assistant Secretary for Communications and Information of the Department of Commerce and report and comment on the Assistant Secretary's views when she makes her recommendation to the Librarian of Congress.

The Register of Copyrights's staff has been in frequent communication with the staff of the National Telecommunications and Information Administration ("NTIA") during the rulemaking process. The new Assistant Secretary at the Department of Commerce, who is also the Administrator of the National Telecommunications and Information Administration, was appointed by the President after the rulemaking process had begun. Prior to the Assistant Secretary's appointment and confirmation, NTIA staff was briefed on the rulemaking process established by the Register, informed of developments, in attendance at many of the hearings, and invited to provide input in the course of this rulemaking proceeding. The Copyright Office General Counsel and an Assistant General Counsel met with the Assistant Secretary and his staff to discuss the rulemaking proceeding, the record in this rulemaking, and the preliminary views of NTIA.

The Assistant Secretary formally communicated his views in a letter to the Register on

---

[42] Commerce Comm. Report at 38; ("The issue of defining the scope or boundaries of a 'particular class' of copyrighted works as to which the implementation of technological protection measures has been shown to have had an adverse impact is an important one to be determined during the rulemaking proceedings.")

[43] *Id.* at 36 ("This mechanism would monitor developments in the marketplace for copyrighted materials, and 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.")

[44] House Manager's Report at 7.

November 4, 2009,[45] supplemented by another letter on April 16, 2010.[46] NTIA's views were considered by the Register in forming her recommendation. A discussion of NTIA's substantive analysis of particular proposals is presented in the relevant sections of this recommendation.

The Assistant Secretary also offered some views on the considerations applicable to the rulemaking process itself, including the scope of a "class of works" and the evaluation of "likely" adverse effects.

With respect to the determination of a "class of works," NTIA supported the decision of the Register to tailor a class to the attributes of the use or the user in appropriate circumstances. The Assistant Secretary stated that tailoring a class in such a manner facilitates addressing the demonstrated harm while at the same time limiting the adverse consequences that may result from the designation of the class.[47] NTIA believes that this approach strikes the appropriate balance by permitting the exemption of a class for affected uses or users without unnecessarily exempting a broad class to accommodate a subset of users or uses.

With respect to the "likely" adverse effects, NTIA noted that while mere speculation cannot support a claim of likely adverse effect, both present and future harms must be considered. NTIA states that mere speculation is insufficient to demonstrate likely harm, but believes that likely adverse effects on noninfringing uses may be satisfied by demonstrating that harm is likely to occur for particular individuals or for the public as a whole. In any case, NTIA believes that an class of works must be specifically tailored to meet the need or mitigate against the adverse impact.[48] NTIA also stresses that it is important to consider the alternative means of accomplishing a noninfringing use that do not require circumvention. Because rights holders could be harmed by an exemption, NTIA hopes that market forces will compel private solutions

---

[45] Letter from Lawrence E. Strickling to Marybeth Peters, Nov. 4, 2009 (hereinafter "NTIA Letter"). The letter is available at the Copyright Office website, http://www.copyright.gov/1201/.

[46] This letter was solely on the subject of mobile phone unlocking. The contents of this letter are fully discussed, *infra*, in the mobile phone unlocking section. This letter is also available at the Copyright Office website, http://www.copyright.gov/1201/.

[47] NTIA Letter, at 2.

[48] *Id.* at 2-3.

that will benefit both rights holders and consumers.[49]

II. SOLICITATION OF PUBLIC COMMENTS AND HEARINGS

On October 6, 2008, the Register initiated this rulemaking proceeding pursuant to Section 1201(a)(1)(C) with publication of a Notice of Inquiry.[50] The NOI requested written comments from all interested parties, including representatives of copyright owners, educational institutions, libraries and archives, scholars, researchers, and members of the public. The NOI devoted a great deal of attention to setting out the legislative parameters and the scope of the rulemaking based on the determinations made in the first rulemaking. It also summarized the scope of the term "class of works" as it has been refined over the course of the three prior rulemakings.[51] As in past Section 1201 rulemaking proceedings, the NOI stated a preference for submission of comments via electronic filing, and the Copyright Office activated a web-based form to facilitate comment submission and subsequent posting of comments to the Copyright Office's website.[52]

During the initial comment period that ended on December 2, 2008, the Copyright Office received nineteen written comments proposing twenty-five classes of works, all of which were posted on the Office's website.[53] Parties submitting comments during this period were asked to specify a class or classes of works adversely affected by the prohibition on circumvention of access controls; to summarize their argument in favor of designating the class of works; and to provide any facts, evidence, and legal arguments supporting the designation. Because some of the initial comments contained similar or overlapping proposals, the Copyright Office arranged related classes into groups, and set forth and summarized all proposed classes in a Notice of Proposed Rulemaking published on December 29, 2008.[54] This NPRM did not present the initial classes in the form of a proposed rule, but merely as "a starting point for further consideration."[55]

---

[49] *Id.* at 3.

[50] *See* Notice of Inquiry, 73 Fed. Reg. 58,073.

[51] *Id.* at 58,076-77.

[52] *Id.* at 58,078.

[53] *See* Section 1201 Comments at http://www.copyright.gov/1201/2008/index.html. (Last visited 4/30/10.)

[54] Notice of Proposed Rulemaking, *Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies*, 73 Fed. Reg. 79,425 (Dec. 29, 2008) (Hereinafter "NPRM").

[55] *Id.* at 79,427.

The NPRM asked interested parties to submit comments providing support, opposition, clarification, or correction regarding the proposed classes of works, and to provide factual and/or legal arguments in support of their positions. The Copyright Office received a total of fifty-six responsive comments before the comment period closed on February 2, 2009, all of which were posted on the Copyright Office website.[56]

On March 9, 2009, the Register published a Notice that public hearings would be conducted at Stanford University in Palo Alto, California and at the Library of Congress in Washington, DC in May 2009. Persons wishing to testify were asked to submit their requests to testify by April 3, 2009.[57] The Register conducted public hearings on four separate days: at Stanford University on May 1, 2009, and at the Library of Congress on May 6, 7, and 8, 2009. Thirty-seven witnesses, representing proponents and opponents of proposed classes of works, testified on twenty-one proposed classes. Written transcripts of the hearings were posted on the Copyright Office website, along with audio recordings of most of the hearing sessions.[58]

Following the hearings, the Copyright Office sent questions pertaining to certain issues to all of the witnesses who had testified regarding those issues. The purposes of these written inquiries were to: (1) clarify for the record certain statements made during the hearings; (2) elicit responses to questions raised by hearing testimony; (3) gather information on the operation of specific technologies, and (4) foster reactions to potential alternatives to specific proposed classes of works. The post-hearing questions from the Copyright Office and the responses from the

---

[56] Section 1201 Comments at http://www.copyright.gov/1201/2008/responses/index.html. (Last visited 4/30/10.)

[57] Notice of Public Hearings, 74 Fed. Reg. 10,096 (Mar. 9, 2009).

[58] Section 1201 Rulemaking Hearings at http://www.copyright.gov/1201/hearings/2009/transcripts/index.html. (Last visited 4/30/10.)

In referring to the comments and hearing materials, the following abbreviations and conventions are used herein: C-Initial Comment, *i.e.,* a comment proposing a class of works; R - Reply to Comment, and T-Transcript. Comment numbers correspond to the number in the indices of comments found at http://www.copyright.gov/1201/2008/index.html (Last visited 4/30/10.) and http://www.copyright.gov/1201/2008/responses/index.html. (Last visited 4/30/10.) References to the transcripts include the name of the witness, the date of the testimony, and the pages of the transcript. Hence, a reference to "C6 (Montoro) at 1" is a reference to the initial comment of Joseph Montoro at page 1. A reference to "T Metalitz, 5/8/09, at 55-56" is a reference to the transcript of the testimony of Steven Metalitz on May 8, 2009, at pages 55-56.

witnesses have been posted on the Copyright Office website.[59]

Following the posting of the responses to Copyright Office questions, Virgin Mobile petitioned the Register to consider additional evidence responsive to allegations contained in the response of the Electronic Frontier Foundation (EFF). The Register granted Virgin Mobile's request and provided the Electronic Frontier Foundation with an opportunity to respond to Virgin Mobile's submission. Both parties agreed that the evidentiary dispute did not affect the interests of any other proponents or opponents, and an assessment of the filings supported this assertion. These filings have also been posted on the Copyright Office's website.[60]

On October 27, 2009, the Librarian of Congress published in the Federal Register a Notice of an interim rule, extending the existing classes of works exempted from the prohibition until the conclusion of the current rulemaking proceeding and the designation of any classes of works to be exempt from the prohibition for the ensuing three-year period by the Librarian of Congress.[61]

III. THE DESIGNATED CLASSES

A. Motion pictures on DVDs that are lawfully made and acquired and that are protected by the Content Scrambling System when circumvention is accomplished solely in order to accomplish the incorporation of short portions of motion pictures into new works for the purpose of criticism or comment, and where the person engaging in circumvention believes and has reasonable grounds for believing that circumvention is necessary to fulfill the purpose of the use in the following instances:

- **Educational uses by college and university professors and by college**

---

[59] U.S. Copyright Office, Copyright Office Questions and Responses at http://www.copyright.gov/1201/2008/questions/index.html. (Last visited 4/30/10.) References to post-hearing comments include the name of the person or organization submitting the comment, the topic of the comment and the date the comment was submitted. Hence, a reference to Response of Decherney to Copyright Office Questions Relating to DVDs of May 9, 2009, at 1-2 is a reference to pages 1-2 of the response submitted by Decherney on May 9, 2009, to post-hearing questions from the Copyright Office.

[60] *See* Petition by Virgin Mobile and Response by the Electronic Frontier Foundation at http://www.copyright.gov/1201/2008/answers/8_28_reponses/virgin-mobile.pdf (Last visited 4/30/10.) and http://www.copyright.gov/1201/2008/answers/9_21_responses/eff.pdf. (Last visited 4/30/10.)

[61] *See* Federal Register Notice of Interim Rule, 74 Fed. Reg. 55,138 (Oct. 27, 2009) at http://www.copyright.gov/fedreg/2009/74fr55138.pdf. (Last visited 4/30/10.)

and university film and media studies students;

- **Documentary filmmaking;**
- **Noncommercial videos**

Background. Eight proposals were submitted requesting the designation of classes of works in order to allow the circumvention of audiovisual works for educational purposes by both educators and students. These proposals follow on the heels of the Register's 2006 designation of a class of "[a]udiovisual works included in the educational library of a college or university's film or media studies department, when circumvention is accomplished for the purpose of making compilations of portions of those works for educational use in the classroom by media studies or film professors."

Two additional proposals were submitted to designate classes of works relating to CSS-protected DVDs.[62] One proposal sought designation of a class to allow qualified documentary filmmakers to circumvent the CSS encryption on DVDs when the motion pictures are not commercially available in unprotected DVD format, and when substantial production has commenced on the documentary film.[63] Another proposal related to noncommercial, transformative use of motion pictures on CSS-protected DVDs for the creation of noncommercial videos.[64] Because of the similar factual and legal issues raised by these proposals, the Register has considered them together. The proposed classes were:

4A. Commercially produced DVDs used in face–to–face classroom teaching by college and university faculty, regardless of discipline or subject taught, as well as by teachers in K–12 classrooms.

4B. Audiovisual works used by instructors at accredited colleges or universities to create compilations of short portions of motion pictures for use in the course of face–to–face teaching activities.

4C. Audiovisual works that illustrate and/or relate to contemporary social issues used for the

[62] CSS is an acronym for "Content Scrambling System." CSS is an encryption-based system that employs an algorithm to encrypt the contents of a DVD. *See, infra*, for more information on this type of TPM.

[63] C11B (Kartemquin Educational Films, Inc. and International Documentary Association) (hereinafter "Kartemquin").

[64] C11A (EFF).

purpose of teaching the process of accessing, analyzing, evaluating, and communicating messages in different forms of media.

4D. Audiovisual works that illustrate and/or relate to contemporary social issues used for the purpose of studying the process of accessing, analyzing, evaluating and communicating messages in different forms of media, and that are of particular relevance to a specific educational assignment, when such uses are made with the prior approval of the instructor.

4E. Audiovisual works contained in a college or university library, when circumvention is accomplished for the purpose of making compilations of portions of those works for educational use in the classroom by media studies or film professors.

4F. Audiovisual works contained in a college or university library, when circumvention is accomplished for the purpose of making compilations of portions of those works for coursework by media studies or film students.

4G. Audiovisual works included in a library of a college or university, when circumvention is accomplished for the purpose of making compilations of portions of those works for educational use in the classroom by professors.

4H. All audiovisual works and sound recordings 'used in face–to–face classroom teaching by college and university faculty, regardless of discipline or subject taught' and regardless of the source of the legally acquired item.

11A. Audiovisual works released on DVD, where circumvention is undertaken solely for the purpose of extracting clips for inclusion in noncommercial videos that do not infringe copyright.

11B. Motion pictures and other audiovisual works in the form of Digital Versatile Discs (DVDs) that are not generally available commercially to the public in a DVD form not protected by Content Scramble System technology when a documentary filmmaker, who is a member of an organization of filmmakers, or is enrolled in a film program or film production course at a post-secondary educational institution, is accessing material for use in a specific documentary film for which substantial production has commenced, where the material is in the public domain or will be used in compliance with the doctrine of fair use as defined by federal case law and 17 U.S.C. § 107.

1. *Proposed Classes for Educational Purposes*

Overview and Comments. In the 2006 proceeding, three professors of film and media studies from the University of Pennsylvania's Cinema Studies Program and Annenberg School for Communication asserted that:

> in order to teach their classes effectively, they need to be able to create compilations of portions of motion pictures distributed on DVDs protected by CSS for purposes of classroom performance. They also asserted that in order to show pedagogically necessary, high quality content in a reasonably efficient manner, they must circumvent CSS in order to extract the portions of motion pictures or audiovisual works necessary for their pedagogical purposes.[65]

The Register found that the proponents convincingly demonstrated that the use alleged to be adversely affected was indeed noninfringing. Performing or displaying portions or individual images from motion pictures "in the course of face-to-face teaching activities of a nonprofit educational institution, in a classroom or similar place devoted to instruction" is noninfringing under Section 110(1) of the Copyright Act.[66] Furthermore, the Register determined that the reproduction of such portions or images into compilations was in many cases a fair use of the motion pictures under Section 107 of the Copyright Act.[67]

In addition, the Register undertook an extensive inquiry into the text and legislative history of the statutory category "class of works" and determined that, while a class must be initially based upon the inherent qualities of the works themselves, and may also be refined by reference to the access controls applied to the works and/or the formats in which the works are distributed (the approach taken in 2000 and 2003), it may also be, in certain cases, appropriate to further tailor a class based upon the use that is being adversely affected by the prohibition on circumvention and/or upon the user who finds his or her noninfringing use adversely affected.[68]

---

[65] *See* Recommendation of the Register of Copyrights in RM 2005-11, Rulemaking on Exemptions from Prohibition on Circumvention of Copyright Protection Systems for Access Control, Nov. 17, 2006, http://www.copyright.gov/1201/docs/1201_recommendation.pdf, at 13 (hereinafter "2006 Recommendation of the Register of Copyrights").

[66] *Id.* at 13-14.

[67] *Id.*

[68] *See id.* at 18-19 ("The tailoring of a 'class' is supposed to be remedial for those users who are adversely affected by the prohibition. Unless a 'class' may describe those uses or users, the regulatory language will not always clearly identify the intended recipients of the remedial exemption. While it is certainly possible, as our past rulemakings have demonstrated, to craft a properly tailored exemption without reference to a particular use or users, in other cases, such as the one here at issue, failing to specify the use or users for whom the exemption was found to be warranted would result in an unnecessarily broad exemption. Further, if a class is too broad, it will often entail undesirable consequences. If those consequences are such that they would lead to undue harm to copyright owners, it may be difficult to justify the exemption at all. Were that the result, the rulemaking proceeding would not be operating as the fail-safe mechanism that Congress intended it to be. Therefore, depending upon the circumstances, it can be appropriate to refine a class by reference to the use or user in order to remedy the adverse effect of the

Because the proposal was narrowly tailored with regard to a discrete set of users who had demonstrated a sufficient need to circumvent DVD access controls for limited noninfringing purposes that are entitled to special consideration under Section 1201(a)(1)(C), and because such tailoring greatly reduced the risk that the circumvention would be for improper purposes or would lead to large-scale circulation of unprotected, digital motion pictures, potentially deterring further rights-holder investment in DVD creation or distribution, the Register found that the circumvention of CSS on DVDs for the purpose of classroom instruction was proper. In addition, the record in the rulemaking demonstrated that the pedagogical needs of film and media studies professors could not be met by analog VHS tapes or by recording the works from the television screen with a video camera because (1) the nature of the courses required high-quality images and sound and (2) DVDs frequently contain extra features not found on VHS tapes. As the Register stated,

> [F]or older works, the DVD version of a motion picture can preserve the color balance and aspect ratio to accurately reflect how the original work would have appeared when it was originally released in theaters. The record does not reveal sufficient viable alternatives to the DVD version of the motion pictures for this purpose. For instance, VHS versions of the films altered the color balance and aspect ratio. Similarly, the demonstration at the hearing of screen shots with a digital video recorder revealed dramatic color distortions and greatly reduced picture quality. While these options may have satisfied the needs of many types of noninfringing users and even many noninfringing educational uses – *e.g.*, those wanting to comment on the historical context of a film or create a parody, or to show a film clip in a class unrelated to cinematographic significance[61] – the reduced quality of alternative formats was wholly insufficient for the pedagogical purposes for which the clips were sought in film and media studies classes.[69]

The Register also relied on evidence that demonstrated the need for film and media studies professors to circumvent CSS in order to extract DVD clips for compilations to be shown in the classroom, as opposed to inserting single DVDs in succession, a practice that would force the students to sit through introductory screens that CSS prevents users from skipping. "[F]or the film and media professors' intended use," wrote the Register in 2006, "these screens waste valuable class time. The larger the number of DVDs that need to be shown, the greater the amount of class time spent watching material that serves no pedagogical purpose."[70] The record revealed that if a

prohibition and to limit the adverse consequences of an exemption.").

[69] *Id.* at 20.

[70] *Id.* at 23.

film professor wanted to show ten 30-second clips in a class session of 50 minutes, the amount of time spent shuffling DVDs into and out of the DVD player would represent "[t]en percent of educational classroom time [which] is a significant social expenditure, particularly when classroom time is a limited and precious resource."[71]

The eight proposals the Copyright Office received in 2009 for classes of audiovisual works for educational uses all seek to build upon the 2006 film and media studies class to apply to broader categories of users and uses. For ease of reference the Copyright Office identified these proposals as numbers 4A through 4H.

Proposal 4E was, with one change, a duplication of the 2006 film and media studies class of works, and was proposed by the same three University of Pennsylvania professors, joined in this rulemaking by the International Communication Association and the Society for Cinema and Media Studies.[72] The difference in the 2009 proposal was an expansion from audiovisual works contained in "the educational library of a college or university's film or media studies department" to those contained in "a college or university library." Proponents of the class asserted that limiting the source of audiovisual works to those in the collections of specialized libraries would unduly restrict the range of titles available for pedagogical use, without any corresponding benefit to rights-holders.[73] If a college or university has already purchased a work for its main (or sole) library, then professors already enjoy legal access to that work, the proponents pointed out, and forcing a school to purchase a separate copy for a specialized library is a waste of scarce resources.[74] In addition, noted the proponents, many schools lack dedicated and separate film and/or media studies libraries altogether.[75]

In support of designating the existing classes again for the ensuing three year period, the proponents presented evidence that the designation of the existing class of works has been a great boon to film and media professors during its three year term,[76] as well as evidence that the same

---

[71] *Id.* at 21, 24.

[72] C4E & 4F (Decherney) at 1.

[73] *Id.* at 15.

[74] *Id.* at 14.

[75] *Id.* at 14-15.

[76] *Id.* at 2-3.

circumstances that prompted its approval in 2006 are still present in 2009, and are likely to remain in effect for the next three years. The need for film and media studies professors to create high-quality clip compilations has not changed since 2006, and the proponents argued that circumvention of access-protected audiovisual works is the only way in which to obtain copies of the desired content with sufficient quality. Many audiovisual works, they asserted, are only available on DVDs, and the extra features on DVDs remain unavailable on any other medium.[77] For those works available on alternative media, such as VHS or YouTube, the quality is inadequate for the intended purpose.[78]

At the hearings in Palo Alto and Washington, representatives of copyright owners argued that the proposed classes relating to DVDs should not be designated if alternative means of engaging in the noninfringing uses are available. Much of the discussion at the Washington hearings focused on two means of copying film clips from DVDs that do not appear to involve circumvention of CSS: the capturing of audiovisual content either (1) by camcording or (2) by using video capture software. Both of these methods involve reproducing the content of a DVD after it has been legitimately decrypted, and thus without circumvention. Camcording involves pointing a digital video camera at a television screen showing a performance of the desired work. The resulting copy can be uploaded to a computer where, free of access or copy controls, it can be edited as needed.[79] At the hearings in Washington, the MPAA demonstrated the quality of video that could be obtained by filming a flat screen television, and showed a video of how it prepared its demonstrative evidence.

The second method—using video capture software—is roughly analogous to camcording in that it reproduces the information stored on a DVD as it is being shown on a screen, and does not access digital content on the disc itself. Video capture software, however, uses software to copy the information, so the reproduction occurs entirely inside the computer. Different video capture programs capture digital signals in different ways, but the fundamental process is that the computer's licensed DVD player decrypts the content, which is sent to the computer's video card and software driver, and from there is sent to the screen. The video capture software copies the content as it is being rendered in unencrypted format to the screen.

---

[77] *Id.* at 10-12.

[78] *Id.* at 5-7; 12.

[79] *See* Ts Attaway & Seymour, 5/6/09, at 207-10 (MPAA demonstration of how to make a camcorded screen shot and what the resulting copy looks like.)

Proponents of class 4E and of the other Category 4 classes considered these two alternative methods of making film clips to be unacceptable due to poor image and sound quality. While proponents of class 4E noted that the quality of the camcording output as shown by the MPAA had improved since 2006, they also stated that it remained inadequate for film and media studies classroom use:

> [T]hey were using a telephoto lens, and there was noticeable distortion . . . there was discoloration; there was a reddish cast to the images; they were still a little muddy and blurred, and you can see bleed-through in the lines . . . especially because they were showing dark scenes, there is actually a lot of detail that . . . apparently wasn't captured by the camcorder.[80]

At the hearings in Palo Alto, CA and in Washington, DC, the Copyright Office demonstrated the results of the use of video capture software and asked a number of questions of both proponents and opponents of the proposed classes of works.[81] The line of questions posed to the opponents of the proposed classes related to whether or not video capture software violated the prohibition on circumvention. At both hearings, opponents of the classes were unwilling to provide a definitive answer to this question. After the hearings, a series of questions were sent to all hearing participants involved in the DVD-related panels in order to clarify whether using video capture software violated the prohibition on circumvention in Section 1201(a)(1), and to clarify whether such software captures were, or could be, sufficient for various uses that were alleged to be adversely affected by the prohibition.[82] The general response was that a number of forms of video capture software do not circumvent any access controls and thus do not violate the prohibition.[83]

Despite the clarification of the legality of video capture software and the use of the

---

[80] T Decherney, 5/6/09, at 242.

[81] The particular software used in the demonstration was *Snagit*. T Kasunic, 5/1/09, at 57-59; T Kasunic, 5/6/09, at 244-45. For more information on *Snagit*, *see* http://www.techsmith.com/screen-capture.asp. (Last visited 4/30/10.)

[82] The questions posed and responses received are available in their entirety on the Copyright Office's website. *See* http://www.copyright.gov/1201/2008/questions/index.html. (Last visited 4/30/10.)

[83] The respondents qualified this legal analysis by noting that they did not examine every screen capture program available, and were limited to publicly available information regarding the programs they did examine.

software, the proponents of the classes stated that video capture software produced less-than-useful results:

> The frame rate is often reduced. Even when the frame rate is very high, the timing of the action can be distorted, creating staccato or jerky motion. More importantly, pieces of the video are simply missing. These "holes" in the video can be particularly noticeable when analyzing a work of animation or claymation, in which every frame has been composed individually by the filmmakers. It seems surprising that educators in any field would be asked to teach works with missing pieces.[84]

Proponents of the classes reiterated their view that no DVD player on the market gave professors the flexibility to create compilations of multiple film clips or spared them from wasting class time by switching among separate discs, noting that the available models only accepted one disc at a time.[85] They also asserted that licensing the use of clips from the rights-holders was an "invalid" alternative because it would retard the spontaneity needed for effective classroom discussions,[86] because it presented a risk that rights-holders might withhold permission for a use they did not approve of,[87] and because the licensing process was labyrinthine and too time-consuming.[88]

Finally, some proponents for redesignation of the film and media studies class made clear that it should not be restricted to CSS-protected DVDs, but also apply to Blu-ray discs, streaming digital media, and all forms of audiovisual content that require circumvention in order to make clip compilations.[89] The examples cited in favor of the proposed class, however, concerned only DVDs.

Copyright owners who commented on the proposed redesignation of the film and media

---

[84] Post-Hearing Response of Decherney to Copyright Office Questions Relating to Video Capture Software of July 9, 2009, at 1-2.

[85] C4E & 4F (Decherney) at 8.

[86] *Id.* at 9.

[87] *Id.*

[88] *See* T Decherney, 5/6/09, at 114.

[89] *See, e.g.*, C4E & 4F (Decherney), at 7, 10, 12; T Decherney, 5/6/09, at 115-116.

studies class did not, in principle, oppose redesignation of the class for another three years;[90] nor did they oppose the expansion to include audiovisual works contained in a college or university library.[91] However, several commenters representing, among others, motion picture studios, recommended that the class be explicitly narrowed in five respects: (1) to apply only to audiovisual works on CSS-protected DVDs; (2) to apply only when circumvention is "truly necessary," such as when the material is not reasonably available through a consensual path;[92] (3) to apply only when "all existing digital copies of a work contain access controls that prevent" the creation of clip compilations; (4) to clarify that it applies "solely" for the stated purpose; and (5) to clarify that the circumvention itself, as well as the classroom use, may only be undertaken by film and media studies professors.[93]

Proposals 4A through 4D and 4F through 4H sought the same fundamental outcome as 4E, circumvention of audiovisual works for educational purposes, but offered different classes of works. Because these proposals shared among themselves many of the same elements of a class of works, and many of the same rationales for defining a class of works by these elements, the following review is organized not by proposal, but by elements of the classes sought to be exempted.

a. Inherent attributes and media of the work

The proponents of the classes relating to educational uses of DVDs tended to define their classes initially in terms of "audiovisual works." However, their comments and testimony focused almost entirely on motion pictures[94] in the form of CSS-protected DVDs. The proponents marshaled substantial evidence of the pervasiveness and importance of audiovisual material in

---

[90] *See, e.g.,* R37 (DVD CCA) at 16; R45 (MPAA) at 10-11; R46 (Joint Creators) at 29; R48 (Time Warner) at 9.

[91] *See, e.g.,* R46 (Joint Creators), at 30, n.54.

[92] Several motion picture industry commenters described a film clip service being designed by the MPAA and the University of Southern California School of Cinematic Arts ("USC") that would provide film professors with free online access to full length films and short clips for educational use. It was proposed that, once this service is operative, the class of works should be limited to works not available through the service. *See, e.g.,* R45 (MPAA) at 10-11; R48 (Time Warner) at 9.

[93] *See* R46 (Joint Creators) at 29-30; R45 (MPAA) at 11.

[94] Under the copyright law "motion pictures" constitute a subset, but a very large subset, of the category of "audiovisual works." *See, infra,* for a fuller discussion.

contemporary education, and further argued that, given this state of affairs, such material should be of a high quality in terms of both image and sound.[95] The proponents asserted that only DVDs provide the necessary quality, and only DVDs are amenable to the kind of clip extraction and editing required for instructors to create compilations that allow the comparison and analysis of multiple audiovisual works without wasting class time.[96] Specifically, the proponents criticized camcording, Hulu, and YouTube as poor alternatives given, respectively, their expense and lower quality, inability to edit, and lack of selection.[97] The proponents also pointed out that DVDs are presently the default format for audiovisual works, having completely eclipsed VHS tapes, which no longer exist as a viable, unprotected, alternative.[98]

b. Source of the work

The current film and media studies class includes only DVDs "included in the educational library of a college or university's film or media studies department." Such restriction of the class to DVDs housed in a library or another specific location was omitted from some of the proposals for expanded classes of works for educational circumvention.[99] One proposal, however, suggested that the DVDs should be "legally acquired,"[100] and two others suggested the same standard as proposal 4E, location in a "college or university library."[101]

c. Use and user of the work

In order for a class of works to be designated in this rulemaking, it must be shown that the prohibition on circumvention adversely affects the noninfringing use of the work. Many of the

---

[95] *See, e.g.*, T Hobbs, 5/6/09, at 238-40 (on the need for clear image in order to do a "careful visual analysis" in *Media Literacy* classes); T Skalbeck, 5/6/09, at 166-7 (on the need for high quality images in copyright law classes); T Band, 5/6/09, at 123-24 (on the need for high quality image and sound quality in criminal justice classes); T Kaiser, 5/1/09, at 49 (on the need for high quality audio tracks in foreign language classes).

[96] *See, e.g.*, C4B (Smith) at 4; C4C & 4D (Hobbs) at 15-16; T Kaiser, 5/1/09, at 24-25.

[97] *See* T Handman, 5/1/09, at 18-19; T De Kosnik, 5/1/09, at 47; R32 (BYU) at 4.

[98] *See, e.g.*, C4C & 4D (Hobbs) at 14-15.

[99] *See* proposed classes of works, 4A, 4B, 4C, and 4D, filed in this proceeding.

[100] C4H (Fedak).

[101] C4E & 4F (Decherney); C4G (Libraries).

proposed classes of works are, and will continue to be, used for classroom instruction.[102] Such uses are, like the uses approved in the 2006 film and media studies class of works, noninfringing by virtue of the Section 110(1) face-to-face teaching exception (performance of works in the course of face-to-face teaching activities) as well as fair use under Section 107 (reproducing portions of motion pictures for inclusion in compilations for classroom performance).[103] In addition, two proposals concerned the use of protected DVDs by students in completing assigned projects and other coursework.[104] Proponents asserted that use of copyrighted DVDs by students in fulfilling course assignments is noninfringing on the same fair use grounds as the clip compilation activities covered by the 2006 film and media studies class of works.[105] Proponents also argued that the Section 110 exceptions apply to performances and displays by pupils as well as by instructors, provided that the performance or display constitutes a "teaching activity."[106]

Beyond the threshold question of whether Section 1201(a)(1)(A) negatively affects, or is likely to affect, the noninfringing use of a class of works, the nature of the use and user of protected works can be relevant to the construction of the exempted class itself. Proponents of the educational exemptions sought to refine their proposed classes by reference to expanded groups of uses and users beyond those included in the 2006 class of works. Regarding the nature of the use, they argued that all disciplines taught at all levels of education rely upon audiovisual works, and that the inability to circumvent DVDs in order to make classroom compilations adversely affects the pedagogical needs of instructors across the educational spectrum. As one commenter put it:

> Since most DVD's are encrypted medium, Section 1201 prevents instructors from compiling film clips for non-infringing teaching purposes. Thus, the demise of VHS dissolves the distinction between film and media studies and other specific subject areas because the pedagogical need for audiovisual works has become inseparably connected to and only satisfied through use of technologically

---

[102] *See* proposed classes of works, 4A, 4B, 4C, 4E, 4G, and 4H, filed in this proceeding.

[103] *See, e.g.*, C4C & 4D (Hobbs) at 9-14.

[104] *See* proposed classes of works, 4D and 4F, filed in this proceeding.

[105] *See* C4C & 4D (Hobbs) at 9-14 (using same fair use analysis for teacher and student use of DVD clips).

[106] *Id.* at 10.

protected DVDs.[107]

In particular, many proponents explained that film and media studies are not the only courses to rely upon audiovisual works as primary texts. Thus, they maintain, the need to closely examine the details and artistic choices of a film that were central to the Register's decision in 2006 are also present in Media Literacy, English, Foreign Language, and multidisciplinary courses.[108]

Regarding the need to create clip compilations of DVD content in non-film and media studies environments, proponents of the class made the point that the problem of serially showing multiple DVDs without the ability to skip the preliminary screens or pre-cue the desired scenes was a significant waste of class time regardless of the subject being taught.[109] It should also be noted, however, that some of the proponents cited examples that did not involve multiple works, but only involved performing a single portion of a work in a classroom.[110]

One particularly contentious expansion of the 2006 film and media studies class of works proposed in the current rulemaking was the inclusion of student uses within the exempted class of works. The proposals regarding circumvention for use in college and university film and media studies courses and in media literacy education courses at all educational levels urged that, in order to prepare and perform coursework assigned by the relevant instructor, students enrolled in these classes should be permitted to circumvent access controls on audiovisual works.[111] Examples presented of the kind of student work that is adversely affected by the current inability to legally circumvent audiovisual works included critical mash-ups, voiceover commentary, and video essays.[112] In one particularly vivid illustration, Professor Decherney of the University of Pennsylvania testified to the inadequacy of broadcast and YouTube clips as incorporated into a student work:

---

[107] R32 (BYU) at 4.

[108] *See, e.g.*, C4B (Smith) at 2; C4C & 4D (Hobbs) at 7; C4G (Libraries) at 10-11.

[109] *See, e.g.*, C4C & 4D (Hobbs) at 16.

[110] *See, e.g.*, C4G (Libraries) at 5-6; T Skalbeck, 5/6/09, at 162-63.

[111] *See* C4C & 4D (Hobbs) at 18; C4E & 4F (Decherney) at 16-18.

[112] *See* C4E & 4F (Decherney) at 16; T Decherney, 5/6/09, at 119.

> The power of blood spewing from a severed arm, and the impact of a gun being placed in a young boy's mouth were nullified by the muddy, pixilated images that they had to use. It was a clear case . . . in which high-quality digital clips were absolutely necessary.[113]

While conceding that the reproduction of portions of motion pictures by instructors and students may often fall within fair use and that the public performance of these portions for educational purposes in the classroom falls within the exemption in Section 110(1) of the Copyright Act,[114] opponents maintained that circumvention was not necessary to achieve the desired uses.

First, opponents challenged the assertion that non-film and media studies classes require DVD-level quality to meet their pedagogical goals.[115] Proceeding from this premise, they asserted that, despite the demise of an analog alternative in the form of VHS tapes, many other non-circumventing options remain, including YouTube, camcording, and requesting permission from rights-holders.[116] Opponents also noted that allowing such a broad exemption presents a risk of legitimizing illegal circumvention tools and services to such a degree that the entire CSS legal and technical regime would be undermined.[117]

Regarding some of the specific elements of the classes of works sought to be exempted, opponents asserted that only the creation and subsequent classroom performance of clip compilations fit within the Register's 2006 approach to defining a class of works. To omit the compilation element (as proposals 4A, 4C, 4D, and 4H do) would, in their view, "result in a "class of works" that is primarily based on a type of use or user rather than a category of works."[118] Furthermore, the opponents maintained that those proposals, such as 4B, that sought an class that covered K-12 instructors, failed to provide any examples where the circumvention ban has adversely affected

---

[113] T Decherney, 5/6/09, at 119.

[114] *See* T Metalitz, 5/6/09, at 196.

[115] *See, e.g.*, T Metalitz, 5/1/09, at 42-43.

[116] *See, e.g.*, R37 (DVD CCA) at 20; T Metalitz, 5/1/09, at 40-41.

[117] *See* R37 (DVD CCA) at 21.

[118] *See* R46 (Joint Creators) at 33.

noninfringing uses in that sector.[119]

In addition to opposing designation of a broad class of audiovisual works for educational uses, commenters from motion picture studios and other rights-holders strongly opposed extending any class to uses by students. Their primary concern was that such an extension would lead to widespread confusion over whether a particular use fell within the scope of the class and over the legality of circumvention in general.[120] The opponents also pointed out that while the limited category of beneficiaries of the class designated in 2006 were familiar with the DMCA and had incentives to act responsibly, those characteristics do not apply to the vast majority of students.[121]

2. *Proposed Class for Documentary Filmmakers*

Comments. Proponents of an class for the benefit of documentary filmmakers claimed that in the course of producing their films, documentary filmmakers often must make fair use of portions of creative works for criticism or analysis of the works themselves, or to make social commentary generally. They stated that the prohibition on circumvention is "crippling filmmakers' abilities to make fair use of works and to use public domain materials."[122] Proponents also stated that alternative formats are no longer available for the vast majority of motion pictures.[123]

In response, the Joint Creators and Copyright Owners[124] stated that the proponents had failed to identify a particular noninfringing use that is being adversely affected by the

---

[119] *See id*.

[120] *See, e.g.*, R37 (DVD CCA) at 22-23.

[121] *See* R45 (MPAA) at 11.

[122] *See* C11B (Kartemquin) at 1.

[123] *Id.* at 3, noting that in 2008, Amazon revealed that only seven titles were released in VHS format, and that in 2009, of the 1950 titles slated for release, only one was announced to be released in VHS format.

[124] The self-styled "Joint Creators and Copyright Owners" (referred to herein as "Joint Creators") are a coalition of copyright industry trade organizations – the Association of American Publishers ("AAP"), American Society of Media Photographers ("ASMP"), Alliance of Visual Artists ("AVA"), Business Software Alliance ("BSA"), the Directors Guild of America ("DGA"), the Entertainment Software Association ("ESA"), Motion Picture Association of America ("MPAA"), the Picture Archive Council of America ("PACA"), and Recording Industry Association of America ("RIAA").

prohibition.[125] The opponents also stated that to the extent that the case for designating the proposed class is aimed at public domain content, it is outside the scope of the rulemaking, because public domain material is not protected by the prohibition. The opponents also argued that the case-by-case nature of fair use precludes documentary filmmakers from asserting that the use of portions of motion pictures in documentary films is generally fair use. They argued that, at most, filmmakers can argue that some such uses will be considered fair. The opponents asserted that the uncertain nature of the noninfringing status precludes articulation of an appropriate class of work "for which circumvention would lead only to noninfringing conduct," or that would be characterized as "clearly" or "generally" noninfringing.[126] The Joint Creators also cited American University's Center for Social Media's analysis for the fact that few infringement cases have been brought against documentary filmmakers and that none of the plaintiffs have been motion picture studios or large archives.[127]

The proponents of the class for documentary filmmakers argued that alternative means of copying the content on CSS-protected DVDs are insufficient for documentary filmmakers' purposes because the three analog alternatives to circumvention result in, *inter alia*, degraded or severely degraded quality reproductions.[128] The degradation is noticeable on a small screen, but becomes pronounced when viewed on a large screen television or in a theater.[129] Additionally, proponents stated that because all DVDs incorporate Macrovision's Analog Copy Protection ("ACP") technology, the alternative analog transfer methods discussed by the proponents must be run through a visual stabilizer or a digital time base corrector in order to remove ACP from the signal sent by the DVD player. Proponents asserted that these devices are not readily available and all but one manufacturer has stopped producing them. Even when ACP can be avoided, the filmmaker will still encounter problems maintaining audio sync and frame rate between the DVD player and the recording device.[130]

The opponents of the proposed class argued that despite the proponents' discussion of

---

[125] R46 (Joint Creators) at 67.

[126] *Id.* at 68.

[127] *Id.* at n. 102.

[128] C11B (Kartemquin) at 6-7. The alternatives listed include: (1) "VHS capture"; (2) "scan conversion" or filming the screen; and (3) "analog transfer" which uses a VCR to capture the output of a DVD player.

[129] *Id.* at 7.

[130] *Id.*

three analog alternatives, the proponents "fail to discuss in much detail the most salient alternative method of making a noninfringing use of audiovisual material, which is to obtain footage directly from the copyright owners."[131] Opponents stated that filmmakers have failed to prove that they could not obtain the portions of motion pictures sought directly from copyright owners and thus have failed to make their case. Moreover, the opponents stated "that digital camcorders are increasingly capable of capturing very high quality images, particularly in the hands of skilled filmmakers."[132] The Joint Creators concluded by stating that although they do not believe that documentary filmmakers have made their case, in the event that the Librarian designates a class, it should be narrowly tailored. One suggestion for tailoring any class was to include a requirement of a good faith effort to obtain the unencrypted material from the copyright owner. The opponents also urged the Librarian to omit any reference in description of the class to fair use as the underlying basis of the noninfringing use. They stated that the use enabled by circumvention must be in fact noninfringing.[133]

3. *Proposed Class Relating to Noncommercial, Transformative Videos*

Comments. Another proposed class involving CSS-protected DVDs related to the ability to circumvent CSS in order to use portions of motion pictures in noncommercial videos that do not infringe copyright.[134] The creation of noncommercial videos that are, at least in some cases, transformative of prior works incorporated into the new work are sometimes referred to as "vids" by their creators (known as "vidders") and admirers.

As a general matter, vids involve the remixing and/or modification of a preexisting work or works in order to criticize or comment upon some aspect of the underlying works, such as a parody or a review, or to make a broader societal statement, perhaps in the form of a satire. While it is possible to criticize or comment upon the source works in textual form, vidders believe that the audiovisual medium provide a more appropriate form of commentary in which to express their point of view.[135] "Vids are commentaries; executed in a visual medium rather than in text, on the

---

[131] R46 (Joint Creators) at 69.

[132] *Id.* at 70.

[133] *Id.*

[134] C11A (EFF) at 18.

[135] *Id.* at 17.

original source material—sometimes celebrating or criticizing political, sexual, or cultural elements that were obvious in the original, sometimes uncovering meanings that were latent in the original; and sometimes creating entirely new meanings with the characters and plotlines of the original."[136]

It is difficult to generalize on the precise attributes of a "typical vid." The proponents proffer numerous examples for the record and cite research on a number of general categories of vids that involve some form of criticism or comment. One category consists of movie trailer remixes, which are original compilations of scenes, made for movie fans and often with a humorous purpose.[137] Another category involves film analysis in which amateur critics provide commentary over clips from the films being analyzed.[138] Vids of movie mistakes are also a distinct genre that comment on anachronisms, continuity errors and other "mistakes" found in films and television programs. Another genre is political commentary that uses clips from film or television to illustrate a particular political message. Other vids criticize the underlying themes or politics of a film or a group of films. Still another genre exists in which the vidder comments on the remix culture itself, mocking the sometimes low technical and aesthetic standards of remixes. Thus, while vids may use one work or a number of works, or may use one clip or many clips from a work, all of the vids within the scope of the proposal are distributed noncommercially for a new and different purpose from the original work or works. In essence, it was alleged that vids utilize preexisting motion pictures (and often sound recordings of musical works unrelated to the motion picture soundtrack) in order to comment upon the work or broader social themes—as a form of video quotation.

The proponents of this class argued that while not all noncommercial videos are noninfringing, some number of vids invariably qualify as noninfringing uses given the scope of

---

[136] *Id.*, quoting Professor Francesca Coppa.

[137] *See* C11A (EFF) at 15-16 for links to examples of each of these genres.

[138] There are also references to critics who provide commentary over the course of entire motion pictures, as opposed to commentary over portions of motion pictures. *See, e.g.*, Post-Hearing Response of EFF and Organization of Transformative Works ("OTW") to Copyright Office Questions relating to DVDs of August 21, 2009, at 4. It is highly questionable whether a commentary combined with an entire film would be considered a fair use. It is also clear that there are alternative means of achieving the same goal, as the EFF response itself noted in relation to Roger Ebert's article. *See id* at 3-4. *See also*, www.rifftrax.com (Last visited 4/30/10.), that offers mp3 discussions that can be synchronized with the playback of a motion picture on a DVD in order to hear simultaneous humorous commentary over the course of an entire film. However, given fair use precedent in the courts, the Register accepts that commentary merged with *a portion* of a DVD may qualify as a fair use in particular cases. *See, infra*.

vidding: "[s]ome remix videos doubtless infringe copyrights; others, thanks to the fair use doctrine, just as surely do not."[139] Conceding that not all vids are noninfringing, and generally applying a fair use analysis to the typical vid, the proponents asserted that "the general characteristics of these videos make it clear that many qualify as noninfringing fair uses under existing precedents."[140] The proponents also presented evidence from a study by Professor Michael Wesch concluding that, based on a random sample of 240 videos uploaded to YouTube, 7.5% of those videos were remixes of preexisting motion pictures taken from DVDs.[141] If this percentage is applied to the number of videos uploaded to YouTube each day, statistically, it translates into potentially 15,000 vids incorporating motion pictures on DVDs each day.[142] A subsequent sampling yielded a slightly reduced percentage, leading to the estimation that the actual daily average of vids uploaded to YouTube was between 2,000 and 6,000.[143] Moreover, the proponents argued that all of the fair use factors generally weigh in favor of fair use when applied to the typical vid.

A threshold question that requires evaluation is whether vidders are making or likely to make noninfringing uses of copyrighted works. The only exception to copyright owners' exclusive rights that would apply to this activity is fair use, and therefore, the mandatory four-factor analysis is required. Proponents of this class of works contended that the four statutory fair use factors support the assertion that the use of clips from motion pictures by vidders generally may be a fair use.

The proponents argued that under the first factor, the noncommercial nature of vids tends to support a finding of fair use.[144] This conclusion, they asserted, is bolstered by the fact that most vids are "by their nature, transformative, creating a new work that does not substitute for the

---

[139] C11A (EFF) at 13.

[140] *Id.* at 18.

[141] *Id.* at 29, Appendix A.

[142] *Id.*

[143] *Id.*

[144] Opponents of the proposed class claim that this noncommercial status is questionable given the indirect advertising revenue received from online video distributors. *See* R46 (Joint Creators) at 66. Opponents do not, however, show why a vidder stands in the shoes of the website rendering the works for purposes of the underlying fair use analysis.

original."[145] They supported this claim of transformativeness with the observation that vids "are frequently parodic, satiric, or created for purposes of commentary or criticism, precisely the kind of transformative uses that have been treated favorably by courts with respect to the first factor."[146] The proponents not only cited illustrations of potential noninfringing uses, but more broadly argued that these examples are part of larger genres and subgenres of vids.[147] Proponents also cited Professor Wesch's Digital Ethnography project which, as noted above, approximated that between 2,000 and 6,000 vids that include clips drawn from DVDs are uploaded to YouTube each day. These numbers were used to demonstrate the scope of the public's involvement in this new creative format. Rather than textually or verbally explaining the comment or criticism, the proponents stated that vidders often use audiovisual material to show, demonstrate, or illustrate their point, a "visual essay that stages an argument," often through the lens of music.[148] Particular music or lyrics will sometimes be chosen as a vehicle to comment upon or criticize portions of motion pictures.[149] For these reasons, the proponents argued that the first factor tends to weigh in favor of fair use due to the noncommercial and transformative nature of vids.

Proponents stated that even if the second fair use factor tips in favor of copyright owners because the works used are typically fictional works, "courts have recognized that this factor is likely to be of little importance in fair use cases involving the creation of transformative, original works."[150]

Proponents argued that the third factor, the amount and substantiality of the portion used in relation to the copyrighted work as a whole, also supports noncommercial video creators because these uses "will generally comprise only a small fraction of the works from which they are taken."[151] Use of a small portion of the motion picture in order to fulfill a transformative

---

[145] C11A (EFF) at 19.

[146] *Id.*

[147] *Id.* at 15-16.

[148] *Id.* at 16, quoting Francesca Coppa.

[149] While the use of musical works and sound recordings may also be implicated in an infringement action, no circumvention issues appear to pertain to these uses since such works are generally available in unprotected formats.

[150] C11A (EFF) at 19, citing *Campbell v. Acuff-Rose Music, Inc.* 510 U.S. 569, 579 (1994) and *Blanch v. Koons*, 467 F.3d 244, 253 (2d Cir. 2006).

[151] C11A (EFF) at 19.

purpose, they argue, will generally lead to the conclusion that the third factor favors fair use.

Proponents also asserted that the fourth fair use factor supports a claim of fair use. They stated that because the use is noncommercial and transformative, the videos "will almost never be a substitute for the original works. In fact, in many cases, a remix video will be hardly comprehensible to someone who has not already seen the original video 'texts' from which the clips are drawn."[152] Moreover, proponents argued that to the extent these works criticize the original work, it is unlikely that a copyright owner would be willing to authorize the use.

Opponents of the proposed class stated that generalizing about the underlying use as fair "would encourage widespread circumvention and subsequent unauthorized copying and creation of derivative works, while leaving it to the courts to sift through the legal rubble that results."[153] They also stated that the limitation for "noncommercial" uses would do little to curb the harmful impact, because these videos are often distributed by online services that earn significant income from the creations of vidders.[154] The Joint Creators also contended that the "[i]ndustry confidence in the average consumer's recognition that digital locks are not meant to be picked has led to the rapid spread of content available in many digital forms" and that designating the class would confuse the public and create a slippery slope to exemptions for particular uses, rather than classes of works.[155]

Finally, the Joint Creators argued that the proponents had not demonstrated that access to motion pictures for noninfringing purposes requires circumvention of access controls. They argued that alternatives are available and that "to the extent that the final product may be, in a particular case, noninfringing, 'fair use has never been held to be a guarantee of access to copyrighted material in order to copy it by the fair user's preferred techniques, or in the format of the original.'"[156]

---

[152] *Id.*

[153] R 46 (Joint Creators) at 66.

[154] *Id.*

[155] *Id.* at 66-67.

[156] *Id.* at 67, citing *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 459 (2d. Cir. 2001).

4. *NTIA Comments*

NTIA expressed support for an expansion of the existing class of audiovisual works to include all college and university level instructors and students. It stated that "proponents persuasively demonstrate that while film and media studies professors have an obvious need to use clips in their instruction, other subject matter instructors at the university level also have a need to use clips to supplement effective instruction."[157] NTIA also found that alternatives to circumvention, such as videotaping clips using a video camera, online movie services, and clip services, were either too expensive or were not viable market options.[158] Moreover, NTIA was not persuaded by the opponents' argument that an expansion of the class would negate the usefulness of access control mechanisms on DVDs or encourage abuse of the exemption. NTIA noted that the opponents of the proposed class have not identified any harm that has resulted from the designation of the current class.

NTIA did not believe that proponents of designation of a class that would include teachers and students in the K-12 setting provided sufficient evidence of harm or need in the record of this proceeding. Specifically, it stated, "Without such proof, the Register should not consider recommending expansion of this exemption beyond the college or university level."[159]

NTIA recommended limiting the class to address the use of DVDs included in the educational library or departments of the academic institutions, noting that such a limitation would limit misuse of the exemption.[160]

NTIA also supported the proposal to designate a class of works for the benefit of documentary filmmakers. While it agreed with opponents of the proposed class that documentary filmmakers are more likely to be sophisticated enough to license the clips used to ensure their compliance with the law, it was also persuaded that license requests may be denied to documentary filmmakers, in certain cases, such as when a clip is to be used to criticize the original film. NTIA was concerned that in those cases, the filmmakers may be unnecessarily foreclosed from a noninfringing use in the proposed class is not designated.

---

[157] NTIA Letter at 4.

[158] *Id.* at 5.

[159] *Id.* at 4.

[160] *Id.* at 6.

NTIA expressed general support for the request to designate a class that would permit extraction of film clips for use in noncommercial videos, noting that since the last DMCA rulemaking, the world of online video has grown significantly, creating new norms and expectations that did not exist in 2006. NTIA expressed its view that the proposed class would offer an important opportunity for education. social comment and criticism, and further innovation. In NTIA's view, the DMCA should not stifle innovation in this area.

However, NTIA was not convinced that all potential uses under this proposal are clearly noninfringing uses. While some remix videos contain criticism and comment, are noncommercial, and use limited clips, thousands of video remixes are posted on a daily basis and not all of them are noninfringing. NTIA suggested a narrowing of the language of the proposed class to ensure that all uses that benefit from the designation of the class are noninfringing. NTIA suggested that such language should require that the clips from the audiovisual work must be for remix videos that are used for social comment or criticism, or that are used in transformative-type works according to established fair use principles.

5. *New Classes of Works–Reasoning and Rationales*

Issues surrounding CSS-protected DVDs have been a feature of the 1201 rulemakings since 2000. Most frequently, concerns have been expressed about: (1) access to DVDs on unsupported platforms; (2) accessing lawfully acquired region-coded DVDs that were purchased in other regions; and (3) avoiding access to unwanted material on DVDs, such as the unskippable promotional trailers sometimes contained on DVDs. In this rulemaking proceeding, offshoots of some of these arguments can be found.[161]

In contrast to the prior access-related proposals, a striking and unifying feature in the proposals for the educational exemptions of CSS-encrypted DVDs, the documentary filmmakers' proposal, and the proposal for noncommercial, transformative uses of CSS-protected DVDs, is that all of these proponents already have access to the works on an ongoing basis.[162] All of the

[161] *See, e.g.,* Carney/Rizik proposed classes, *infra* at p. 215

[162] This analysis is limited to CSS even though some proponents also mentioned motion pictures in Blu-ray format as well. The record in this rulemaking did not demonstrate that any works available in Blu-ray format were not also available in CSS-protected DVDs. Moreover, there was no showing that the quality of a motion picture contained on a Blu-ray disc was needed in order to make a noninfringing use. The record in relation to the AACS protection contained on Blu-ray discs was essentially nonexistent. Accordingly, the Register finds no basis on which to separately assess an exemption related to Blu-ray discs within the present rulemaking.

proponents own, rent, or borrow lawful copies of CSS-protected DVDs. All of the proponents own, possess, or have access to DVD CCA-licensed DVD players that lawfully decrypt these works. All of the proponents obtain lawful access to these works every time they seek access to the works. All of the proponents wish to circumvent access controls not in order to access the works, but rather to display and/or make copies of portions of a work contained on a CSS-protected DVD. Film professors seek to make copies of portions of motion pictures on DVDs to put together in compilations for efficient use in class. Other educators seek to reproduce clips of motion pictures[163] for illustration, demonstration, and examples in class. Documentary filmmakers seek to reproduce portions of motion pictures for use as illustration, demonstration, commentary, or criticism in the creation of new works. Noncommercial creators seek to use portions of motion pictures to create noninfringing works involving criticism and/or comment that they assert are transformative.

The striking feature about all of these proposals related to CSS-protected DVDs is that the proponents all seek *to use* works for which they have lawful access. They all seek to make uses that implicate Section 106 rights, but in ways that are alleged to be noninfringing. They also all seek to use only portions of works. The question fairly raised is: why would their ability to make such noninfringing uses be adversely affected by a technological measure that controls *access*? The answer to that question lies in the nature of CSS and the definitions in the statute.

a. The use of an access control to control use of a work

CSS is a form of encryption. It is an encryption-based system that employs an algorithm to encrypt the contents of a DVD and combines multiple layers of encryption with an authentication process to protect a DVD's (typically copyrighted) video content from unauthorized access or unauthorized consumer copying.[164] Encryption is one of the repeatedly cited forms of technological measures that protect access to works that are mentioned in the legislative history of the DMCA.[165] Encryption, such as CSS, fits the statutory definition of a technological measure that effectively controls access to a work because, in the ordinary course of its operation, the encryption requires the application of information, or a process or a treatment,

---

[163] As noted elsewhere, for purposes of copyright law, the term "motion pictures" includes not only movies but also works such as television shows and "bonus" material on DVDs.

[164] *Realnetworks, Inc. v. DVD Copy Control Ass'n*, 641 F. Supp.2d 913, 919 (N.D. Cal. 2009) ("Realnetworks").

[165] *See, e.g.*, Commerce Report at 37.

with the authority of the copyright owner, to gain access to the work.[166] CSS is a technological measure that controls access to a work.[167]

But that encrypted work is automatically decrypted whenever a person in possession of a DVD places the DVD in an authorized DVD player. What is the point of an access control when access is granted to everyone in possession of the DVD? [168] The answer is that CSS as an access control is a means to a further end. Applying CSS, a technological protection measure that controls access to a work, ensures that decryption must be accomplished in a particular manner authorized by the copyright owner, that is, access is provided only on use-limited DVD players. To obtain authorized decryption, copyright owners require device manufacturers to agree to additional contractual terms, specifically, terms that inhibit the reproduction of the content on DVDs. Decryption keys are licensed to device manufacturers that produce DVD players.[169] All authorized DVD players, whether a stand-alone DVD player or a DVD drive in a computer, obtain the keys to decrypt CSS from the DVD CCA. As a condition of obtaining the decryption keys, the device manufacturer agrees to certain conditions on the capabilities of the DVD player, including an agreement that the device will not contain a digital output that will allow digital reproduction of the decrypted content.[170] By design, the CSS encryption system serves as a link in a chain of legal and technological requirements that ultimately inhibit the possessor of a CSS-protected DVD from copying the work or works embodied in it. Practically speaking, CSS does not so much limit access to the works contained on the DVD, but rather limits the means of obtaining access, or the manner in which access is granted. To the extent that access is limited, it is limited only in relation to the type of device that can provide access. The only type of device that can provide authorized access is a device authorized through license by the DVD CCA, which contractually obligates device manufacturers to limit the reproduction capabilities of the device.

This decryption process is generally unseen by the person playing or accessing a DVD,

---

[166] 17 U.S.C. §1201(a)(3)(B).

[167] *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp.2d 294, 318 (S.D.N.Y. 2000), *aff'd, Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 436-37 (2d Cir. 2001). *Accord, RealNetworks*, 641 F. Supp. 2d at 922.

[168] One example of an access control on DVDs that does actually prevent access is region coding, which precludes DVDs from different geographical regions from playing on a single DVD player. *See* 2003 Recommendation of the Register of Copyrights at 120-24.

[169] *RealNetworks*, 641 F. Supp.2d at 919.

[170] *Id.* at 950.

because the keys to decrypt the encryption are not directly distributed to the end-user. The possessor of a DVD must use a licensed device,[171] with limited copying capabilities, in order to access the work. CSS, although a technological measure that controls access to a work, essentially prevents digital reproduction of the motion pictures on DVDs.[172] Thus, CSS is an access control that also (and, arguably, primarily) serves to prevent copying.[173]

In 2000, the Register recognized that CSS may interfere with use in a manner that was not contemplated by Congress, stating:

> Proponents of an exemption for motion pictures on DVDs raised four general arguments. First, they asserted that CSS represents a merger of access and use controls, such that one of those two control functions of the technology cannot be circumvented without also circumventing the other. . . Since Congress prohibited only the conduct of circumventing access measures and declined to enact a comparable prohibition against circumvention of measures that protect the rights of the copyright owner under § 1201(b), they argued that a merger of controls exceeds the scope of the congressional grant. In this view, the merger of access and use controls would effectively bootstrap the legal prohibition against circumvention of access controls to include copy controls and thereby prevents a user from making otherwise noninfringing uses of lawfully acquired copies, such as excerpting parts of the material on a DVD for a film class, which might be a fair

---

[171] If using an unlicensed device, the user's access would not be "with the authority of the copyright owner" and thus would constitute circumvention of the Section 1201(a)(1) prohibition.

[172] Analog reproduction may be impeded by Macrovision's automatic gain control and color stripe copy control technology that is used on many commercially released DVDs.

[173] *Id.* at 28. *See also*, *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp.2d at 322. ("Perhaps more significantly, it prevents exact copying of either the video or the audio portion of all or any part of the film.") While it is true that limiting the decryption of CSS through a licensing system *has the effect* of preventing copying, no court has concluded that CSS, as a technological protection measure unrelated to licensing concerns, is in fact a technological protection measure that "effectively protects the right of a copyright owner." *See* 17 U.S.C. § 1201(b). The encryption itself does not "prevent[], restrict[], or otherwise limit[] the exercise of a copyright owner under this title." It is the licensing arrangement with device manufacturers that inhibits digital reproduction. This contractual restriction is not part of CSS itself and does not constitute a technological protection measure that protects the rights of the copyright owner. Two recently introduced technological measures, ARccOS and RipGuard, appear to qualify as such measures,. ARccOS is a copy-protection system developed and marketed by Sony DADC and RipGuard is a copy-protection system developed by Macrovision, Inc. Both measures attempt to impede the functionality of DVD copying programs by inserting corrupted or "bad" sectors on DVDs: intentional obstacles placed subversively in DVD data that cause "read" errors when the sectors are read by a DVD drive so as to severely impede copying of the DVD. *See RealNetworks, Inc.*, 641 F. Supp. 2d at 936-940. In contrast to these copy controls, CSS itself appears to be solely a technological protection measure that protects access which, through licensing arrangements with device manufacturers, has the effect of restricting unauthorized copying by the users of DVD players. It bears noting that not all unauthorized copying is infringing, *ergo*, authorization is not necessary for a noninfringing use of a copyrighted work.

> use. While this is a significant concern, there are a number of considerations to be balanced. From the comments and testimony presented, it is clear that, at present, most works available in DVD format are also available in analog format (VHS tape) as well. . .When distributed in analog formats—formats in which distribution is likely to continue for the foreseeable future— these works are not protected by any technological measures controlling access. . . Therefore, any harm caused by the existence of access control measures used in DVDs can be avoided by obtaining a copy of the work in analog format. See House Manager's Report, at 7 (''in assessing the impact of the prohibition on the ability to make noninfringing uses, the Secretary should take into consideration the availability of works in the particular class in other formats that are not subject to technological protections.''). Thus far, no proponents of this argument for an exemption have come forward with evidence of any substantial or concrete harm. Aside from broad concerns, there have been very few specific problems alleged. The allegations of harm raised were generally hypothetical in nature, involved relatively insignificant uses, or involved circumstances in which the noninfringing nature of the desired use was questionable (e.g., backup copies of the DVD) or unclear. . . This failure to demonstrate actual harm in the years since the implementation of the CSS measures tends to undermine the fears of proponents of an exemption. . . .
>
> The merger of technological measures that protect access and copying does not appear to have been anticipated by Congress. Congress did create a distinction between the conduct of circumvention of access controls and the conduct of circumvention of use controls by prohibiting the former while permitting the latter, but neither the language of section 1201 nor the legislative history addresses the possibility of access controls that also restrict use. It is unclear how a court might address this issue. It would be helpful if Congress were to clarify its intent, since the implementation of merged technological measures arguably would undermine Congress's decision to offer disparate treatment for access controls and use controls in section 1201. At present, on the current record, it would be imprudent to venture too far on this issue in the absence of congressional guidance. The issue of merged access and use measures may become a significant problem. The Copyright Office intends to monitor this issue during the next three years and hopes to have the benefit of a clearer record and guidance from Congress at the time of the next rulemaking proceeding.[174]

The passage of time has brought about a number of changes that affect the equation that was before the Register in 2000. While there has been no guidance from Congress on the issue, the factual record is significantly different and much more developed in 2009 than the record before the Register in 2000. The proponents of the classes of works involving motion pictures on

---

[174] *See* 2000 Recommendation of the Register of Copyrights, 65 Fed. Reg. at 64,568 (footnotes and citations to the record omitted).

CSS-protected DVDs have demonstrated that certain noninfringing uses are being affected by the prohibition, and that alternative formats are no longer available, in sharp contrast with the record in 2000.

In 2006, the film and media studies professors demonstrated that high-quality resolution and additional attributes of motion pictures on DVDs were reasonably necessary for the noninfringing pedagogical purpose of the use. The 2009 record is largely congruent with the evidentiary record in 2006 in regard to noninfringing uses that film and media studies professors desire to make. However, in the current rulemaking, a broader range of educators have made a persuasive case that the use of portions of CSS-protected DVDs would generally constitute a noninfringing use in the classroom. Similarly, educational use is not limited to teachers, but also often involves student uses of works.

However, the record in relation to the use of motion pictures contained on CSS-protected DVDs is not limited to educational use. Documentary filmmakers have made a compelling case for the need to use portions of the digital versions of motion pictures that exist on CSS-protected DVDs for purposes of criticism and comment within a documentary.

The creators of noncommercial, transformative works have also presented evidence which reasonably demonstrates that some number of works created for purposes of criticism or comment benefit from and, for certain purposes, depend upon the use of portions of motion pictures contained on CSS-protected DVDs.

Given the fact that all of these proposals seek to circumvent CSS-protected DVDs in order to accomplish an allegedly noninfringing use, the Register finds it appropriate to analyze these proposals in an aggregated analysis. As stated previously, there is no dispute that CSS qualifies as a technological protection measure that "effectively protects access" to the motion pictures on CSS-protected DVDs. This threshold determination leads to the next level of discussion, that is, whether each of these proposals involves underlying noninfringing uses.

If the proposed purpose of the circumvention is demonstrated to be a noninfringing use, the next critical question will be whether the prohibition against circumventing the technological protection measure is causing an adverse effect on such noninfringing uses. In essence, this is the inquiry mandated by the first statutory factor, the availability for use of copyrighted works.[175] In

[175] 17 U.S.C. § 1201(a)(1)(C)(i).

this assessment, the Register will need to examine whether alternative formats of the works are available for use and/or whether alternative means of accomplishing the noninfringing uses are available to users without circumventing CSS. If the result of that analysis reveals that, up to that point, the case for designating a class of works has been made, the Register will examine the other statutory factors contained in Section 1201(a)(1)(C)(ii)-(v), including the likely effect of circumvention to the market for or value of copyrighted works, to assess the propriety and scope of the class or classes to be designated

b. The underlying noninfringing use

All of the proponents and supporters of the classes covering CSS-protected DVDs for educational, documentary and noncommercial videos have demonstrated that some of the underlying uses may be fair uses. The educational users, the documentary filmmakers and the noncommercial, transformative users all fit squarely within the illustrative uses of criticism, comment, or teaching, set forth in the preamble of Section 107.

Under the first fair use factor, the proposed uses of portions of motion pictures are generally transformative in nature—they use the work for a different purpose than the entertainment purpose of the original work, such as criticism, comment, or as an illustration for teaching purposes.[176] In the academic and the noncommercial transformative use context, the character of the use is also noncommercial. In the case of documentary films, although the use may frequently be commercial in nature, the purpose of criticism or comment about the original works will generally be transformative, and thus the commercial purpose is less significant when assessing a transformative use.[177]

The Register does not conclude that all, or even most, of the examples offered by proponents of these classes – and especially of the class consisting of "noncommercial videos" – are transformative in the sense that is relevant to an analysis of the first fair use factor. However, it is fair to conclude that more than a trivial portion of those examples do qualify as

[176] Educators' use of the portions of motion pictures do not transform the works themselves, but extract portions for the transformative purpose of comment, criticism and analysis of those portions in the classroom setting. In the preamble of Section 107, the illustration of teaching is followed by the parenthetical clause "(including multiple copies for classroom use). . . ." This reference suggests that a mere reproduction may be transformative if the context of the use is for a new and different purpose. Moreover, to the extent that educators seek to create a compilation of clips, they are creating that compilation for a different purpose from the original works.

[177] *Campbell v. Acuff-Rose Music*, 510 U.S. at 584-585.

transformative.

Despite the frequently commercial nature of the use with respect to documentary filmmakers, the activities of documentary filmmakers may be transformative in nature and purpose.[178] Documentary filmmakers and noncommercial vidders may use works in order to criticize or comment upon the copyrighted work being used. When a motion picture is used for purposes of criticism and comment, such a use is a form of quotation, long recognized as paradigmatic productive use with respect to textual works, which is at the core of fair use's function as a free-speech safeguard.[179] For example, clips from one or more copyrighted works may be used to make a point about some perceived theme or undercurrent in works, such as violence against women or racism.[180] In other situations, portions of works may be used and remixed in order to make political statements about candidates[181] or copyright law itself.[182]

Under the second fair use factor, the nature of the copyrighted motion picture is generally creative in nature and thus within the core of copyright's protective purposes.[183] On the other

---

[178] C11B (Kartemquin) at 2-3, citing examples of motion picture clips used to illustrate a documentary filmmaker's point, (*e.g.*, the 2000 film *It Conquered the World! A Story of American International Pictures*, which addressed the history and development of the horror film genre, made fair use of clips from horror films to show, *inter alia*, the political context of "alien visitation films."). *See Hofheinz v. Discovery Communs., Inc.*, 2001 U.S. Dist. LEXIS 14752 (S.D.N.Y. Sept. 10, 2001)(citations omitted). In addition to summary judgment due to the tolling of the limitations period, the *Hofheinz* court found that the use of the alien films was a fair use. ("Setting aside the fact that Hofheinz has produced no evidence as to the existence of such a market, apart from the nine licenses that she has entered into in the last six years, or any evidence whatsoever that the two clips had an adverse impact on the market for clips of *Invasion of the Saucermen*, to find that the use of short clips presumptively constitutes infringement would eviscerate the fair use defense in this area 'since every copyright infringer seeking the protection of the fair use doctrine could have potentially sought a license from the owner of the alleged mark.'").

[179] *See Eldred v. Ashcroft*, 537 U.S. 186, 220 (2003) ("[T]he 'fair use' defense allows the public to use not only facts and ideas contained in a copyrighted work, but also expression itself in certain circumstances.")

[180] *Wormen's Work*, available at: http://www.blip.tv/file/2299910/ (critical observation of female characters in numerous episodes of the television series, *Supernatural*); *Racism in Disney*, available at: http://www.youtube.com/watch?v=LibK0SCpIkk (Last visited 4/30/10.) (criticizing the characterization of race and ethnicity in numerous Disney films).

[181] *See* http://www.youtube.com/watch?v=6h3G-lMZxjo (Last visited 4/30/10.) (remix of famous 1984 Apple Superbowl advertisement).

[182] *See* http://www.youtube.com/watch?v=CJn_jC4FNDo (Last visited 4/30/10.) (copyright law explained through the remixing of Disney movies).

[183] Given that this analysis is generalized, and does not analyze a specific use, the assessment of the actual nature of the copyrighted work will vary from case to case. However, the record in this rulemaking generally revealed examples of motion pictures on the creative side of the spectrum, rather than factual in nature.

hand, the work is also published if it is available on DVD.[184] The ambiguity created by the weight of these intra-factor inquiries must also be considered in relation to the transformative purpose of the uses. The Supreme Court has stated that in relation to certain transformative uses, the second factor is of limited assistance in evaluating whether the use is a fair use.[185] Literary quotation often includes references to novels to make a point (fair use quotation is not limited to quotations of non-fiction works), and there appears to be no reason why short clips from creative motion pictures should not be able to serve a similar purpose when the use of the motion picture is transformative.

Under the third factor, an essential component of all of the proposals for use is that only a short portion of the work is used.[186] Quantitatively, the evidence in the record suggests that most of the uses by educators, students, documentary filmmakers, and noncommercial, transformative users involve a relatively small portion of the copyrighted work. For example, evidence demonstrated at the hearings generally involved the use of portions of motion pictures that were in some cases less than 1 minute and never more than 3-5 minutes in length. In relation to a typical movie of perhaps 120 minutes, that is a quantitatively small amount that is comparable to a quotation of a short passage from a book, particularly when used for a new and different purpose from the original.[187] Qualitatively, although the portion used may be an important scene or scenes from one or more movies, the transformative nature of the use in relation to a published work tends to avoid a situation where the portion used, either quantitatively or qualitatively, would adversely affect or supersede the potential market for or value of the underlying works. As the Supreme Court has stated, in certain situations, using the heart of the work may be the optimal way of avoiding taking too much quantitatively, particularly where it is necessary to "conjure up"

---

[184] The scope of fair use generally is narrower with respect to unpublished works than to published works. *Harper & Row, Publrs. v. Nation Enters.*, 471 U.S. 539, 564 (1985).

[185] *Campbell v. Acuff-Rose Music, Inc*. 510 U.S. at 579.

[186] The Register has taken this factor, as well as the evidence in the record, into account in recommending an exemption that permits circumvention only for the purpose of using short portions of a work. *See infra*.

[187] While in some cases, multiple clips from the same motion picture were used, or larger percentages of interviews contained on the DVD were used, the question of whether the amount used was reasonable in relation to the purpose is a fundamental fair use question that should be addressed under the rubric of fair use analysis, not precluded *per se* as a result of the prohibition on circumvention. There were undoubtedly some examples introduced into record that used an amount of the work that may well disqualify them from relying on the fair use defense. *See, e.g.*, Luminosity's *Vogue/300* (available at http://www.youtube.com/watch?v=QNRjzUB7Afo (Last visited 4/30/10.) showing an extensive montage of scenes from the movie *300* mixed with Madonna's sound recording, *Vogue*).

the work used.[188] Moreover, unlike the situation in which a significant qualitative use of an unpublished work adversely affected the first publication of the work, all of the works at issue in these proposals have been published.[189]

Under the fourth factor, when the use of the work is transformative, there is likely to be no interference with the primary or reasonable derivative markets for the underlying work. Opponents of the proposed classes did not identify any use by educators, documentary filmmakers, or noncommercial vidders that has harmed the market for, or value of, any copyrighted motion picture. Any diminution in value resulting from the use for purposes of criticism or commentary would also not be cognizable harm under the Copyright Act.[190] The use of small portions of motion pictures for criticism or commentary is not likely to be a market that the copyright owner would reasonably be expected to exploit. Indeed, even if such a potential market were reasonably anticipated, it would not eliminate the need to permit an unauthorized use that was fair. Moreover, while copyright owners have begun to experiment with models for providing clips to educators, there was no evidence in the record that a viable or efficient mechanism for permissions or licensing exists or is likely to exist in the ensuing three-year period.[191] Thus, the fourth factor tends to weigh heavily in favor of fair use for the vast majority of truly transformative uses.

On balance, the fair use analysis tends to demonstrate that many of the uses sought by the proponents may be considered fair uses. Importantly, the Register is not making any judgment as to whether any particular example offered by proponents actually is a fair use. Some uses in the educational, documentary, and noncommercial, transformative context will undoubtedly be infringing. The point is that a cognizable basis has been established for concluding that some (probably many) uses in each of the proposed classes are likely to qualify as noninfringing uses under established judicial precedents.

---

[188] *Campbell v. Acuff-Rose Music*, 510 U.S. at 588-589 ("But if quotation of the opening riff and the first line may be said to go to the 'heart' of the original, the heart is also what most readily conjures up the song for parody, and it is the heart at which parody takes aim. Copying does not become excessive in relation to parodic purpose merely because the portion taken was the original's heart. If 2 Live Crew had copied a significantly less memorable part of the original, it is difficult to see how its parodic character would have come through.")

[189] *Harper & Row, Publrs. v. Nation Enters.*, 471 U.S. at 564-565.

[190] *Id.* at 591-592.

[191] The creation of such a mechanism would be a relevant consideration in any future Section 1201 rulemaking proceeding.

However, the fact that the proponents have identified a number of noninfringing uses that could be accomplished by means of circumvention does not necessarily mean that the prohibition on circumvention is having an adverse effect on noninfringing uses. Other means of accomplishing the noninfringing uses without circumventing access controls might be available. That question is addressed below in the discussion of Section 1201(a)(1)(C)(i).

c. The meaning of a "portion" of a work

The proponents of classes of works related to DVDs relied only on activities involving the use of portions of DVDs[192] "for the purpose of extracting clips for inclusion in noncommercial videos that do not infringe copyright,"[193] or "for the purpose of making compilations of portions of those works for educational use in the classroom by media studies or film professors."[194] The Copyright Office sought clarification for the contours of a "portion" in questions after the hearing, inquiring whether specific quantitative limitations would be advisable.[195] Proponents and opponents both generally opposed quantifying a "portion" in relation to a maximum length or percentage. Although delineation of what amount or percentage of a work would, at its outer limits, constitute a "portion" was generally said to be impossible, all of the specific evidence introduced into the record to illustrate vids or documentaries demonstrate that, generally, a relatively small percentage (quantitatively) of the motion picture is needed for the creation of a vid.[196] The Register agrees that the use of some portion of a motion picture for a transformative

---

[192] The class proposed by documentary filmmakers did not mention a portion or clip from a work. However, documentary filmmakers repeatedly made it clear in their testimony that they sought to circumvent solely to obtain clips from DVDs. *See, e.g.*, T Quinn, 5/7/09, at 21 ("in our work and in particularly in some other documentaries work which is also very professional and I highly respect, there are a lot of clips used from a lot of different things. They're very short.")

[193] C11A (EFF) at 1.

[194] C4E & C4F (Decherney) at 1.

[195] *See* Copyright Office Questions to Panelists on DVD-related Hearing Panels, http://www.copyright.gov/1201/2008/answers/9_21_responses/questions-panelist.pdf (Last visited 4/30/10.) (" A number of the proposals for exemptions for DVDs included, within the descriptions of their proposed classes, a condition that the use be for the purpose of compiling *portions* of motion pictures....From your unique perspectives, is there a limitation, either in terms of duration or percentage (or both), which could be incorporated into the definition of an exempted class of works?").

[196] In responses to questions, the Organization of Transformative Works and EFF argued that since "voice-over commentaries" combined with films is now possible, it would not be prudent to quantify the percentage of a work that could be used. *See* Post-Hearing Response of OTW and EFF to August 21st Supplemental Questions to Panelists on DVD-Related Hearing Panels at 3-4. While such an activity may be possible, no particular example of a use of more than a portion of a work was introduced, and it is questionable whether the use of more than a

purpose may qualify as a fair use.

The opposition to any form of delineation of a portion in regard to time-length or percentage of the overall work was, broadly speaking, two-fold. First, proponents argued that a precise limit would raise a host of questions, such as, what would the percentage specifically apply to: the contents of a DVD or a component work on the DVD? Second, both proponents and opponents stated that since the amount of the use was only one factor in the fair use analysis, delineating a particular amount in an exemption to the prohibition on circumvention might mislead the public. On one hand, opponents argued that the public might interpret the exemption to indicate that any use of such a "portion" is necessarily noninfringing. On the other hand, proponents argued that some uses in excess of the articulation of a "portion" might be a fair use under the totality of the fair use analysis, but would be precluded by the exemption. While it was not the Copyright Office's intention to suggest that any temporal limitation set forth in the definition of the class should be interpreted as drawing the line between a fair use and an unfair use, the Register recognizes that any attempt to determine precisely how large an excerpted portion could be without violating the prohibition on circumvention would be problematic. An amount that might be reasonable in one context might be excessive in another. Moreover, a regulation defining how large an excerpted portion of a work could be for purposes of the exemption from the prohibition on circumvention could well mislead the public into a false belief that the regulation was, for all practical purposes, defining the quantitative limits of fair use.

Nevertheless, the Register concludes that some characterization of the quantitative amount of the use for purposes of criticism or comment is appropriate. No commenter or witness has persuasively argued that designation of a class of works is warranted in order to permit the use of extensive excerpts of motion pictures. Virtually all of the evidence of noninfringing uses of motion pictures for criticism or comment has involved short portions of motion pictures in order to make a pedagogical point or to use a work for criticism or comment in a documentary film or noncommercial vid. There was concern expressed that qualification of a "portion" in some way might raise questions about the cumulative amount of a work used in a transformative work, or the cumulative amount used within a semester of classes. While these concerns have some merit, the Register finds that the benefit of some qualification of the term "portion"outweighs the costs. The inclusion of the phrase "short portions of the works" in the description of the class will make it clearer that a case that extensive use of a motion picture is a noninfringing use has not been

---

portion of a work in a vid would support a claim of fair use. Thus, the record demonstrates only that the use of portions of works in a vid may be noninfringing uses that are adversely affected by the prohibition.

established in the record, and that such uses disqualify a user from the benefit of the designation of this class of works. Likewise, if a film class focused on a particular film over the course of a semester, the fact that most (or all) of the work was cumulatively used during the semester would not prevent the application of the exemption to short portions incorporated into a number of compilations of clips for use in individual classes.

The use of the phrase "short portions of the works" highlights the evidentiary record that forms the basis of this recommendation. The proponents' justification for the need for designating a class of works has not established that relief is needed to permit circumvention for the purpose of making more than a short portion of a work. This is not to suggest that the use of a long portion cannot be a noninfringing use in a particular circumstance. However, noninfringing uses may be accomplished in various ways without circumvention, as the record in this rulemaking demonstrates. The harm to copyright owners' interests that could result from a generalized perception that any amount, or large portions, of a motion picture can be reproduced through circumvention warrants a balancing of the interests in this case. Those interests can best be balanced by limiting the class to permit the use of short portions of motion pictures.

d. Application of statutory factors

The proponents have demonstrated that there are an appreciable number of noninfringing uses that they contend are, or are likely to be, adversely affected by the prohibition on circumvention, because CSS prevents certain forms of reproduction of motion pictures contained on CSS-protected DVDs. Having established that CSS is a technological protection measure that effectively controls access to the work, and that there are noninfringing uses that are adversely affected by the prohibition on circumvention, the proponents have met their threshold burdens in support of designating a class of works.

These threshold inquiries do not, however, end the analysis of whether designation of a class of works is warranted. Congress established a series of factors in Section 1201(a)(1)(C) to be considered in the rulemaking proceeding in order to assess whether relief from the prohibition on circumvention of access controls is appropriate.

Factor One

The first factor requires the Librarian to consider "the availability for use of copyrighted

works."[197] In considering the availability for use of copyrighted works, Congress indicated that the prohibition does not only have the ability to limit uses, but also to foster new use-facilitating business models that offer the public access to works in a variety of new ways. The House Manager's Report stated:

> In assessing the impact of the implementation of technological measures, and of the law against their circumvention, the rulemaking proceedings should consider the positive as well as the adverse effects of these technologies on the availability of copyrighted materials. The technological measures -- such as encryption, scrambling and electronic envelopes -- that this bill protects can be deployed, not only to prevent piracy and other economically harmful unauthorized uses of copyrighted materials, but also to support new ways of disseminating copyrighted materials to users, and to safeguard the availability of legitimate uses of those materials by individuals. These technological measures may make more works more widely available, and the process of obtaining permissions easier. . . .
>
> Similarly, in assessing the impact of the prohibition on the ability to make noninfringing uses, the Secretary should take into consideration the availability of works in the particular class in other formats that are not subject to technological protections. [198]

This statement in the legislative history has application to both the first and the fourth statutory factors. In relation to the first factor, the Register has interpreted the relevant inquiry to include, (1) whether the availability of the work in protected format enhances and/or inhibits public use of particular works, (2) whether the work protected is also available in other formats (and whether those formats are protected by access controls), and (3) if alternative formats are available, whether such formats are sufficient to accommodate noninfringing uses.[199]

i. Does the protection of the work enhance and/or inhibit the availability of the work for use?

In past rulemakings, the MPAA has offered evidence that CSS protection was a critical

---

[197] 17 U.S.C. § 1201(a)(1)(C)(i).

[198] House Manager's Report at 6-7.

[199] 2006 Recommendation of the Register of Copyrights at 19-22.

factor in the decision to release motion pictures in digital format.[200] It has also been argued in the past that without the provisions in Section 1201, the motion picture industry would have been, and would prospectively be, reluctant to distribute motion pictures in DVD format if protected DVDs were to constitute a class exempted from the prohibition against circumvention. This assertion was credited in past rulemaking proceedings and is not questioned retrospectively in this proceeding. But to the extent that this proposition was true in the past, it is questionable whether this continuing assertion is supportable in the realities of the current marketplace. CSS-protected DVDs are now the dominant form of distribution for motion pictures to the public.[201] CSS-protected DVDs have continued to be the dominant format even though circumvention tools have long been widely available online.[202] At this point in time, the suggestion that an exemption for certain noninfringing uses will cause the end of the digital distribution of motion pictures is without foundation. It is clear that a transition is currently taking place to new forms of digital distribution, such as Blu-ray discs protected by the AACS system, and it is possible that an designating a class based on motion pictures on CSS-protected DVDs will lead to an increased desire to foster that transition. However, the availability of motion pictures generally is unlikely to be diminished by designating such a class of works. Thus, while CSS-protected DVDs may very well have fostered the digital distribution of motion pictures to the public, there is no credible support for the proposition that the digital distribution of motion pictures continues to depend on the integrity of the general "principle" that the circumvention of CSS is always unlawful. While it may well be true that an class that was not carefully tailored (such as "motion pictures on CSS-protected DVDs") would risk confusion, an appropriately tailored class should not compromise the integrity of the prohibition for circumvention with respect to non-covered uses, as will be examined further below.

ii. Is the protected work available in other formats?

There is also evidence that the availability of the works for use has been diminished in relation to particular uses as a result of CSS-protected DVDs displacing alternative formats for

---

[200] *See, e.g.*, 2000 Recommendation of the Register of Copyrights, 65 Fed. Reg. at 64,569. (" The release of audiovisual works on DVDs was predicated on the ability to limit piracy through the use of technological access control measures).

[201] *See, e.g.*, "Blu-ray market share on the decline? http://news.cnet.com/8301-17938_105-10050918-1.html (Last visited 5/5/10.); "Blu-ray Disc Statistics - Blu-ray Software Market Share Vs. DVD and HD DVD," http://www.blu-raystats.com/MarketShare/index.php. (Last visited 4/30/10.)

[202] *See, e.g.*, Copyright Office Hearing Transcript, April 3, 2006, at 75-80.

motion pictures. In past rulemaking proceedings, the availability of motion pictures in unprotected formats was a significant consideration. In the 2000 rulemaking, the record demonstrated that most motion pictures on CSS-protected DVDs were also available on VHS tape.[203] Although some additional or "bonus" material on the DVDs was not available in unprotected formats, the public benefitted from the availability of the added features contained on DVDs that were not otherwise available, and the proponents did not sufficiently demonstrate that the need for the protected material outweighed the benefit of the prohibition in encouraging the digital dissemination of motion pictures together with those added features.[204]

The current record reveals a very different picture with respect to the existence of alternative formats from what existed in 2000. CSS-protected DVDs are now the dominant form of distribution for motion pictures. VHS tapes of motion pictures are no longer being commercially distributed. Some content may be available from other sources, such as Hulu and other authorized websites, but that content is not a viable alternative to the multitude of motion pictures available on DVD. The offerings on Hulu and other authorized sources are very limited relative to the works available in DVD format. CSS-protected DVDs are the primary, and often sole, source of the motion pictures for the public in general, and for the proponents of these classes of works in particular.

(iii) Are Alternative Means of Accomplishing the Noninfringing Use Available to Users?

Camcording the Screen Output. Rather than focus on alternative unprotected formats of motion pictures that are available to the public,[205] the MPAA focused on an alternative means of obtaining the content of CSS-protected DVDs that does not involve circumvention. Specifically, the MPAA demonstrated at the May 6 hearing how the screen output of a CSS-protected DVD may be camcorded while the DVD is being performed on a television screen.[206] However, the proponents of the class for educational uses argued that better-quality copies are needed because:

---

[203] 2000 Recommendation of the Register of Copyrights, 65 FR at 64,568.

[204] *Id.*

[205] It should also be noted that motion pictures on Hulu are not "unprotected." Rather, access is available through a proprietary player using the Macromedia Flash format.

[206] The demonstration by the MPAA is available for viewing in the public records of the Copyright Office. This is not the first time that this alternative to circumvention was raised in the Section 1201 rulemaking context, but in the current proceeding, the quality of the copy was superior to the copy used in the demonstration given by the MPAA at the 2006 hearings.

> Sound quality is critical in language classes, to ensure that students can understand the dialogue and the technical differences. Music and theater classes need high-quality sound to reflect correctly the tone of musical instruments, or the inflection of the human voice. High image quality enable[s] students to see the nuances of facial expressions and hand gestures. These subtle, non-verbal forms of communication may convey the essential point of a clip used in psychology, sociology, or in literature classes.[207]

Given the fact that the quality obtained from camcording the screen appears to be of reasonably good quality (particularly in comparison to the demonstrative evidence introduced at the hearings three years ago), the question of the sufficiency of the quality from this non-circumventing alternative is significant . However, there are several considerations that diminish the value of camcording the screen as a reasonable alternative to circumvention. First, while alternative non-circumventing copying techniques, such as camcording the screen, may appear to produce results comparable to the results from circumvention, they also require a significantly higher monetary investment. When the cost of the equipment required to camcord from the screen to accomplish high-quality output is demonstrated to be very high—in the realm of $1200 to $1500—the expense of such an option becomes a practical impediment to use.[208] It is specious to suggest that such an alternative means of copying CSS-protected DVDs is a reasonable substitute for circumvention. Moreover, given the significant price, it cannot be said that camcording the screen constitutes a "mere inconvenience." The high cost of obtaining the content through video camera capture is a significant obstacle for use.

Second, camcording the screen may appear to produce results of reasonably good quality, but proponents argue credibly that this quality is, as a functional matter, inferior. Limiting uses based on camcording the screen would adversely affect the ability to engage in many of the intended noninfringing uses.[209] This is the case not only with respect to image/video quality, but also sound quality.[210]

---

[207] T Band, 5/6/09, at 122.

[208] The record reveals that the cost of the equipment used by the MPAA in the demonstration exceeded $1500.00 including the video camera, the flat screen high definition television, the tripod, and the DVD player. *See* T Seymour, 5/6/09, at 209 ("It's about a $900 HD camera. You don't need to use an HD, if you are just recording off of standard DVD. The monitor was $300."); T Tushnet, 5/7/09, at 97 ("We were offered yesterday the prospect of using a $900 camera, plus a tripod -- which, by the way I priced, $300 -- plus a flat screen TV in a room that you can make it completely dark.").

[209] *See* T Decherney, 5/6/09, at 118-119.

[210] *See* T Band, 5/6/09, at 122.

If a motion picture is camcorded from the screen, a technically degraded reproduction is the result. Depending on the quality of the equipment and the conditions in which the screen is filmed, the quality of the reproduction will vary. Although the quality may be sufficient for some uses, such as to show the general development of a scene, that quality will be degraded if the copy must be edited or reformatted. The quality of the picture or sound may also be degraded by the size or format of the performance of the work. For instance, a copy that appears adequate on a television screen may be quite grainy when displayed on a large screen in a classroom, as part of a theatrical screening of a documentary film, or a noncommercial screening at a vidder event.[211] Similarly, converting a reduced quality copy to a format typically used on user-generated content sites may increase the degradation to a level where certain criticism or comment is obscured. The proposed noninfringing uses may not be realized when the reproduction of the work entails uncontrollable degradation of the image and/or sound. Because the point being made may be subtle, the degradation in quality may impede the purpose of the use.[212] The cost and degradation issues related to camcording the screen diminish the value of this alternative to circumvention in a significant number of situations relevant to the proposed class.[213]

Video Capture Software. In order to explore whether other alternatives to circumvention were available to enable noninfringing uses of motion pictures on CSS-protected DVDs, questions about video capture software were raised at the hearings and in post-hearing questions. Video capture software allows a computer user to capture the screen output of a DVD as it is being rendered on the computer monitor. It would appear that this screen capture occurs after lawful decryption of the work has taken place in the DVD player. The Copyright Office inquired about the legality of the use of such software and whether video capture software was similar to camcording the screen with a video camera. Ultimately, and with qualifications, the MPAA stated that the "capture software currently in general use" reproduced motion picture content *after* it has been lawfully decrypted.[214] As a consequence, the use of some types of video capture software is,

---

[211] *See* T Coppa, 5/7/09, at 111-112. While there is a record on the distortion that can occur at a live premiere of a vid, the more compelling argument for vidders is the argument that follows—reduced quality input will result in significant distortion in the reduced-quality formats for online viewing that constitute the primary way in which vids are viewed.

[212] T Tushnet, 5/7/09, at 104-106, and T Coppa, 5/7/09, at 112-114.

[213] *See, e.g.*, *How Much is that Geisha in the Window*, http://www.youtube.com/watch?v=fZr9wsZz_bk.; *see also* R33 (Organization for Transformative Works) at 12-14. *Women's Work* is available on the Organization for Transformative Works' website at http://transformativeworks.org/projects/vidtestsuite. (Last visited 4/30/10.)

[214] *See* Post-Hearing Response of MPAA to Copyright Office Questions relating to DVDs of June 19, 2009, at 3.

for purposes of Section 1201(a)(1), comparable to camcording the screen -- a process that has been identified as a non-circumventing option for accomplishing noninfringing uses.

Particular types of screen capture software discussed at the hearings and in post-hearing questions from the Copyright Office are available for less than $50, significantly less than the costs associated with camcording the screen output. While a record has been established that cost-effective alternative copying techniques, in the form of video capture software, are available for copying portions of CSS-protected DVDs, and while the use of such software may be valuable for some, or even many, noninfringing uses of motion pictures, the record also includes allegations that a substantial number of noninfringing uses could not be adequately accomplished by the use of video capture software or the significantly more expensive alternative of camcording of the screen.[215] The demonstration that the need for high quality video was reasonably necessary to accomplish a particular noninfringing purpose was a critical factor in the 2006 rulemaking proceeding with respect to film and media studies professors. The evidence in the current rulemaking demonstrates that some significant number of noninfringing uses and users would be adversely affected if limited to non-circumventing alternatives. However, not all proponents established a record that alternatives to circumvention would be insufficient to accomplish the pedagogical purpose of the use.

Educational Uses of Motion Pictures. Educators in various fields demonstrated that video capture software produces pixilated output that reduces the overall video quality and, in some cases, may obscure the particular point to be made by the educator.[216] Film and media studies educators demonstrated that the inferior quality copies made with video capture software will frustrate the goal of their intended use.[217] In addition to functional problems encountered with the video output, the audio output was also either adversely affected by screen capture software, resulting in poor quality or out-of-sync sound, or was impossible to obtain with some software.[218]

---

[215] *See generally* the Copyright Office's "DVD-related questions" on video capture software and the responses received by the Office to these questions, http://www.copyright.gov/1201/2008/questions/index.html. (Last visited 4/30/10.)

[216] *See, e.g.*, Post-Hearing Response of American Association of Law Libraries/Medical Library Association and Special Libraries Association to Copyright Office Questions relating to DVDs of June 19 and 22, 2008, at 2-3.

[217] *See* T Decherney, 5/6/09, at 233-235 and 245-246.

[218] *Id.* It is possible that the complete inability to capture the sound of a motion picture might have been avoided if the hardware acceleration on the host personal computer had been turned off, but the evidence demonstrates that even with such an adjustment to the hardware, the sound quality would continue to be distorted.

The importance of sound quality to some educators, such as language instructors who seek to demonstrate nuanced inflections, demonstrates that the use of video capture software is not a viable alternative for a substantial number of noninfringing users.[219]

For the most part, opposition to the proposed classes was aimed at any expansion beyond the scope of the existing class of works. The record in the current rulemaking continues to support the need for for film and media studies professors in higher education settings to circumvent access controls in may instances. A critical question is whether video capture software is an acceptable substitute for the intended noninfringing uses by other educators, as well as documentary filmmakers and noncommercial, transformative creators. To the extent that this software reasonably enables the noninfringing use, a broadening of the scope of the existing class might not be warranted.

Some proponents argued for expansion of the existing class to include all college and university educators, students in film and media studies courses, and students in any college and university course, as well as teachers and students in the K-12 educational environment. While there was some evidence that college and university professors and students have been, or are likely to be, adversely affected by the inability to circumvent, a comparable case was not made by teachers and students in the K-12 context. This assessment was corroborated by NTIA's evaluation of the record.[220]

Proponents of an expansion of the class to include college and university professors provided a number of specific examples that illustrated the need to designate an expanded class. For instance, one proponent noted that a large portion of materials used in college and university courses outside of film studies classes are subtitled, and degradation of the output can affect the legibility of these subtitles.[221] Similarly, foreign language instruction classes use scenes from motion pictures in order to understand and differentiate between sounds and also to observe gestures and facial expressions.[222] Degraded audio and video quality will adversely affect the educational purpose of the use of the clip. Another witness cited a college criminal justice teacher

---

See T De Kosnik, 5/1/09, at 60-61.

[219] *See* T Kaiser, 5/1/09, at 21-26.

[220] *See* NTIA Letter at 4-7.

[221] *See* T Handman, 5/1/09, at 49.

[222] *See* T Kaiser, 5/1/09, at 49.

who noted that teaching police officers involves observational skills that can be developed by performing clips from motion pictures for classroom observation and discussion.[223] One proponent pointed to the need for close observation of particular aspects of scenes in the course of legal and medical education.[224] The evidence did not demonstrate that every use of motion pictures in a classroom requires the circumvention of CSS-protected DVDs.[225] Compilations of high-quality clips appear to be reasonably necessary for some pedagogical purposes in colleges and universities, but in other cases, moderate quality reproductions appear to be sufficient or high quality presentations may be rendered in non-circumventing ways. For instance, in some cases, professors needing to perform only one clip in a class may be able to use the CSS-protected DVD itself in a DVD player by cuing the scene up before class. In other situations, video capture software appears to be sufficient in order to make the pedagogical point.[226] For example, one proponent of an expanded educational class stated that his use of WinTV2000 was important to his educational goals in the classroom.[227] However, this software appears to be video capture software that records screen output. The record demonstrates that while a number of noninfringing uses may reasonably require higher quality than is available from video capture software for the particular pedagogical purpose of the use, in some (probably a much greater) number of classroom situations, compilations created through the use of video capture software are sufficient to accomplish the intended purpose of the use.

In contrast to the record for college and university professors, there is little evidence that college and university students (other than those students in film or media studies classes) or K-12 teachers and students need to use enhanced quality copies of DVD content. Although students in college and university courses may, on occasion, need to create class projects or assignments that create compilations of clips from motion pictures, there has been no factual demonstration of

---

[223] T Band, 5/6/09, at 123-124.

[224] T Skalbeck, 5/6/09, at 166-167.

[225] The record evidence did not show that all of the uses identified above necessarily require circumvention. Further, it is not clear to the Register that the use of video capture software would not be adequate for at least some of those uses.

[226] *See* T Rife, 5/6/09, at 187-188, stating that she would use Camtasia software for creating compilations of clips for the classroom if she would not be violating the law. Camtasia is video capture software (referred to as "screen recorder software" by its distributor, TechSmith) and appears to operate in the same manner as the non-circumventing video capture software demonstrated at the hearings.

[227] *See* R13 (Frank Baker) at 1 (discussing the importance of using clips to demonstrate the "techniques of persuasion" in commercials). Despite the fact that CSS-protected DVDs do not appear to be the source of most commercials, this comment is instructive for the educational benefits of non-circumventing alternatives.

such a need or the likelihood of such a need for the ensuing three-year period. Moreover, to the extent that such a need is likely to exist, there has been no evidence introduced that alternatives to circumvention, such as the use of video capture software, would be unable to sufficiently accommodate those needs.

As with college and university students, the factual record on the educational need for circumvention by K-12 teachers and students is absent. Although a few proponents generally asserted the need for the extension of the class to include K-12 education,[228] specific evidence of why non-circumventing alternatives were, or would be, insufficient for educational purposes was not demonstrated. The submission of assorted hypothetical situations in which non-circumventing alternatives might not be sufficient for educational purposes did not purport to provide evidence of the prohibition's adverse effect on noninfringing uses, but rather provided speculation about hypothetical situations that could or might be affected if they were attempted.[229] Mere conjecture that a particular use could be affected by the prohibition is insufficient to establish a likelihood of harm. In fact, the record indicates that video capture software resolves many of the problems identified by the proponents of expansion of the class. Video capture software allows teachers and students to use clips from motion pictures released on CSS-protected DVDs for educational purposes when use of the DVD itself would cause teachers to incur excessive classroom time to locate particular scenes. Video capture software also resolves the cost and other problems that were asserted to make camcording of the screen an insufficient alternative for teachers and students.[230] Moreover, by using video capture software, teachers will not have to be concerned about whether they are running afoul of Section 1201; the only legal questions that they must confront are those that have existed since the effective date of the 1976 Copyright Act: (1) is the reproduction a fair use or (2) is the public performance of a lawful reproduction within the scope of Section 110(1)?

Of critical importance to the class proposed by film and media studies professors in the previous rulemaking was the demonstrated need for high-quality portions of motion pictures in order to fulfill a noninfringing purpose. The identification of adverse effects of the prohibition on

---

[228] *See* C4C and 4D (Hobbs); *see also*, T Hobbs, 5/8/09, at 126-127, 129, 132, 135, 263, and 283.

[229] *See* Post-Hearing Response of Jaszi (on behalf of Renee Hobbs) to Copyright Office Questions relating to DVDs of July 10, 2009.

[230] Costs relating to camcording the screen have been addressed, *supra*. Hobbs also stated that the inability to obtain a sufficiently darkened room for a successful camcording session demonstrated that this method was not a viable alternative to circumvention. One can ask whether conducting the camcording after dark would resolve that alleged obstacle.

noninfringing uses must be provided with sufficient specificity to analyze the issue. In this rulemaking, specific examples have been provided on behalf of college and university professors as well as college and university film and media studies students regarding situations in which other alternatives have been or are likely to be insufficient for the intended pedagogical purpose of the use. Such specificity has not been established for college and university students in general, or for K-12 teachers and students. The record in this rulemaking establishes that video capture software is more likely than not to meet the needs of college and university students (other than those in film and media studies classes) as well as K-12 teachers and students. Given the lack of any specific evidence to the contrary, the prposed expansion of the existing class is not justified by the record.

The Register agrees with NTIA that proponents of a class extending to teachers and students in the K-12 setting have not proven their case. However, the Register finds that the same is true with respect to college and university students outside of film and media studies courses. As the Assistant Secretary stated: "proponents persuasively demonstrate that while film and media studies professors have an obvious need to use clips in their instruction, other subject matter instructors at the university level also have a need to use clips to supplement effective instruction."[231] A comparable showing was not made in relation to college and university students generally. Without such proof, the Register does not believe that designating a class of works the direct beneficiaries of which include all college and university students is justified.

The Register is also not convinced that there is sufficient basis to limit the class to DVDs owned by an institution or department library. There appears to be no good reason why a professor who has not lawfully acquired a lawfully made DVD should not be able to use the DVD in order to fulfill his or her pedagogical purpose if the DVD cannot be found in the departmental library or the college or university library. No evidence was introduced to suggest that harm to copyright owners' interests would result from professors' noninfringing uses of lawfully acquired DVDs.

Documentary Filmmakers' Use of Motion Pictures. Documentary filmmakers and noncommercial users have also provided persuasive evidence that non-circumventing alternative means of obtaining portions of DVDs cannot substitute for the decrypted content obtained through circumvention. Documentary filmmakers demonstrated that, for example, FCC requirements demand that the "sync signal, the blanking signal, [and] the color burst signal" be

[231] *Id.* at 4.

within certain specifications that can only reasonably be accomplished with the use of a portion of a motion picture from a decrypted DVD.[232] Documentary filmmakers also note that distributors of their films for theatrical exhibition generally require that the films meet certain quality standards that cannot be met by alternative means of making copies, including video capture software.[233] Thus, neither video capture software nor camcording is a viable option.

Noncommercial, Transformative Users of Motion Pictures. Noncommercial, transformative users have also sufficiently demonstrated that certain uses require high quality in order for the purpose of the use to be sufficiently expressed and communicated. For instance, where focus on background material in a motion picture is essential to the transformative purpose, as exemplified in the situation of bringing the background to the foreground, the use of decrypted DVDs is necessary to make the point.[234] One particular example of "bringing the background to the foreground" was demonstrated in the vid, *How Much Is That Geisha In The Window*, by Lierdumoa. This vid criticizes and comments upon Joss Whedon's science fiction television series *Firefly*. The series incorporates Asian culture and art, but the vid demonstrates that almost no Asian characters are featured and that they appear only in the background. The vid concludes with a text screen that states: "There is only one Asian actor with English dialogue in all of Firefly" and in the next screen states, "She plays a whore."[235] The creator of the vid also argues that "Southern culture, particularly the confederacy is perhaps the *main* thing Joss fetishizes in Firefly. It is a post civil war story from the point of view of the side that lost and all the characters speak in a bastardized Southern dialect."[236]

Moreover, they assert that because noncommercial users typically perform their works on a "lossy" medium such as the Internet, if a transformative user begins with a work of degraded quality, the further degradation that will likely occur in rendering the work to the public can completely obscure the purpose of the use. For instance, *Women's Work*, by Luminosity and Sisabet, assembles short clips from the television series *Supernatural* depicting images of women

---

232 T Morrissette, 5/7/09, at 29-30 and 159-160.

233 T Quinn, 5/7/09, at 15 and T Morrissette, 5/7/09, at 29-40.

234 T Tushnet, 5/7/09, at 104-106 and T Coppa, 5/7/09, at 112-114.

235 *See* http://www.youtube.com/watch?v=fZr9wsZz_bk. (Last visited 4/30/10.)

236 *Id.*

who are "shown only as eroticized, suffering or demonized."[237] In a number of the clips, the images are difficult to see and had this video been made using pixilated video capture, it is reasonably likely that the point of many scenes' inclusion would not be perceptible.[238]

Several vids cited in the record reveal that extensive editing is often performed on the clips reproduced from motion pictures. For instance, in Luminosity's *Vogue*, (using clips from the motion picture *300* to cast the violence in scenes from the movie in an aesthetically modified manner), not only are clips often rendered side-by-side and synchronized, but there is also color and timing modification of the clips used.[239] Other vids also modify the original clips and images, saturating them with color and morphing images into others. For instance, Lim's *This Is How It Works* (using clips from the series *Stargate: Atlantis*)[240] and *Us* (with clips from a long list of movies)[241] both morph and colorize clips to serve the messages of the vids. Although some vids cited do not significantly alter the actual images, the pace of the clips or the focus on a particular part of the clip by the vidder tend to demand clarity of the clips in order to perceive the purpose for inclusion. For instance, in *Closer*, by T. Jonesy and Killa, the vidders present an alternative interpretation of an episode from *Star Trek* in order to hypothesize about the relationship between Captain Kirk and Spock.[242] In *Handlebars*, by Seah and Margie, the vidders examine the Doctor character in the series *Dr. Who*, extracting a multitude of short clips from the series to demonstrate the development of the character while also choosing scenes that fit the lyrics of the song that accompanies the clips.[243] In the course of the character development, the vidders begin whimsically, and then reveal how the smaller exercises of power lead to violence and destruction at the Doctor's hands. This vid criticizes the "moral blind spots by recontextualizing events viewers have already seen."[244] Although some may question the significance of the comment or

---

[237] R33 (Organization for Transformative Works) at 2. *Women's Work* is available on the Organization for Transformative Works' website at: http://transformativeworks.org/projects/vidtestsuite. (Last visited 4/30/10.)

[238] *See id.* For example, one scene depicting a woman being decapitated in the background or another scene depicting a woman being hoisted into the air by a noose would likely not have been perceptible if the quality of the capture was degraded.

[239] *See* http://www.blip.tv/file/2289271. (Last visited 4/30/10.)

[240] *See* http://transformativeworks.org/node/552. (Last visited 4/30/10.)

[241] *See* http://www.blip.tv/file/2286307. (Last visited 4/30/10.)

[242] *See* http://www.blip.tv/file/2289542. (Last visited 4/30/10.)

[243] *See* http://flummery.org/. (Last visited 4/30/10.)

[244] *See* http://transformativeworks.org/node/552. (Last visited 4/30/10.)

criticism at issue in these vids, some comment or criticism is involved that either requires or significantly benefits from the use of high quality reproductions of the clips from motion pictures.

The Register does not take a position on whether each and every use of a clip in vids cited in this section constitutes a noninfringing use. The point of the examples is that frequently when one is engaging in commentary about audiovisual works, it is necessary to use high quality reproductions in order to make one's point.

Authorization from the Copyright Owner as a Substitute for Circumvention. The proponents of a class of works that would permit circumvention in order to use portions of CSS-protected DVDs for comment or criticism in education, documentary filmmaking and noncommercial videos all presented evidence that some of their uses warranted circumvention of CSS in order to accomplish their noninfringing purpose. Opponents of the proposed classes stated that the availability of authorization from the copyright owner is a reasonable alternative to designating a class of works that are not subject to the prohibition on circumvention. For example, one opponent discussed a beta film clip service that seeks to streamline the permissions process, and also introduced letters seeking permission to use works and the responses from the copyright owner.[245] However, there was no evidence demonstrating that it was likely that an efficient permission service covering most motion pictures would be functional in the marketplace during the next three-year period.

Proponents of the class also persuasively argued that permission or authorization was not a viable substitute for the independent ability to make a noninfringing use on a timely basis.[246] The record included responses to requests to use works from copyright owners. These responses revealed why permission often is not an adequate substitute for the ability to make noninfringing use without having to seek permission. For instance, there was evidence in the record that permission may be contingent upon receiving further permission from additional entities for various potential rights.[247] Educators also made the point that in light of the time and effort required to obtain permission, it "would be inefficient and retard the spontaneity of classroom

---

[245] T Aistars, 5/6/09, at 220-221 and 278-283.

[246] Ts Hobbs and Decherney, 5/6/09, at 283-285.

[247] T Aistars, 5/6/09, at 279-281 (conditioning permission on obtaining further permission from the Screen Actors' Guild).

instruction in which professors must respond quickly to student questions and needs."[248] On the present record, permission does not appear to be a viable substitute for designation of a class of works in order to address the prohibition's impact on noninfringing uses.

The record demonstrates that many works available on CSS-protected DVD are not available in unprotected formats and that alternative means of obtaining clips, in a wide range of situations related to the use of CSS-protected DVDs, are insufficient to accomplish the intended use. The lack of alternative formats or alternative means to accomplish the noninfringing uses answers the inquiry under the first factor to be considered by the Librarian in the statutory factors of Section 1201(a)(1)(C). This factor weighs in favor of a designation of an appropriate class of works. This analysis also demonstrates that the prohibition on circumvention is, in a substantial number of cases, having an adverse effect on the ability of users of motion pictures on DVDs to engage in noninfringing uses of those works.

Factor Two

Turning to the second statutory factor, the availability for use for nonprofit archival, preservation, and educational uses, the focus on education is relevant to the proposals relating to educational uses of CSS-protected DVDs. The proponents have demonstrated that motion pictures contained on CSS-protected DVDs are not available for some significant uses by educators and students. CSS-protected DVDs can be accessed in the classroom with the use of widely-available, authorized DVD players, but for the reasons stated above, if professors or film and media studies students need to use multiple high-quality clips from a DVD or portions of high-quality clips from numerous motion pictures for educational uses, it is evident that a substantial number of uses in higher education cannot be achieved by resort to alternative formats or alternative means of copying. However, some educational uses can be achieved without resorting to circumvention. This factor thus weighs in favor of designating a properly tailored class of works for those educational uses in higher education that cannot be accomplished without circumvention.

Documentary filmmakers made the case that "[d]ocumentary films are intrinsically educational in that they purport to tell the truth or document reality, and of course, many documentary films are made specially for use in the classroom setting. Additionally, documentary films are used as teaching tools at all educational levels for a variety of purposes."[249]

---

[248] C4E (Decherney) at 9.

[249] C11B (Kartemquin) at 12.

Section 1201(a)(1)(C)(ii) therefore also weighs in favor of crafting a class of works that includes use in documentary films.

However, this factor does not appear to have any bearing – positive or negative -- with respect to the proposal on behalf of other noncommercial, transformative users.

Factor Three

The third factor, the impact that the prohibition on circumvention has on criticism, comment, news reporting, teaching, scholarship, or research, is a critical factor in the context of the proposals related to CSS-protected DVDs. Most of the uses in the DVD-related proposals involve the adverse effect of the prohibition on criticism, comment, or teaching. Educators have demonstrated that a subset of noninfringing uses of works on CSS-protected DVDs are hampered or precluded as a result of the prohibition on circumvention. Documentary filmmakers have demonstrated that their ability to use motion pictures for purposes of noninfringing criticism, comment or illustration is inhibited by the prohibition. Proponents on behalf of vidders have demonstrated that the creation of noninfringing videos for purposes of comment or criticism can also be adversely affected by the prohibition. The importance of criticism, comment and education in our society, as evidenced by the existence of this statutory factor, strongly weighs in favor of designating a class of works in order to permit circumvention for purposes of enabling the use of portions of motion pictures for noninfringing uses.

Factor Four

The fourth factor, the effect of circumvention on the market for or value of copyrighted works, also weighs in favor of a designating a class. The proponents of a class related to CSS-protected DVDs for education, documentary filmmaking and other noncommercial uses have all placed in evidence the need to use portions of copyrighted motion pictures in certain situations. It is important to add, however, that no proponent has demonstrated the need to circumvent in order to copy a motion picture in its entirety, and no proponent has demonstrated the need to use a quantitatively large percentage of a motion picture. The motion picture industry has a legitimate interest in preventing motion pictures from being copied in their entirety or in a manner that would adversely affect the market for or value of these works, including reasonable derivative markets. Unquestionably, motion pictures involve significant expense to create and have become a vital creative component of American culture. Indeed, motion pictures are so central to modern

American society and the lives of individual citizens that the need to comment upon and criticize these works has become an important form of social discourse. Motion pictures have an enormous influence on our social, political and cultural identity, and the record in this rulemaking illustrates that educators need to teach and demonstrate to students the artistic, communicative and rhetorical capabilities of this medium. The medium is, in some educational situations, the relevant "text" for the class. Similarly, as documentary filmmakers and noncommercial vidders seek to comment or criticize in the motion picture medium, their subject frequently focuses on or includes prior uses of this medium. Each of the uses involving criticism or comment may be transformative, and thereby unlikely to affect the relevant markets for the original work.

The proposed classes, if properly limited in scope to *portions* of motion pictures and for the *purposes* asserted by the proponents (criticism and comment), would not adversely affect the market for or value of these works. The noninfringing, transformative uses that would be enabled or facilitated by designating a properly-fashioned class of works are the kinds of uses that this rulemaking was intended to preserve. Such uses would also preserve such noninfringing uses as a free-speech safeguard in copyright law.

Other Factors

The Librarian is also authorized to take into account other factors that are appropriate in particular circumstances. In the case of CSS-protected DVDs, the fact that a technological measure that controls access is being used predominantly for the purpose of preventing reproduction and other rights of the copyright owner is a relevant consideration in this case. The fact that Congress clearly distinguished between measures that control access and measures that protect the rights of the copyright owner is undisputed. On the record before the Register ten years ago, there was insufficient evidence to draw any conclusions based on this distinction in relation to noninfringing uses of CSS-protected DVDs. Times have changed. The record now demonstrates that socially-beneficial noninfringing uses are being adversely affected by the prohibition on circumvention in relation to certain uses of portions of motion pictures on CSS-protected DVDs. In addition to the other four factors weighing in favor of designating a class of works, the fact that in this case the effect of the access control is not to prevent unauthorized access, but rather to restrict uses of motion pictures, is an additional factor weighing in favor of designating a class. There is no question that digital reproduction poses a serious threat to copyright creators and owners. But the purpose of the rulemaking is to assess whether methods of controlling access to works that fall within the scope of the prohibition are, often unintentionally,

also adversely affecting noninfringing uses. The present record demonstrates that the deployment of CSS over time has begun to adversely affect some legitimate uses of motion pictures. This is presumably an unintended by-product of the use of CSS to protect the copyright owners' legitimate interests, but one that requires a carefully balanced and properly tailored exception to the default prohibition. The fact that a technological measure that qualifies as an access control is affecting use, not access, is another relevant consideration for the Librarian.

Classes of Works Defined and Explained

For the foregoing reasons, the Register recommends that the Librarian designate the following class of works:

> Motion pictures on DVDs that are lawfully made and acquired and that are protected by the Content Scrambling System when circumvention is accomplished solely in order to accomplish the incorporation of short portions of motion pictures into new works for the purpose of criticism or comment, and where the person engaging in circumvention believes and has reasonable grounds for believing that circumvention is necessary to fulfill the purpose of the use in the following instances:
>
> - Educational uses by college and university professors and by college and university film and media studies students;
> - Documentary filmmaking;
> - Noncommercial videos

Except for the educational subset, this recommendation does not specify particular users but rather refines the class by reference to particular uses identified in the record. The Register finds that tailoring the class to the purpose of the use is the optimal means of permitting these users to accomplish their purpose. Documentary filmmakers seek to use portions of motion pictures for criticism or comment, including illustration of a particular point, and it is the use of such portions that the Register has concluded will often be a fair use. The noncommercial videos identified by proponents of proposed Class 11A also often use portions of motion pictures for comment and criticism (including parody). These transformative uses – again involving portions of motion pictures -- are socially beneficial uses that implicate core First Amendment values reflected in the fair use doctrine. Educators' and students' use of portions of motion pictures typically involve criticism (an assessment of a work; considered judgment of or discussion about

the qualities of something, especially a creative work) and comment (discussion, analysis, criticism, explanation or illustration).

The Register sees no workable way to further qualify the class of works for documentary filmmaking and noncommercial videos by including specific requirements relating to the identify of the users who would be permitted to circumvent. While the proponents of the class pertaining to documentary films suggested that persons eligible to take advantage of that class be limited to documentary filmmakers who are members of an organization of filmmakers or are enrolled in a film program or film production course at a post-secondary educational institution, the Register does not believe that it is appropriate to require membership in any particular organization in order to qualify. It makes sense to conclude that the best way to determine whether someone is a documentary filmmaker is to ask whether that person is making a documentary film. Further, noncommercial videos that comment on motion pictures can be made by anyone; fair use does not depend upon the credentials of the person engaging in the noninfringing act.

However, the record is different with respect to the proposed class relating to educational uses. Proponents have not proved that all educational uses of motion pictures on CSS-protected DVDS have been adversely affected by the prohibition on circumvention. Moreover, clear dividing lines are available for certain classes of users in the educational context that are not available with respect to documentary filmmakers or noncommercial transformative users. College and university professors can easily be distinguished from K-12 teachers, and college and university film and media studies students can easily be distinguished from other college and university students, as well as from K-12 students. The recommended class expands upon the existing class in a manner that comports with the evidence introduced in this rulemaking proceeding. Although not all educators will directly benefit from the designation of this class, the clarified status of video capture software is likely to benefit all educators, including those who cannot benefit from the recommended class, in their ability to make non-circumventing, noninfringing uses of motion pictures on CSS-protected DVDs. If such alternatives are demonstrated to be insufficient for educators or students who cannot take advantage of the newly-designated class, the Register assumes that evidence to that effect will be introduced in future rulemaking proceedings.

The scope of the class is appropriately tailored in relation to the cases that were made for designating a class of works. For instance, only those uses that involve creating new works (including compilations) that are for specific, transformative purposes that can rather easily be

identified objectively (namely, criticism and comment) are within the scope of the class. Those who circumvent CSS for the purpose of copying a portion of a motion picture for exploitation of that portion, or for marketing purposes, rather than for the purposes identified in the designation of the recommended class, will not qualify to invoke the Section 1201(a)(1)(D) exemption. Those who circumvent in order to extract portions of a motion picture purely to entertain also fall outside of the exemption. Similarly, extensive use of a work will also fall outside of the exemption. Even though it is possible that the use of a significant portion of a work may in some cases qualify as a fair use, the record does not demonstrate that the use of large amounts of a feature-length motion picture are, or are likely to be, needed to serve the goals of criticism, comment and education in the contexts presented in this rulemaking. The fact that whole works may be used in the classroom even with CSS intact (*i.e.*, under the Section 110(1) exemption by using a DVD player) eliminates the need for an expansive class. Documentary filmmakers and noncommercial users have not demonstrated that either the use of a significant amount of a motion picture is noninfringing in their respective contexts, or that a significant amount is typically used in their works. The cases they made in this proceeding did not purport to suggest that there is a legitimate need to use substantial portions of a motion picture in their work.

Limiting the class by reference to the purposes of criticism and comment protects owners of copyrights in motion pictures from nontransformative uses that merely exploit their works for commercial or predatory purposes. Limiting the permitted uses to "short portions" bolsters the limitation based on the nature of the use, and tends to eliminate from the scope of the Section 1201(a)(1)(D) exemption uses that are more likely to be infringing. As noted above in the discussion of the third fair use factor, the examples presented in the record consist of uses of short portions; the record does not support designation of a class that would extend to anything beyond use of short portions. Moreover, without limiting the class to permit use only of a portion of the work, the use of entire feature length motion pictures would be sanctioned. Because the current record does not demonstrate a present or likely need for circumvention beyond short portions of a work, such a limitation is appropriate. While a different record in the future could lead to a different result, the current record demonstrates only that the prohibition on circumvention has had an adverse effect on the ability to use short portions of the feature length film or of some of the other extra content, such as interviews and outtakes contained on a DVD, for the purposes of criticism and comment. The use of technology to prevent piracy is consistent with the purpose of the DMCA and a class of works designated under Section 1201(a)(1)(C) must be tailored to balance the respective interests of affected parties. The Register believes that the recommendation accomplishes this goal.

Another limitation is that the person engaging in the circumvention must believe and have reasonable grounds for believing that circumvention is necessary in order to fulfill the purpose of the use – *i.e.*, the purpose of criticism or comment. This qualification is included in order to provide some degree of assurance that the designation of this class may not be used as a pretext for circumvention in cases where circumvention was not really necessary in order to engage in the noninfringing use. If, for example, it would have been sufficient for purposes of the noninfringing criticism or comment to use screen capture software rather than to circumvent in order to obtain a higher quality digital film clip, and if the person engaging in the circumvention did not both (1) actually and (2) reasonably believe that circumvention was necessary in order to engage in such criticism or comment, the prohibition on circumvention would remain in force. This might be the case, for example, when the somewhat inferior copy made using screen capture software would be perfectly adequate for purposes of demonstrating a point being made about the story line of a motion picture.

The recommended class is also based on motion pictures and intentionally does not extend to all audiovisual works. Section 101 of title 17 defines motion pictures as follows:

> "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.[250]

Section 101 defines audiovisual works as follows:

> "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.[251]

"Motion pictures" are a subset (albeit a very large one) of "audiovisual works." All of the uses identified in the record relating to CSS-protected DVDs involved motion pictures, such as feature films, television series episodes, interviews, commercials, trailers, etc. All involve related images shown in succession that impart an impression of motion. No evidence was introduced in relation to audiovisual works outside of the subset of motion pictures, such as video games or

---

[250] 17 U.S.C. § 101.

[251] *Id.*

slide presentations. Based on the record, there is no basis for extending the class beyond that of motion pictures.

The Register also notes the objection by the Joint Creators that the designation of a class of works that is defined with reference to the nature of the use or user is a deviation from statements made by the Register in earlier recommendations.[252] As the Register has stated above, a class of works must begin with a category, categories, or a subcategory of copyrightable subject matter and then refine that starting point based on the facts present in the record. As the House Manager's Report stated:

> Deciding the scope or boundaries of a 'particular class' of copyrighted works as to which the prohibition contained in section 1201(a)(1) has been shown to have had an adverse impact is an important issue to be determined during the rulemaking proceedings. The illustrative list of categories appearing in section 102 of Title 17 is only a starting point for this decision.[253]

In all cases, the scope of a class is determined on the basis of the rulemaking record during a particular three-year period. Attributes of a class are generally incapable of being circumscribed in a factual vacuum. While the Register continues to believe that a class of, for example, "motion pictures for non-infringing purposes" or "fair uses of motion pictures" would not constitute an appropriate class, the relationship between the "class of works" and the particular non-infringing uses that were proven to be, or likely to be, adversely affected may be, in certain cases, the optimal means of balancing the interests identified in the record. Similarly, the Register believes that circumscribing a class by a long laundry list of limitations is also inappropriate in a factual vacuum.[254] While one or many conditions *may* be appropriate in a particular factual situation, a comprehensive list of limitations is inappropriate as a general proposition.

The Register refined the designation of a class in 2006 as a result of the unique facts presented in that particular rulemaking. That refinement was not a generalized change to the nature of a class of works, but a careful attempt to designate a class that was neither too broad nor

---

[252] *See* Post-Hearing Response of MPAA to Copyright Office Questions relating to DVDs of August 21, 2009, at 8-12.

[253] House Manager's Report at 7.

[254] *See* Post-Hearing Response of MPAA to Copyright Office Questions relating to DVDs of August 21, 2009, at 10-12.

too narrow.[255] In the current context, if refinement of the class in relation to the nature of the particular use were unavailable, the class might have been designated to be "motion pictures on CSS-protected DVDs." An exemption of such breadth would allow circumvention for many uses that were not presented in the record of this rulemaking and presumably would draw much stronger objections from opponents of the proposed classes than the more carefully crafted class recommended herein. The Register will continue to assess the scope of a class in relation to each particular proposal and the market context in which that proposal is raised. As Congress indicated, determining the scope of the class is a critical component of the examination in the rulemaking process and the Register will consider any arguments about the appropriate means of crafting the scope of a particular class.

B. Computer programs that enable wireless telephone handsets to execute software applications, where circumvention is accomplished for the sole purpose of enabling interoperability of such applications, when they have been lawfully obtained, with computer programs on the telephone handset.

Background. Mobile phones have evolved from relatively simple communication devices into increasingly sophisticated, advanced computing devices with the capability to run a variety of applications and perform or display numerous types of copyrighted works. These "smartphones"[256] have, in today's society, begun to supplant laptops as the predominant mobile device due to their portability, cost, and increasing computing capacity.[257] Devices, such as Apple's iPhone, allow users to make wireless phone calls, write and receive text messages, browse the Internet, read and send e-mail, run operating system and application programs, display images, photographs, and documents, store and display or perform ebooks, music and motion pictures. The iPhone, in particular, has created a robust environment on which third-party programmers can create applications for use on that device. According to the testimony in this

---

[255] House Manager's Report at 7.

[256] Smartphones are mobile phones with advanced data features and keyboards. What makes the phone "smart" is its ability to manage and transmit data in addition to voice calls. *See* CTIA Wireless Glossary of Terms, http://www.ctia.org/consumer_info/index.cfm/AID/10406. (Last visited 4/30/10.) In the second quarter of 2009, 28% of all handsets sold were smartphones. *See* Letter from Christopher Guttman-McCabe, Vice President, CTIA, to Marlene H. Dortch, Secretary, FCC, February 12, 2010, http://files.ctia.org/pdf/filings/100212_Wireless_Competition_Update_-_Innovation_and_Investment_FINAL.pdf. It is important to recognize that not all mobile phones in today's wireless marketplace are smartphones as some are designed simply to provide voice service.

[257] *See* Mark Hamblin, *Businesses Eye Smartphones to Supplant Laptops*, PCWorld, November 23, 2008, at http://www.pcworld.com/article/154377/businesses_eye_smartphones_to_supplant_laptops.html. (Last visited 4/30/10.)

proceeding, as of May 1, 2009, there were over 35,000 authorized applications available for the iPhone on Apple's App Store, making it the world's largest application marketplace.[258]

Apple, as well as several other mobile phone manufacturers, have allegedly placed restrictions on which particular third-party applications can be used in conjunction with a particular device. Despite the fact that proponents have alleged that a number of manufacturers (or, in some cases, providers) impose technological restrictions on interoperability between third-party applications and the operational programs resident on the devices themselves, the vast majority of the record in this rulemaking relates to one particular device and its restrictions—the Apple iPhone.[259] In part, this is the result of the Apple iPhone becoming the best selling mobile phone handset in the United States.[260]

Comments. EFF proposed an class of works to allow circumvention of the technological measures that prevent third-party software applications from being installed and run on wireless telephone handsets. The Apple iPhone is used by EFF to illustrate its argument that the prohibition on circumvention is adversely affecting non-infringing uses by smartphone users. EFF states that Apple uses technological measures "to prevent iPhone owners from loading or executing applications unless they are purchased from Apple's own iTunes App Store or otherwise approved by Apple."[261] Apple's testimony confirmed that any software to be used on the iPhone must begin with the firmware, in this case, the read-only memory, or "ROM," in the hardware,[262] which contains information necessary for starting up the iPhone.[263] The secure ROM contains "crypto keys" that validate and establish a "root of trust" necessary to load the

---

[258] T Joswiak, 5/1/09, at 231.

[259] Some evidence was introduced in the record regarding other smartphones, such as the G1 phone from T-Mobile (with Google's Android operating system) and the Nokia 2366i from Verizon. *See* C5A (EFF) at 6 and R19 (Hallett) at 1. The lack of development in the record precludes an analysis of these examples.

[260] R49 (EFF) Appendix A: "A Technical Overview of Smart Phone Jailbreaking and Unlocking," at 10.

[261] C5A (EFF) at 4.

[262] Firmware can be identified as a microprogram present on read-only memory ("ROM") modules, containing low-level (hexadecimal machine code) software. *See* http://www.topbits.com/flashing-firmware.html. (Last visited 5/1/10). For purposes of this discussion, firmware may be defined as a "computer program contained permanently in a hardware device (as a read-only memory)." *See* http://www.merriam-webster.com/dictionary/Firmware. (Last visited 4/30/10.)

[263] T Joswiak, 5/1/09, at 234.

"bootloader" program.[264] The bootloader contains the information necessary for initializing the hardware and the hardware's operating system, a modified version of Apple's OS X.[265] The iPhone operating system "does everything necessary to run the iPhone, as well as validate each of the applications through a signature each time they're launched."[266] This chain or "root of trust" is intended "to make it impossible for users to substitute their own software for Apple's at any point in the process; even if they can somehow change the code installed on the phone, the signature checking is intended to prevent the modified software from running."[267] Despite this validation process, a very large number of purchasers of iPhones have circumvented these restrictions, a practice colloquially referred to as "jailbreaking," in order to install third-party applications that have been rejected by Apple for inclusion into its "Apps Store."[268]

EFF argued that jailbreaking is a non-infringing activity for three reasons. First, it alleges that at least in some cases, jailbreaking can be done within the scope of what is authorized under the licence Apple grants to every iPhone user. It states that "[t]o the extent a jailbreaking technique does not modify any of the individual software programs that comprise the iPhone firmware collection, but instead simply adds additional software components to the collection, the practice may not exceed the scope of the license to 'use the iPhone software' or constitute a 'modification' of any Apple software components, any more than the addition of a new printer driver to a computer constitutes a 'modification' of the operating system already installed on the

---

[264] *Id; see also*, R49 (EFF) Appendix A: "A Technical Overview of Smart Phone Jailbreaking and Unlocking," at 10-11("The process begins with the bootrom, software burned into the iPhone's permanent, nonvolatile memory. The bootrom loads a piece of software called the LLB, which is stored in an area of memory known as NOR flash. The LLB then loads a piece of software called iBoot, performing a digital signature check to ensure that iBoot software has not been modified. iBoot then loads the operating system kernel, performing a digital signature check to ensure that operating system software has not been modified. The operating system kernel then loads and manages all other "userland" applications (essentially, all the applications that users interact with), performing a digital signature check to ensure that the applications have been approved by Apple and have not been modified.")

[265] T Joswiak, 5/1/09, at 234. OS X is the operating system that is used to run many Apple computers and laptops

[266] *Id.*

[267] R49 (EFF) at 11.

[268] EFF asserted that approximately 1.8 million iPhones have been jailbroken, constituting roughly 10% of the iPhones in circulation. Of these 1.8 million jailbroken phones worldwide, approximately 400,000 are located in the United States. *See* T von Lohmann, 5/1/09, at 245.

computer."[269]

Second, EFF asserted that "to the extent a jailbreak technique requires the reproduction or adaptation of existing firmware beyond the scope of any license or other authorization by the copyright owner, it would fall within the ambit of 17 U.S.C. § 1l7(a)."[270] EFF contended that the iPhone owner is also the owner of the copy of the iPhone's firmware and that jailbreaking falls within the owner's privilege "to adapt those copies to add new capabilities, so long as the changes do not "harm the interests of the copyright proprietor."[271]

Finally, EFF contended that in any event, jailbreaking constitutes fair use of the firmware because jailbreaking is a purely noncommercial, private use of computer software, a largely functional work that operates the phone, and that the phone owner must reuse the vast majority of the original firmware in order for the phone to operate. Because the phone owner is simply modifying the firmware for her own use on the phone, there is no harm to the market for the firmware.

Apple responded that jailbreaking by purchasers of the iPhone is a violation of the prohibition against circumvention of access controls. It cited that its validation system is necessary to prevent: (1) crashes and instability: jailbroken iPhones crash more frequently and become unstable; (2) malfunctioning and safety: battery life, safe charging capacity and volume control can all be affected (3) invasion of privacy: the data, camera, microphone and GPS functions of the iPhone can be exploited by third-parties; (4) exposing children to age-inappropriate content: the App Store filters content made available to users, but jailbreaking allows age-inappropriate content to be installed; (5) viruses and malware: without a secure environment, it is easier for malicious code to be injected into the iPhone "ecosystem;" and (6) the inability to update software: a jailbroken phone might prevent Apple software updates from

---

[269] C5A (EFF) at 8. EFF noted that the iPhone license permits the user to "use the iPhone Software on a single Apple-branded iPhone," but also obligates the iPhone owner not to "decrypt, modify, or create derivative works of the iPhone Software." *Id.* The Register declines to interpret the license to determine whether it permits jailbreaking.

[270] This provision provides that "it is not an infringement for the owner of a copy of a computer program to make or authorize the making of another copy or adaptation of that computer program provided: … that such a new copy or adaptation is created as an essential step in the utilization of the computer program in conjunction with a machine and that it is used in no other manner."

[271] *Id.* at 8-9.

loading and installing.[272] Apple also cited the risks and damage that can occur with its developer partners when the iPhone ecosystem is compromised, including: network impact, piracy of developers' applications, and the instability of developers' applications. Jailbreaking is also claimed to harm Apple's goodwill with its customers, increase Apple's support costs, harm developer relationships, damage Apple's brand, and limit its ability to innovate.[273]

Apple further contended that modifying Apple's operating system leads to the creation of an infringing derivative work. In Apple's view, an iPhone purchaser's interest in adding applications that are not approved by Apple to an iPhone constitutes an infringing act and therefore the prohibition is not adversely affecting non-infringing uses when it prevents such conduct. Apple further argued that there are no defenses to infringement that transform jailbreaking into a non-infringing act. First, it argued that Section 117 is inapplicable in relation to purchasers of an iPhone because they are licensees of the computer programs contained on the phone, not owners of copies of the computer programs as Section117 requires. Apple also asserted that "the adaptation right of Section 117 can be negated by contract," and that the iPhone software license forbids modification of the iPhone software.[274] It also argued that Section 117 does not apply when, as here, the modifications to the computer program are created by others and then downloaded by end-users. Rather, the modifications must be made by the end-user or at least authorized by the end user. Apple also argued that although Section 117 "allow[s] a user of a computer program to add new features to it," that permission is "subject to a number of limitations," including the limitation that "the right to add features can 'only be exercised so long as they [do] not harm the interests of the copyright proprietor,'"[275] and that jailbreaking does harm Apple's interests because it causes functional problems that diminish the value of the iPhone and the software that makes it operate.[276] Finally, Apple argued that because Section 117 permits modifications to software only as an essential step in the utilization of the computer program in conjunction with a machine and "in no other manner," and since jailbreaking entails the use of the iPhone and its software in a way that destroys its operational integrity, the "[u]se of these copyrighted programs in a jailbroken phone is therefore use 'in another manner' that is not

---

[272] T Joswiak, 5/1/09, at 236-239.

[273] *Id.* at 240-242.

[274] R30 (Apple) at 13-14.

[275] *Id.* at 14, citing *Krause v. Titleserv, Inc.*, 402 F.3d 119, 129 (2d Cir. 2005), *cert. denied*, 126 S. Ct. 622 (2005).

[276] *Id.* at 15-16.

covered by Section 117(a)."[277]

Second, Apple argued that the defense of fair use would not apply to this activity. Reviewing the fair use factors set forth in Section 107, it pointed out that "although the use *per se* of the modified iPhone bootloader and OS on an individual handset is of a personal nature, it is not a transformative use, and because a jailbroken OS is often used to play pirated content, such activity should be considered of a commercial nature since it avoids paying fees for the content." It argued that the second and third factors weigh against fair use "because the copyrighted works at issue are highly creative and not factual in nature, and essentially the entire work is being copied." With respect to the fourth factor, it asserted that "the effect of these unauthorized uses is to diminish the value of the copyrighted works to Apple." It elaborated by stating that "jailbreaking the bootloader and the OS clearly diminishes the value of those copyrighted works directly by giving rise to a host of problems in the safety, security and operation of the iPhone, and by substantially increasing Apple's costs to support the software." [278]

EFF contended that the protection system implemented by Apple is unrelated to copyright interests, but rather is a business model decision to prevent competition.[279] Similarly, in testimony, Charles Carreon stated that protecting access to a copyrighted work is not Apple's goal, but rather the purpose is to prevent interoperability with the device. In other words, proponents of the proposed exemption believe that Apple's goal is not to prevent reading, viewing, comprehension, understanding, or modification of creative content, but rather to prevent execution, use, and functional modification of the binary code.[280]

Discussion. In order to meet their burden in favor of an exemption, proponents must first show that the prohibition is adversely affecting, or likely to have an adverse effect on, non-infringing uses. This, in turn, entails two distinct considerations. First, for the prohibition to be causally related to the adverse effect, a technological measure controlling access must be protecting a copyrighted work. Second, the proponents must demonstrate that the prohibition is adversely affecting, or likely to adversely affect, a non-infringing use.

---

[277] *Id.* at 17.

[278] *Id.* at 17-18.

[279] *See* R49 (EFF) at 6. Apple requires developers to pay a 30% commission on any sales through the App Store and refuses to authorize applications that "duplicate functionality" offered by Apple's own software or AT&T's services. C5A (EFF) at 5-6.

[280] T Carreon, 5/1/09, at 283-284.

1. *The nature of the technological measure*

During the hearings, there was some dispute about the nature of the technological measures employed on the iPhone. Counsel for Apple argued that access controls simply prevent one from gaining access to a work without authorization from the copyright owner. In contrast, the system Apple employs does more than this—it is designed to prohibit modification of the operating system and thus the measures that Apple employs are "essentially, quintessentially copy controls."[281] Despite the fact that the purpose of Apple's system of authentication is intended to prevent any modification of the operating system, the evidence in the record demonstrates that the operation of iPhone software is protected by encryption which requires authentication by cryptographic keys loaded into the bootloader which, in turn, authenticates the iBoot program and the integrity of the operating system. This system of authentication and decryption meets the statutory definition of a technological measure that effectively controls access to a work because, in the ordinary course of its operation, the technological protection measure requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work. In order to obtain access to the operating system that runs the iPhone, the application of a particular process is required. While it is true that this authentication process seeks to verify that modifications have not been made to the iBoot program or the operating system program, the process denies access to the operating system if the process discovers that modifications have been made. This access control may also protect certain rights of the copyright owner in the course of effectively controlling access.

Apple ultimately admits that the technological measures on the iPhone are "both copy controls and access controls" and include encryption.[282] And, encryption is a classic form of access control.[283] That admission makes Apple's point that this process is fundamentally a copy control, not an access control, more or less moot. To the extent that the technological measures on the iPhone are access controls – and both EFF and Apple appear to agree that they are, at least in part, they are properly a subject of this rulemaking proceeding. To the extent that they are also

---

[281] T Hayes, 5/1/09, at 266. Apple's written comment made no such argument and appeared to accept the characterization of the technological measures on the iPhone as access controls.

[282] *Id.* at 296.

[283] *See* 17 U.S.C. § 1201(a)(3)(A) (defining, in the context of Section 1201(a), to "circumvent a technological measure" as "to descramble a scrambled work, to decrypt an encrypted work," etc.). *See also,* Commerce Comm. Report, at 39, 40 (characterizing encryption as an access control).

technological measures that protect a right of a copyright owner, there is no prohibition on the conduct of circumvention in the statute. Section 1201(b) only prohibits the manufacture, importation, offering, provision, or trafficking of technology, processes, services, devices or components that circumvent a technological measure that protects the right of a copyright owner; it does not make it unlawful to use such a tool or service in order to circumvent. A suit may be brought against the entity trafficking in a device or service that facilitates circumvention of a measure that protects a copyright owner's rights, but no suit may be brought under Section 1201(b) against someone who uses such a tool to circumvent such a technological measure. Of course, if the user of the circumvention tool circumvents in order to engage in infringement, the copyright owner may file an infringement suit, but if the user circumvents in order to engage in a non-infringing act, the user is not liable for any act under title 17.

In the case of the Apple iPhone, because the authentication process constitutes a technological measure that effectively controls access, Section 1201(a)(1) would prohibit its circumvention, including the use of a tool to circumvent. Thus, if no statutory exemption in Section 1201 is applicable, the only means of avoiding liability under the prohibition in order to accomplish a non-infringing use is through this rulemaking proceeding. The next critical step in the analysis is to determine whether technological measures controlling access on the iPhone are adversely affecting a non-infringing use or uses. Before resolving that question, however, a potentially relevant statutory exemption may warrant consideration.

Apple and other opponents of the proposed class[284] argue that the activity sought to be accomplished by proponents of the class falls within the realm of reverse engineering for which Congress enacted a specific statutory exemption.[285] It is true that the activity sought to be accomplished *relates to* making independently created computer programs (here, third-party applications) interoperable with Apple's modified OS X operating system on the iPhone. However, iPhone owners do not seek to reverse engineer their phones in order to install interoperable, unapproved applications on their iPhone. They seek to use a tool that enables unauthorized applications to run on the iPhone. In other words, users seek to circumvent the access control in order to install the programs with the assistance of a previously created tool, device, or program that enables such installation and operation.

Section 1201(f) may in some cases be a defense to the manufacture and distribution of

[284] *See, e.g.*, R46 (Joint Creators) at 36-38.

[285] *See* R30 (Apple) at 2 and 25.

such tools or programs. Section 1201(f) exempts not only the act of circumvention for the purpose of reverse engineering to identify and analyze those elements of a computer program that are necessary to achieve interoperability of an independently created computer program with other programs, but it also exempts liability under Sections 1201(a)(2) and 1201(b) for circumvention in order to develop and employ technological means to circumvent under certain conditions as long as such activity does not constitute infringement under title 17.[286] Moreover, Section 1201(f)(3) allows disseminating the information acquired about achieving interoperability and "the means permitted under paragraph (2)" to be made available to others.[287] Such activities are outside the scope of this rulemaking, and they are not the activities for which an exemption is sought. Thus, Section 1201(f) does not appear to limit the liability of smartphone owners who jailbreak their devices in order to add software applications not authorized by the device manufacturer or service provider.

This rulemaking is the appropriate forum to address whether an exemption to the prohibition is warranted as a result of the adverse effects on non-infringing uses. The question before the Register is whether purchasers of smartphones have been adversely affected in their ability to make noninfringing uses. The non-infringing use alleged is the purchasers' ability to add independently created computer programs to their phones.

The evidence supports the contention that a technological measure is adversely affecting adding applications to the iPhone. The evidence in the record suggests that approximately 350,000 iPhone owners have jailbroken their iPhones to load applications from one independent app store alone.[288] The record tends to indicate that the total number of jailbroken iPhones is significantly higher, constituting up to ten percent of all iPhones sold.[289] Given the scale of Apple's iPhone market, this effect must be accepted as substantial in relation to the smartphone market.[290] Although the vast majority of the evidence relates solely to the iPhone, that showing combined with the anecdotal evidence relating to other smartphones establishes an effect on use

---

[286] 17 U.S.C. § 1201(f)(2).

[287] 17 U.S.C. § 1201(f)(3).

[288] C11A (EFF) at 5, citing Erica Sadun, *The story behind Cydia on the iPhone*, Ars Technica, at http://arstechnica.com/apple/news/2008/10/the-story-behind-cydia-on-the-iphone.ars. (Last visited 4/30/10.)

[289] T von Lohmann, 5/1/09, at 245.

[290] R49 (EFF) Appendix A at 10 (noting that iPhone has become the best selling handset in the United States).

that is more than merely trivial or anecdotal. The next question to resolve is whether this desired use is non-infringing.

2. *The nature of the underlying use*

The critical determination in considering this proposed class, and the one over which the greatest controversy has been generated in the record, is whether the modification of the Apple software in order to enable interoperability with independently created computer programs is a non-infringing use. EFF argues that this activity is non-infringing under Section 117(a) or, alternatively, under Section 107.

a. Section 117

Section 117(a) states:

> Notwithstanding the provisions of section 106, it is not an infringement for the owner of a copy of a computer program to make or authorize the making of another copy or adaptation of that computer program provided:
>
> (1) that such a new copy or adaptation is created as an essential step in the utilization of the computer program in conjunction with a machine and that it is used in no other manner, or
>
> (2) that such new copy or adaptation is for archival purposes only and that all archived copies are destroyed in the event that continued possession of the computer program should cease to be rightful.[291]

In the case of the iPhone, the new copy or adaptation created is the new copy or modification of Apple's bootloader and/or operating system in the device. iPhone owners would need to modify the bootloader and/or operating system in order to run applications of their choice. The making and use of that new copy or adaptation of the firmware is alleged to be "an essential step for the utilization of the computer program" that would allow adding new applications to the iPhone.[292] The pivotal questions in relation to Section 117(a) turn on: (1) whether the iPhone purchaser is an owner of a copy of the computer program, or is merely a licensee of a copy, and (2) whether the adaptation is an essential step in the utilization of the program in conjunction with

[291] 17 U.S.C. § 117(a).

[292] *See* T von Lohmann, 5/1/09, at 256.

a machine.

EFF argued that the purchaser of an iPhone is the owner of a copy of any computer program embedded in the hardware. It did not dispute that Apple retains ownership of the copyright in the "computer programs" for the bootloader, the operating system, or any other computer programs created by Apple that reside on the iPhone. In other words, EFF agreed that Apple owns the "work." But the particular "copy" of the computer program is bundled with the iPhone hardware. The copy of the software is necessary to make that hardware function, is purchased as part of the single price of the iPhone, and may be retained perpetually. EFF argued that regardless of what Apple calls the transaction, the purchaser as a practical matter owns the phone and the copies of the computer programs residing on that hardware.[293]

Apple's end-user license agreement states that the user owns the media on which the software resides, but Apple retains ownership of the software. Apple argued that this provision means that a purchaser owns the hardware, but is only licensed to use the software in the prescribed manner.[294] Proponents responded that the software is fixed on the hardware. A copy is the tangible manifestation of the intangible copyrighted work. If the user owns the hardware, they reason, then the user necessarily also owns the copy of the program.[295] Apple may retain ownership of the intangible work, the software, but does not own the media on which the software is fixed. EFF asserted that the iPhone Software License Agreement confirms this point.[296]

Apple contended that the license agreement demonstrates that the owner of an iPhone is simply a licensee of the copy of the computer programs on the phone and that as a licensee, Section 117(a) is inapplicable. In other words, Apple asserted that a licensee, as distinguished from an owner of a copy, has no right to make a modification of the computer program and is prohibited by the terms of the license from adapting the program. Therefore, any such unauthorized modification is an infringing derivative work. In Apple's view, because there is no underlying non-infringing use established by the proponents, there is no basis for an exemption. If the underlying use is infringing, the prohibition is not adversely affecting a non-infringing use,

---

[293] C5A (EFF) at 8-9.

[294] *See* Post-Hearing Response of Apple to Copyright Office Questions relating to iPhone modification of June 23, 2009, at 3-4.

[295] T Carreon, 5/1/09, at 286.

[296] C5A (EFF) at 8.

but is simply preventing an infringing use.[297]

Apple and EFF both provided separate interpretations of the Software License Agreement that accompanies each sale of an iPhone.[298] Not surprisingly, they disagreed as to whether the effect of that agreement is to vest ownership of the copy of the software in the purchaser of the iPhone or in Apple. The answer does not turn solely on the characterization of the transaction in the contract. Several courts have held that in addition to assessing formal title, it is also necessary to look to the incidents of ownership in order to determine whether the transaction is in fact a transfer of ownership or a license. Both Apple and EFF agreed that the recent decision from the Second Circuit in *Krause v. Titleserv*[299] is "good law." Each also believed that the case supports its respective position.[300]

In *Krause*, the Second Circuit concluded that rather than looking to formal title as an "absolute prerequisite to qualifying for § 117(a)'s affirmative defense … [i]nstead, courts should inquire into whether the party exercises sufficient incidents of ownership over a copy of the program to be sensibly considered the owner of the copy for purposes of § 117(a). The presence of formal title may of course be a factor in this inquiry, but the absence of formal title may be outweighed by evidence that the possessor of the copy enjoys sufficiently broad rights over it to be sensibly considered its owner."[301]

---

[297] *See* Post-Hearing Response of Apple to Copyright Office Questions relating to iPhone modification of July 13, 2009, at 1-2.

[298] Apple has explained that there have been, over time, four different versions of the Agreement. Apple has provided copies of each version. *Id*. at 17-45.

[299] 402 F.3d 119 (2d Cir. 2005). In *Krause*, the plaintiff was the author and copyright holder of several computer programs. The plaintiff alleged that the defendant, Titleserv, a client and user of those computer programs, infringed his copyright by modifying the source code of the programs. The plaintiff claimed that Titleserv never owned the program copies saved on defendant's file server, but rather possessed the copies as a licensee pursuant to an oral agreement. Titleserv countered that it owned the program copies because it had paid the plaintiff a substantial sum to develop the program, and also had an undisputed right to possess and use the copies permanently. Employees of Titleserv "subsequently circumvented the 'lock' [that the plaintiff, Krause] had placed on the executable code and decompiled it back to the source code."

[300] T Hayes & von Lohmann, 5/1/09, at 326-327.

[301] *Id.* at 124. The court concluded that for purposes of Section 117, Titleserv was the owner of the copy of the software because:

> Titleserv paid Krause substantial consideration to develop the programs for its sole benefit. Krause customized the software to serve Titleserv's operations. The copies were stored on a server owned by Titleserv. Krause never reserved the right to repossess the copies used by Titleserv and

The Register notes that with respect to the iPhone Software License Agreement, some of the considerations that led the Second Circuit to conclude that Titleserv was the owner of copies of the computer programs in *Krause* would appear to favor the iPhone purchaser, while other considerations would not. If *Krause* were the only authority on point, it would still not offer definitive guidance as to who is the owner of the copy of the software in the iPhone. Moreover, other cases, relied upon by Apple, take an approach that is less generous to the licensee.

Apple relied on *Wall Data Inc. v. Los Angeles County Sheriff's Dep't*,[302] for the proposition that if "severe restrictions" are imposed on the use or transfer of the copy, then the transaction is a license, not a sale, and the purchaser of the copy is a licensee, not an "owner" within the meaning of Section 117.[303] Unfortunately, the *Wall Data* court failed to articulate which parts of the licensing agreement constituted "severe restrictions."[304] The court simply stated that "[g]enerally, if the copyright owner makes it clear that she or he is granting only a license to the copy of software and imposes significant restrictions on the purchaser's ability to redistribute or

---

> agreed that Titleserv had the right to continue to possess and use the programs forever, regardless whether its relationship with Krause terminated. Titleserv was similarly free to discard or destroy the copies any time it wished. In our view, the pertinent facts in the aggregate satisfy § 117(a)'s requirement of ownership of a copy.

[302] 447 F.3d 769 (9th Cir. 2006), cited by Apple in its Post-Hearing Response to Copyright Office Questions relating to iPhone modification of July 13, 2009, at 3. In *Wall Data*, the court found that the defendant Sheriff's Department was a licensee and not an owner of copies of a computer program. In reaching this conclusion, the court cited the fact that, as in *MAI*, the license agreement "imposed severe restrictions on the Sheriff's Department's rights with respect to the software." *See* 447 F.3d at 785.

[303] The Ninth Circuit found authority for this caveat in *MAI Sys. Corp. v. Peak Computer Inc.*, 991 F.2d 511 (9th Cir. 1993).

[304] The only portion of the license agreement quoted by the court provided:

> Wall Data ... grants you ("You"), the end user, a non-exclusive license to use the enclosed software program ... on a single Designated Computer for which the software has been activated. A "Designated Computer" is either (I) a stand-alone workstation, or (ii) a networked workstation which does not permit the Software to be shared with other networked workstations. You may not use the Software in any other multiple computer or multiple user arrangement. You may not use the Software other than on a Designated Computer, except that You may transfer the Software to another Designated Computer and reactivate it for use with such other Designated Computer not more than once every 30 days, provided that the Software is removed from the Designated Computer from which it is transferred.

447 F.3d at 775, n. 5. In its discussion of Section 117, the court did not specifically refer to that language.

transfer that copy, the purchaser is considered a licensee, not an owner, of the software."[305]

Apple pointed out that the iPhone Software License Agreement contains restrictions that it asserts are, under Ninth Circuit law, sufficient to make iPhone users licensees.[306] But in light of the lack of clarity as to what restrictions the Ninth Circuit was referring to in *Wall Data*, it is unclear whether the restrictions in the iPhone agreement are sufficiently "severe," in the Ninth Circuit's words, to warrant a conclusion based on *Wall Data* that Apple retains ownership of the copies of the software. For example, reasonable minds might differ as to what conclusion to draw from provisions stating that Apple owns the "software" while the purchaser of the iPhone owns the media. Moreover, a recent case from a district court interpreting Ninth Circuit case law found a conflict in Ninth Circuit cases on the question of ownership of a copy of a work.[307]

The Register concludes that the law relating to who is the owner of a copy of a computer program under Section 117 is in flux. In light of this uncertainty, the Register is reluctant to take a firm position on whether a purchaser of an iPhone is, or is not, the owner of the copy of the computer programs on the device. Where the law is unclear, the regulatory process (as distinguished from the legislative process) should be used to resolve difficult issues only as a last resort, especially when the issue is to a large degree a matter of contract interpretation. It is not

---

[305] *Id.*

[306] Apple characterizes those restrictions as follows:

> "Specifically, Section 1 of vers.1.0, 1.1.1, and 2.0 of the IPSLA all state, 'You own the media on which the iPhone Software is recorded but Apple and/or Apple's licensor(s) retain ownership of the iPhone software itself.' Section 1 of ver. 3.0 of the IPSLA simply states, 'Apple and its licensors retain ownership of the iPhone Software itself and reserve all rights not expressly granted to you.' Section 3(a) of all versions of the IPSLA further provides that the licensee may not rent, lease, lend, or sublicense the iPhone Software (versions 2.0 and 3.0 also prohibit the sale or redistribution of the software), subject to a limited exception described in the response to question 4 below."

See Post-Hearing Response of Apple to Copyright Office Questions relating to iPhone modification of July 13, 2009, at 4. The "limited exception" to the restriction on sale or redistribution is a provision permitting the purchaser to "make a one-time permanent transfer of all of your license rights to the iPhone Software to another party in connection with the transfer of ownership of your iPhone." *See id.* at 11.

[307] *Vernor v. Autodesk, Inc.*, 2009 WL 3187613, 2009 U.S. Dist. LEXIS 90906 (W.D. Wash. Sept. 30, 2009)(finding a conflict between *United States v. Wise*, 550 F.2d 1180 (9th Cir. 1977) and what the court referred to as the "*MAI* trio," consisting of *MAI Sys. Corp. v Peak Computer, Inc.*, 991 F.2d 511 (9th Cir. 1993); *Triad Sys. Corp. v. Southeastern Express Co.*, 64 F.3d 1330 (9th Cir. 1995); and *Wall Data Inc. v. Los Angeles County Sheriff's Dep't*, 447 F.3d 769 (9th Cir. 2006)). The ruling in *Vernor* is now on appeal to the Ninth Circuit. *See Vernor v. Autodesk*, No. 09-35969 (9th Cir., appeal docketed Oct. 28, 2009).

necessary to make such a determination here, or delve into the essential step analysis that is required under Section 117, because (as discussed below) the Register has concluded that fair use provides an alternative legal basis for designating a class of works.[308] As a result, the Register declines to base her recommendation on a finding centered on the question of whether "jailbreaking" involves non-infringing activity under Section 117.

b. Fair use

As an additional basis for finding a non-infringing use that would justify designating the proposed class, proponents asserted that "even if any reproduction and modification of firmware incident to jailbreaking were to fall outside the scope of both authorization and § 117(a), it would nevertheless constitute a non-infringing fair use."[309] The Register agrees that the activity of an iPhone owner who modifies his or her iPhone's firmware/operating system in order to make it interoperable with an application that Apple has not approved, but that the iPhone owner wishes to run on the iPhone, fits comfortably within the four corners of fair use.

Fair use has traditionally been defined as "a privilege in others than the owner of the copyright to use the copyrighted material in a reasonable manner without his consent."[310] In evaluating whether a particular use is being made in such a reasonable manner, it is helpful to look at the judgments Congress has made as to what kinds of uses of copyrighted material are reasonable and should be considered non-infringing.

In this case, one does not have to look far. In fact, Section 1201 itself offers strong evidence that the conduct at issue here is conduct that, at the time Congress enacted the prohibition on circumvention, it anticipated and considered to be reasonable and lawful. The proposed exemption would make it lawful for iPhone users to circumvent technological measures in the iPhone firmware in order to install and run independently created software applications designed to run on the iPhone, albeit without Apple's approval.

In Section 1201(f), Congress provided a statutory exemption that permits circumvention in

---

[308] *Accord Sony Computer Entertainment, Inc. v. Connectix Corp.*, 203 F.3d 596, 600 n.1 (9th Cir. 2000) ("Connectix contends that its copying is within the protection of section 117, but our disposition of the fair use issue makes it unnecessary for us to address that contention").

[309] C5A (EFF) at 9.

[310] *Harper & Row, Publrs. v. Nation Enters.*, 471 U.S. at 549.

order to identify and analyze the elements of a computer program that are necessary to achieve interoperabilitiy of an independently created computer program. The exemption also permits the development and employment of technological means to circumvent a technological measure in order to enable such identification and analysis, as well as to enable interoperability of an independently created computer program with other programs. Finally, the exemption permits the making available to others of such information and of the means to circumvent, solely for the purpose of enabling interoperability of independently created computer programs.

In the legislative history associated with that provision, Congress expressed a commitment to permit and encourage interoperability between independently created computer programs and existing programs. Endorsing the holding of *Sega Enters. Ltd. v. Accolade, Inc.*,[311] Congress stated in the legislative history that the purpose of the reverse engineering exemption, an exemption that it described as permitting "the circumvention of access control technologies for the sole purpose of achieving software interoperability," was to "avoid hindering competition and innovation in the computer and software industry."[312] In enacting Section 1201(f), Congress provided that one who created a circumvention tool (a "means") to enable an independently created computer program to interoperate with a computer program (including a bootloader or an operating system) would be permitted to provide that circumvention tool to others so that they may use the tool to enable an independently created computer program to interoperate with another computer program when such activity is non-infringing. Since Congress determined that it is lawful to make such tools and provide them to others for such purposes, it is difficult to imagine why Congress would nevertheless have wished to make it unlawful for others to use the tools for the purposes for which they were lawfully provided.[313]

A review of the four factors enumerated in Section 107 leads to the conclusion that making minor alterations in the firmware of an iPhone (or any smartphone) in order to permit

---

[311] *Sega Enters. Ltd. v. Accolade, Inc.* 977 F.2d 1510 (9th Cir. 1992); s*ee also, Sony Computer Entertainment, Inc. v. Connectix Corp.*, 203 F.3d 59; *Bateman v. Mnemonics, Inc.*, 79 F.3d 1532, 1540 (11th Cir. 1996); *Assessment Technologies of WI, LLC v. WIREdata, Inc.*350 F.3d 640, 644-45 (7th Cir. 2003).

[312] House Manager's Report at 14.

[313] The Register takes no position on the factual question of whether any particular person or entity has met the statutory requirements of Section 1201(f) for exempted reverse engineering or dissemination of the information and means discovered. The point of this discussion is to highlight the fact that Congress specifically provided that subject to certain requirements, Congress provided that it would not be a violation of Section 1201(a)(1) to circumvent an access control in order to achieve interoperability between computer programs and that it would not be a violation of Section 1201(a)(2) or 1201(b) to provide others with the means to enable interoperability.

independently created software applications to run on the iPhone is a fair use. In making its case that the first fair use factor, "the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes,"[314] favors a finding of fair use, EFF simply states that "[t]he first factor favors fair use because jailbreaking a phone in order to use lawfully obtained computer programs is a purely noncommercial, private use."[315] That is accurate as far as it goes, but at the very least requires elaboration. The fact that the use is noncommercial and private does not necessarily make it a fair use, nor does it even mean that the nature and purpose of the use is necessarily favored under the first fair use factor.[316] In this case, it appears fair to say that the purpose and character of the modification of the operating system is to engage in a private, noncommercial use intended to add functionality to a device owned by the person making the modification, albeit beyond what Apple has determined to be acceptable. The user is not engaging in any commercial exploitation of the firmware, at least not when the jailbreaking is done for the user's own private use of the device, in the situation under consideration by the Register.

The fact that the person engaging in jailbreaking is doing so in order to use Apple's firmware on the device that it was designed to operate, which the jailbreaking user owns, and to use it in precisely the purpose for which it was designed (but for the fact that it has been modified to run applications not approved by Apple) favors a finding that the purpose and character of the use is innocuous at worst and beneficial at best. As discussed below,[317] Apple's objections to the installation and use of "unapproved" applications appears to have nothing to do with its interests as the owner of copyrights in the computer programs embodied in the iPhone, and running the unapproved applications has no adverse effect on those interests. Rather, its objections relate to its interests as a manufacturer and distributor of a device, the iPhone.

Moreover, as noted above, Congress has determined that reverse engineering for the purpose of making computer programs interoperable is desirable when certain conditions are met, and has crafted a specific exemption from Section 1201(a)'s prohibition on circumvention in such cases. While an iPhone owner who "jailbreaks" does not fall within the four corners of the

---

[314] 17 U.S.C. § 107(1).

[315] C5A (EFF) at 9.

[316] *See BMG Music v. Gonzalez*, 430 F.3d 888, 889-90 (7th Cir. 2005).

[317] *See* discussion of fourth fair use factor, *infra*.

statutory exemption in Section 1201(f),[318] the fact that he or she is engaging in jailbreaking in order to make the iPhone's firmware interoperable with an application specially created for the iPhone suggests that the purpose and character of the use are favored.

Further support for that conclusion can be found in case law relating to reverse engineering and fair use. In *Sega,* the case the legislative history of Section 1201(f) relied on, the court of appeals found that the first factor favored a finding of fair use when Accolade reverse engineered object code in a Sega video game console in order to learn how to make its own video games compatible with, and therefore run on, the Sega console. While much of the court's analysis of the first factor focused on the fact that Accolade needed "to discover the functional requirements for compatibility" with the Sega console in order to create games that were compatible for the console,[319] the court concluded that "Accolade copied Sega's code for a legitimate, essentially non-exploitative purpose, and that the commercial aspect of its use can best be described as of minimal significance."[320] Similarly, iPhone users who jailbreak the iPhone firmware in order to install and operate compatible applications do so for a legitimate, non-exploitative purpose which, as noted above, has no commercial aspects.

The Sega court also expressly considered the "public benefit" from Accolade's activity, which "has led to an increase in the number of independently designed video game programs offered for use with the Genesis console."[321] Similarly, the whole point of jailbreaking is to permit the use of independently designed applications on the iPhone, and the activity of jailbreaking encourages the creation of such applications.

Whether the use is "transformative" is a more difficult question. The user may be altering the firmware in a way that creates a derivative work, but such a work is not always, and not commonly, a transformative work. In this context, questions arise as to whether the alterations to the firmware are transformative in the sense described by the Supreme Court; that is, do they "adds something new, with a further purpose or different character, altering the first with new

---

[318] The iPhone owner is not the person who has "identif[ied] and analyz[ed] those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs." *See* Section 1201(f)(1). Rather, the iPhone owner will be the beneficiary of that person's efforts and will be using the means provided by that person to install and run the independently created application on his or her iPhone.

[319] *See* 977 F.2d at 1522.

[320] *Id.* at 1522-23.

[321] *Id.* at 1523.

expression, meaning, or message."[322] The proponents of the exemption make no claim of transformative use, and in light of the modest nature of the modifications to the Apple firmware,[323] it is unlikely that they would be considered transformative. However, a use need not be transformative in order to be a fair use;[324] indeed, the language of Section107(1) does not state or imply that a use must be transformative in order to be fair. Given that the user is simply enabling compatibility with the smartphone's operating system so that an independently created application will operate on the user's device, the proponents appear to have made a good case that the nature and purpose of the use is favored.

Apple's entire analysis of the first fair use factor stated:

> [A]lthough the use *per se* of the modified iPhone bootloader and OS on an individual handset is of a personal nature, it is not a transformative use, and because a jailbroken OS is often used to play pirated content, such activity should be considered of a commercial nature since it avoids paying fees for the content. Therefore, factor 1 weighs against fair use.[325]

Thus, Apple admitted that the use is personal; while that in and of itself hardly makes a use fair, it certainly does not suggest that the use is unfair. Apple's observation that the use is not transformative is accurate, but all that means is that one of the favored types of use (albeit an increasingly important one) is not present here; it hardly disqualifies the use from being fair. The fact that a jailbroken OS might be used to play pirated content hardly makes the purpose and character of the use in question here, jailbreaking "accomplished *for the sole purpose* of enabling interoperability of [software] applications," a disfavored use, and it certainly doesn't make that activity commercial. In short, Apple has not made a persuasive case that the purpose and character of the use militate against a finding of fair use.

As in *Sega,* the second factor, "the nature of the copyrighted work,"[326] is perhaps more important than usual in cases involving the interoperability of computer programs. First, the

---

[322] *Campbell v. Acuff-Rose Music, Inc*., 510 U.S. at 579.

[323] *See* R49 (EFF) at 11 (modifications consist of "patched" versions of LLB, iBoot, and operating kernel that do not perform signature checking).

[324] *Campbell v. Acuff-Rose Music, Inc*., 510 U.S. at 579.

[325] R30 (Apple) at 17.

[326] 17 U.S.C. § 107(2).

programs are published works. Second, the bootloader and operating system are both highly functional works used to operate a device.[327] As functional works, certain features are dictated by function and in order to interoperate with those works certain functional elements of those programs, elements that in and of themselves may or may not be copyrightable, must be modified. Even though the works may contain creative elements, there is no evidence in the record that suggests that creative elements are copied. The only evidence about the particular nature of the changes that might be involved indicate that approximately 50 bytes of code need to be altered out of Apple's 8 million bytes of code in order to enable interoperable software programs to work on the iPhone.[328]

Apple's analysis of the second factor was simply that "the copyrighted works at issue are highly creative and not factual in nature."[329] But Apple ignored the authority, cited above, that the functional nature of computer programs is not a favored "nature of the copyrighted work." Nor does it offer any explanation or cite any authority for its assertion that its firmware is "highly creative." In fact, the case cited by Apple as blanket authority for the proposition that "Factors 2 and 3 also weigh against fair use because the copyrighted works at issue are highly creative and not factual in nature, and essentially the entire work is being copied,"[330] simply states, "Although the RUMBA software products are not purely creative works, copyright law nonetheless protects computer software,"[331] hardly an endorsement for the proposition that computer software is "highly creative."

Looking further at operating systems generally under the second factor, it is customary for these copyrighted works to enable third party programs to interoperate with them. While a copyright owner might try to restrict the programs that can be run on a particular operating system, copyright law is not the vehicle for imposition of such restrictions, and other areas of the law, such as antitrust, might apply. It does not and should not infringe any of the exclusive rights

---

[327] *See Sega*, 977 F.2d at 1524 (noting, that in the context of the second fair use factor, functional and factual works are not entitled to the same level of protection as other works). *See also, Sony v. Connectix*, 203 F.3d at 603.

[328] *See* Post-Hearing Response of EFF to Copyright Office Questions relating to iPhone modification of July 13, 2009, at 5.

[329] R30 (Apple) at 17.

[330] *Id.*

[331] *Wall Data Inc. v. Los Angeles County Sheriff's Dep't*, 447 F.3d at 779-80 (9th Cir. 2006).

of the copyright owner[332] to run an application program on a computer over the objections of the owner of the copyright in the computer's operating system. Thus, if Apple sought to restrict the computer programs that could be run on its computers, there would be no basis for copyright law to assist Apple in protecting its restrictive business model. The Register therefore concludes that the second factor decisively favors a finding of fair use.

Turning to the third factor, "the amount and substantiality of the portion used in relation to the copyrighted work as a whole,"[333] Apple argued that "essentially the entire work is being copied,"[334] and in one sense, EFF agreed, stating that because the Apple firmware is necessary in order to operate the iPhone, that "makes it necessary for individuals who jailbreak their phones to reuse the vast majority of the original firmware."[335] But it is worth noting that according to EFF, the amount of the copyrighted work modified in a typical jailbreaking scenario is fewer than 50 bytes of code out of more than 8 million bytes, or approximately 1/160,000 of the copyrighted work as a whole.[336] In a case where the alleged infringement consists of the making of an unauthorized derivative work, and the only modifications are as *de minimis* as they are here, the fact that iPhone users are using almost the entire iPhone firmware for the purpose for which it was provided to them by Apple undermines the significance of this factor. As EFF has observed, courts have been willing to permit extensive copying of the original where it is necessary to accomplish a salutary purpose.[337] Thus, while the third factor arguably disfavors a fair use finding, the weight to be given to it under the circumstances is slight.

Addressing the fourth factor, "the effect of the use upon the potential market for or value of the copyrighted work,"[338] EFF pointed out that the iPhone firmware is not sold separately, but is simply included when one purchases an iPhone. EFF asserted that this means the firmware has

---

[332] *See* 17 U.S.C. § 106.

[333] 17 U.S.C. § 107(3).

[334] R30 (Apple) at 17.

[335] C5A (EFF) at 10.

[336] Post-Hearing Response of EFF to Copyright Office Questions relating to iPhone modification of July 13, 2009, at 5.

[337] C5A (EFF) at 10 (citing *Sony Corp. of Amer. v. Universal City Studios*, 464 U.S at 417, 449-504 (1984); *Perfect 10, Inc.* v. *Amazon. com, Inc.*, 508 F.3d 1146, 1167 (9th Cir. 2007)). *See also Bond v. Blum*, 317 F.3d 385, 396 (4th Cir. 2003).

[338] 17 U.S.C. § 107(4).

no independent economic value. EFF also argued that the ability to lawfully jailbreak a phone will increase, not decrease, overall sales of the phones because users will know that by jailbreaking, they can "take advantage of a wider array of third party applications."[339]

Apple responded that the effect of the unauthorized uses "diminishes the value of the copyrighted works to Apple." It does so "by giving rise to a host of problems in the safety, security and operation of the iPhone, and by substantially increasing Apple's costs to support the software."[340] According to Apple, the fact that the firmware is a component of the iPhone mobile computing product simply means that the value of Apple's operating system software cannot be evaluated independently of the iPhone itself and that the value of the software is related to the number and quality of applications for the iPhone, as well as the availability of safe and secure means to distribute those applications to consumers.[341]

Ultimately, Apple's position with respect to harm to the market for and value of its firmware boils down to Apple's conclusion that "the value of the iPhone, and hence the software embedded in it, is substantially diminished when the integrity and functionality of that software is compromised by jailbreaking, when Apple is left to deal with the problems that ensue, and when the positive feedback loops enabled by the App Store and the iPhone Developer Program are compromised."[342] The Register concludes that these concerns are not what the fourth fair use factor is intended to address.

In this instance, *Consumer Union of the United States, Inc. v. General Signal Corp,*[343] is instructive. In that case, the publisher of *Consumer Reports* claimed that the defendant's quotation in television commercials of favorable *Consumer Reports* reviews of the defendant's product, in violation of *Consumer Reports'* policy against the use of its ratings and reports in advertising, constituted copyright infringement. The Second Circuit concluded that the quotations were fair use. Addressing the fourth factor, the court observed:

---

339 C5A (EFF) at 9.

340 R30 (Apple) at 18.

341 *Id.*

342 *Id.*

343 724 F.2d 1044 (2d Cir. 1983).

> The district court accepted CU's argument and stated that "Regina's commercial use of the article could be the demise of Consumers Union since such commercial use could lead the public to view Consumers Union as [an] unfair tester of products." We believe that this conclusion is based on a faulty premise. The Copyright Act was not designed to prevent such indirect negative effects of copying. The fourth factor is aimed at the copier who attempts to usurp the demand for the original work. The copyright laws are intended to prevent copiers from taking the owner's intellectual property, and are not aimed at recompensing damages which may flow indirectly from copying. [344]

The court concluded that the defendant's use of the plaintiff's work did not usurp demand for that work, and determined that the use was a fair use.[345]

The type of harm alleged by Apple is similar in nature. Apple is not concerned that the practice of jailbreaking will displace sales of its firmware or of iPhones; indeed, since one cannot engage in that practice unless one has acquired an iPhone, it would be difficult to make that argument. Rather, the harm that Apple fears is harm to its reputation. Apple is concerned that jailbreaking will breach the integrity of the iPhone's "ecosystem."[346]

As Judge Pierre Leval has said,

> Not every type of market impairment opposes fair use. An adverse criticism impairs a book's market. A biography may impair the market for books by the subject if it exposes him as a fraud, or satisfies the public's interest in that person. Such market impairments are not relevant to the fair use determination. The fourth factor disfavors a finding of fair use only when the market is impaired because the quoted material serves the consumer as a substitute, or, in Story's words

---

[344] *Id.* at 1050 (citations omitted).

[345] *Id.* at 1051. *See also Association of American Medical Colleges v. Cuomo*, 928 F.2d 519, 526 (2d Cir. 1991) (rejecting claim of purported harm that stems from "a non-commercial, non-competing use").

[346] *See* R30 (Apple) at 18. What actually appears to be the case is that iPhone owners who elect to jailbreak, contrary to Apple's policy, may end up regretting that decision if the consequences about which Apple warns take place. But those who elect to engage in such activity have themselves, and not Apple, to blame, and there is no reason to conclude that Apple will suffer reputational harm based upon conduct of users who have engaged in activity that is contrary to Apple's well-known policies. In any event, as noted above, such reputational harm is not the kind of harm that is relevant to the fourth factor.

> "supersede[s] the use of the original." Only to that extent are the purposes of copyright implicated.[347]

The ultimate determination of whether a use is fair involves more than tabulating the results of the four-factor analysis, but it is nevertheless telling when three of the four factors tip decisively in favor of a finding of fair use. On balance, the Register concludes that when one "jailbreaks" a smartphone in order to make the operating system on that phone interoperable with an independently created application that has not been approved by the maker of the smartphone or the maker of its operating system, the modifications that are made purely for the purpose of such interoperability are likely to be fair uses.[348] Case law and Congressional enactments reflect a judgment that interoperability is favored.

Having established that a technological measure that controls access is at issue and that the use for which circumvention is sought is a non-infringing use, it is necessary to turn to the question whether the prohibition is adversely affecting that non-infringing use. The Joint Creators argued that since no allegations of lawsuits have been brought by the proponents, the apparent lack of threats or actions indicates that the prohibition is not adversely affecting non-infringing uses. To some extent, the suggestion in the record that approximately 350,000 or more iPhones have been jailbroken in the United States might be construed as supporting this proposition.[349] However, there is nothing in the statute or the legislative history that suggests that adverse effects on non-infringing uses must be premised on actual enforcement of the prohibition. Moreover, the fact that Apple has testified in this proceeding to object to any exemption and to assert that jailbreaking violates the prohibition undermines the Joint Creators' argument and demonstrates that those who engage in jailbreaking are, at best, doing so under a legal cloud. The evidence demonstrates that the prohibition in Section 1201(a)(1)(A) could reasonably serve as the basis for a legal action substantially affecting non-infringing uses, and therefore is sufficient to establish that the prohibition is, or is likely to have, an adverse effect on non-infringing uses.

---

[347] P. Leval, *Toward a Fair Use Standard*, 103 Harv.L.Rev. 1105, 1125 (1990)(footnotes omitted).

[348] Because fair use involves a case-by-case analysis, see *Campbell v. Acuff-Rose Music*, 510 U.S. 569, 577(1994), the Register refrains from concluding that such activity will invariably constitute fair use. However, a typical case involving such a fact pattern is likely to result in a finding of fair use.

[349] C11A (EFF) at 5, citing http://arstechnica.com/apple/news/2008/10/the-story-behind-cydia-on-the-iphone.ars. (Last visited 4/30/10.) (noting that Cydia allows users of jailbroken phones to download and install apps that were not approved by Apple and are not available in the Apple App Store. Cydia's creator stated that the method the site uses to track unique iPhone identifiers has identified 350,000 unique users, but since this identification system is new, the number of jailbroken iPhone owners that use the site is believed to be higher.)

3. *Application of statutory factors*

Having concluded that the prohibition on circumvention does have an adverse effect on non-infringing uses in such cases, the Register now turns to the statutory factors that must be considered by the Librarian of Congress.

Factor One.

Apple has created a system of customizable applications on wireless communication handsets that has made it possible for the public to use a wide variety of independently created computer programs on the iPhone. Despite the enormous choices available to consumers, the record reveals that restrictions that do not implicate copyright interests are placed on independently created interoperable computer programs. Thus the existing market creates legal barriers for the use of copyrighted works. An exemption would encourage the availability of additional applications for use on smartphones. At the same time, there is no reason to believe that an exemption would discourage smartphone manufacturers and those who create the operating systems for those smartphones from continuing to do so. The iPhone is a huge success in the marketplace even though jailbreaking is a common practice.

Exempting the proposed class of works will likely increase the availability of independently created computer applications for smartphones, while simultaneously being unlikely to interfere with the availability of smartphone operating systems or other works currently being used or created for wireless communications devices.

This factor favors exempting the proposed class.

Factor Two

The recommended exemption will be unlikely to affect the availability of works for these purposes in any way. This factor appears to be neutral.

Factor Three

Like the previous factor, the recommendation is unlikely to affect the interests in this factor. This factor also appears to be neutral.

Factor Four

There is no reason to believe that the proposed exemption would adversely affect the value of the copyrighted firmware that is the class of works directly affected by the exemption. If any effect on the market for, or value of, such works can be expected, it is quite possible that the exemption could increase the market for or value of such works, since the availability of additional applications to be used on smartphones may well make them more attractive to consumers.

Although there has been speculation that an exemption might expose copyrighted content that is protected by access controls on wireless handsets to unlawful copying and distribution, no factual basis for such speculation has been presented.[350] Moreover, the proposed exemption is tailored to permit circumvention only to permit circumvention to enable wireless telephone handsets to execute *lawfully obtained* software applications.

To the extent that unlawfully obtained applications are made interoperable with wireless communication devices, circumvention in order to make telephone handsets execute those applications will remain actionable under the prohibition notwithstanding the exemption.

4. *NTIA Comments*

The Assistant Secretary for Communications and Information of the Department of Commerce does not support designation of the proposed class. NTIA acknowledged that exempting iPhone jailbreaking could facilitate innovation, better serve customers, and encourage the market to utilize open platforms, but it believes "it might just as likely deter innovation by not allowing the developer to recoup its development costs and to be rewarded for its innovation."[351] NTIA also believes that the proponents' "public policy" arguments should properly be considered by expert regulatory agencies, the Department of Justice, and the Congress. However, NTIA

[350] *See* R46 (Joint Creators) at 38.

[351] NTIA Letter at 9.

qualifies that view by stating that the "Register ought only to consider recommending the proposed exemption if she concludes that the access control measure would be a bar to actions that the above bodies might take in response to policy judgments made at those agencies."[352] NTIA also expresses concern about the effect of an exemption on contractual agreements and how these agreements might alter the underlying nature of the use.[353]

The Register appreciates that other administrative agencies also have jurisdiction on potential issues relating to the iPhone, smartphones, and other mobile phone and data services. However, the focus in this rulemaking is limited to actual or likely adverse effects on non-infringing uses of copyrighted works. No other agency has delegated authority to temporarily limit the application of the prohibition on circumvention. This prohibition was established to provide legal support for, and foster the availability of, copyrighted works in the digital environment. The Register has found that the prohibition is adversely affecting the ability to engage in the non-infringing use of adding unapproved, independently created computer programs to their smartphones. The Register also finds that designation of this class will not adversely affect the market for or value of the copyrighted works to the copyright owner.

If the Librarian does not designate the proposed class, Section 1201 may be used to prevent jailbreaking. Any action by a federal regulatory agency to permit jailbreaking will be futile if jailbreaking violates Section 1201(a)(1), and outside of this rulemaking, no federal agency has the authority to exempt such activity from liability under Section 1201(a)(1). On the other hand, if the proposed class of works is designated by the Librarian, all that it will mean is that Section 1201 cannot be used to prevent jailbreaking, without prejudice to any other legal or regulatory authority that might limit or prohibit jailbreaking. In fact, as NTIA notes, state contract law is also at issue in the relationship between purchasers of smartphones and manufacturers and/or service providers. Nothing in this rulemaking will alter the contractual obligations between parties. Therefore, the Register finds that designating the proposed class of works will remedy the adverse effects on non-infringing uses caused by the prohibition on circumvention without interfering with other policy, legal, or regulatory concerns appropriately addressed by other governmental bodies or between the parties to the transaction themselves.

NTIA also stated that it "views this proposed exemption as somewhat analogous to the platform shifting proposals rejected previously by the Librarian. As in those cases, an exemption

---

[352] *Id.* at 9-10.

[353] *Id.* at 10-11.

is not warranted that will guarantee the device owner the ability to use any software on any and all platforms."[354] However, the platform-shifting proposals referred to by NTIA related to technological measures that were applied, by or on behalf of copyright owners, to tether copies of audiovisual and musical works to particular devices in order to prevent illegal digital distribution. In recommending against an exemption to permit such platform-shifting, the Register observed, "tethering and DRM policies serve a legitimate purpose for limiting access to certain devices in order to protect the copyright owners from digital redistribution of works" and that the "effect of circumvention of the protection measures employed on these works would be likely to decrease the digital offerings for these classes of works, reduce the options for users, and decrease the value of these works for copyright owners."[355] That does not appear to be the case where access controls are placed *on a device* in order to prevent software applications written by third parties to run on that device. Here, the user wants to use a particular computer program on a device for which that computer program was specifically created. It is the creator of the device who is trying to prevent the running of that computer program on the device. The access control does not really appear to be protecting any copyright interest.

5. *New Class of Works*

Accordingly, the Register recommends the following exemption:

> Computer programs that enable wireless communication handsets to execute software applications, where circumvention is accomplished for the sole purpose of enabling interoperability of such applications, when they have been lawfully obtained, with computer programs on the telephone handset.

This is the language suggested by the proponent, with one change. The proponent had proposed the following class:

> Computer programs that enable wireless telephone handsets to execute *lawfully obtained* software applications, where circumvention is accomplished for the sole purpose of enabling interoperability of such applications with computer programs on the telephone handset. (Emphasis added).

---

354 NTIA Letter at 10 (citing *2006 Final Rule*, 71 Fed. Reg. at 68,478).

355 2006 Recommendation of the Register of Copyrights at 71-72.

The notion clearly was that the exemption would apply only in cases where the software application that is being made interoperable with the telephone handset's firmware and/or operating system must have been lawfully obtained. Since the computer programs themselves will enable execution of an application whether or not the application has been lawfully obtained, the restriction more properly belongs in the description of circumstances under which the permitted circumvention will occur. The recommended class applies only when the circumvention is accomplished to enable interoperability of lawfully obtained applications with the computer program (e.g., the operating system) that is protected by access controls.

C. Computer programs, in the form of firmware or software, that enable used wireless telephone handsets 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.

1. *The 2006 class of works*

In the 2006 rulemaking, the Wireless Alliance and Robert Pinkerton proposed a class of works consisting of computer programs that operate wireless communications handsets. The proponents stated that providers of mobile telecommunications networks were using various types of software locks in order to control customer access to the "bootloader" programs on mobile phones and the operating system programs embedded inside mobile handsets. According to the record established three years ago, these software locks prevented customers from using their handsets on an alternative wireless network by controlling access to the firmware that operates the mobile phones (*i.e.*, the mobile firmware).[356]

At that time, the Register concluded that consumers who wanted to use their mobile phones on a different wireless network were often precluded from doing so unless they could obtain access to the bootloader or operating system within the phone in order to direct the device to a different carrier's network. The record evidence then demonstrated that most wireless providers did not allow a consumer to obtain such access in order to switch a mobile phone from one network to another, and that the consumer could not use the mobile phone elsewhere, even after fulfilling her contractual obligations with the carrier that sold the device. The Register found

[356] *See* 2006 Recommendation of the Register of Copyrights at 48.

that, in order to switch carriers, the consumer had to purchase a new phone from a competing wireless carrier.[357]

The Register specifically concluded that the software locks were access controls that adversely affected the ability of consumers to make non-infringing use of the software on their mobile phones. She noted that there had been no argument or suggestion that a consumer wishing to switch a lawfully purchased mobile handset from one network carrier to another is engaging in copyright infringement or in an activity that in any way implicates copyright infringement or the interests of the copyright owner. The underlying activity sought to be performed by the owner of the handset is to allow the handset to do what it was manufactured to do – lawfully connect to a carrier. She concluded that this is a non-infringing activity by the user.

A review of the factors enumerated in Section 1201(a)(1)(C)(i)–(iv) supported the conclusion that an exemption was warranted at that time. First, there was nothing in the record suggesting that the availability for use of copyrighted works would be adversely affected by permitting an exemption for mobile phone locks. Second, there was no reason to conclude that there would be any impact (positive or negative) on the availability for use of works for nonprofit archival, preservation, and educational purposes or on the ability to engage in criticism, comment, news reporting, teaching, scholarship, or research. Third, circumvention of the locks to connect to alternative wireless networks was not likely to have any effect on the market for, or value of, copyrighted works. The Register stated that the reason that the factors appeared to be neutral was that the access controls did not appear to be deployed in order to protect the interests of the copyright owner or the value or integrity of the copyrighted work; rather, they were used by wireless carriers to limit the ability of subscribers to switch to alternative wireless networks, a business decision unrelated to copyright protection.

This outcome required an examination of the additional factor set forth in Section 1201(a)(1)(C)(v): "such other factors as the Librarian considers appropriate." The Register concluded that when application of the prohibition on circumvention of access controls would offer no apparent benefit to the author or copyright owner in relation to the work to which access was controlled, but simply offered a benefit to a third party who may use Section 1201 to control the use of hardware which may be operated in part through the use of computer software or firmware, an exemption from the prohibition on circumvention may well be warranted. The

---

[357] *Id*. at 49.

Register concluded that such appeared to be the case with respect to software locks on wireless handsets.[358]

The Register acknowledged that copyright owners (of music, sound recordings and audiovisual works whose works are offered for downloading onto mobile phones) expressed some concern about the proposal. She noted their stated concerns that designation of the class might permit circumvention of access controls that protect their works when those works have been downloaded onto mobile phones. She found that the record on this issue was inconclusive, but nevertheless took this concern into account by fashioning a class in a way that permitted mobile phone unlocking, but at the same time, avoided unintended consequences related to other types of copyrighted works contained on the handset.

Because the Register stated that, in appropriate circumstances, a class of works may be refined by reference to uses made of the works, she concluded that the matter may be best resolved by modifying the proposed class of works. As such, the Register recommended approval of the following class of works in 2006:

> *"Computer programs in the form of firmware that enable wireless telephone handsets to connect to a wireless telephone communication network, when circumvention is accomplished for the sole purpose of lawfully connecting to a wireless telephone communication network."*

2. *Background*

The issues discussed herein are particularly complicated because of the mobile phone technologies at issue and the business models used in the wireless industry. Therefore, it is useful to provide a brief overview of several key terms and concepts used throughout the discussion.

- This class of works here pertains to mobile phones (or "cellphones" as they may be called)[359] as well as so-called "smartphones," such as the iPhone.[360]

---

[358] *Id.* at 52.

[359] According to the CTIA-The Wireless Association (CTIA), the trade association representing wireless carriers and their suppliers, as well as providers and manufacturers of wireless data services and products, more than 630 devices were manufactured for the wireless market last year. *See* CTIA comments filed in FCC WT Docket No. 09-66 (filed Sept. 30, 2009).

[360] For a discussion of smartphones, *see the* discussion *supra* at p. 78.

- The computer programs that are the subject of the proposed class are embedded in the mobile phone's firmware.[361]
- There are several different wireless carriers in the United States, the four largest of which are Verizon Wireless, AT&T Mobility, Sprint-Nextel, and T-Mobile USA. There are also several smaller wireless telecommunications companies, such as MetroPCS[362] and Pocket Communications,[363] as well as mobile virtual network operators ("MVNOs"),[364] such as Virgin Mobile.[365]
- Wireless carriers use different transmission technologies on different wireless networks. Verizon and Sprint, for example, use Code Division Multiple Access ("CDMA") technology. AT&T and T-Mobile use Global System for Mobile communications ("GSM") technology.[366] These technological standards are incompatible so, for example, a consumer cannot use a CDMA phone on a GSM network.[367]

---

[361] For a definition of "firmware," *see* the discussion *supra* at p. 79.

[362] C5B (MetroPCS) at 2. MetroPCS, one of the proponents of an exemption here, stated that it is a new wireless carrier focusing on low cost, flat rate services in major metropolitan areas. Through its affiliates and subsidiaries, it noted that it owns or has access to wireless licenses covering a population of approximately 149 million people in 14 of the top 25 largest metropolitan areas in the United States.

[363] C5C (Pocket) at 2-4. Pocket Communications, another proponent of an exemption targeting mobile phones, stated that it is a regional wireless carrier providing prepaid, flat rate, unlimited use voice and data services over its south Texas communication networks.

[364] An MVNO is a company that buys network capacity from a wireless carrier in order to offer its own branded mobile subscriptions and value-added services to customers. *See* CTIA Wireless Glossary of Terms, http://www.ctia.org/advocacy/research/index.cfm/AID/10408. (Last visited 4/30/10.)

[365] Virgin Mobile, one of the opponents of the proposed mobile phone exemption, stated in the record that it is one of the ten largest wireless service providers in the United States. Its wireless service is operated on nationwide network facilities provided by Sprint Nextel. R 51 (Virgin Mobile) at 4. Sprint Nextel acquired Virgin Mobile at the end of 2009. *See* Press Release, Sprint Nextel Completes Acquisition of Virgin Mobile USA (November 24, 2009). Sprint stated that customers using Virgin Mobile's products will "continue to enjoy the benefits of their current phones, service plans and features." *See id.*

[366] Aside from CDMA and GSM, there are two older, lesser used, mobile phone technologies. First, there is Time Division Multiple Access or "TDMA." This technological standard permits the transmission of information by dividing calls into time slots, each one lasting only a fraction of a second. AT&T, along with Cingular (now part of AT&T), have used this technology in the past. Then, there is the Integrated Digital Enhanced Network ("iDEN") standard. This specialized mobile technology combines two-way radio, telephone, text messaging and data transmission into one digital network. It was primarily used by Nextel Communications before its merger with Sprint. Other smaller wireless carriers, such as AirTel Montana and Southern LINC Wireless, have used it as well. *See* CTIA Wireless Glossary of Terms, http://www.ctia.org/media/industry_info/index.cfm/. (Last visited 4/30/10.)

[367] *See* T Lurie, 5/1/09, at 126 (A Virgin Mobile phone could be used on Sprint's network, but it could not be used on AT&T's network). It is possible, however, for a consumer with a GSM phone to swap out an existing SIM card (for use with a wireless network in the United States) with another SIM card so that the same phone can be used on wireless networks in most European countries. T Granick, 5/1/09, at 194.

- There are two competing business/marketing models in the wireless industry. There is the "postpaid" plan where a consumer signs a long term service contract with a wireless carrier at the time the phone is purchased and is obligated to pay for service after use. If the consumer wishes to terminate service earlier than the end of the contract term, she may be required to pay an early termination fee. The other model is known as the "prepaid" plan where a consumer pays for service in advance of use and is not required to sign a long term contract at the time of purchase, but nonetheless may be bound by other specified terms of use. There are generally no early termination fees under this type of arrangement.

- The wireless carrier often subsidizes the cost of the phone to make it more affordable for the consumer. Subsidies exist in both the prepaid and the postpaid markets. There are unsubsidized phones available for purchase in the marketplace, but they are in the minority compared to the number of subsidized devices. There is also an after market for used phones through commercial resellers or through online marketplaces, such as eBay.

- Current mobile phones typically include two operating systems inside the same device: a "baseband system," which controls the mobile phone's radio and communications with the mobile phone network, and a separate "host system" that manages user applications. The baseband and host systems generally have their own separate CPUs, memory, and operating systems. Changes made to either system need not affect the other because the baseband and host systems are distinct. Carrier locks, when present, are normally implemented by the baseband system, whereas application locks and related restrictions are normally implemented by the host system.[368]

- In order to retain customers, and recoup the costs of the subsidy, wireless carriers have implemented different types of carrier locks on the phones they sell to consumers. The lock prevents a mobile phone owner from accessing and instructing the firmware that directs the phone to connect to a particular network. The most commonly recognized locking measures are:

    - Service provider code locking ("SPC"). The SPC code is often a six digit number derived from an algorithm that uses the handset's electronic serial number ("ESN"). The carriers provide the algorithm to the phone manufacturers who input the ESN and use the resulting number to set an access code on new handsets. An SPC-locked mobile phone cannot be reprogrammed to operate on a wireless network unless the programmer first inputs the correct SPC code.[369] Sprint and Verizon both employ SPC locks on their mobile phones.

---

[368] R 49 (EFF) Appendix A at 9.

[369] C5D (Wireless Allliance) at 8.

- Master Subscriber Lock ("MS"). The MS lock protects a number of functions on the handset. It prevents the phone from being unlocked and used on another network. It also prevents access to the "embedded file system," where address books, calendars, and other mobile phone utilities are located. MS locks are currently being used by Virgin Mobile.[370]

- Subscriber identity module locking ("SIM"). This type of locking involves a SIM card which is a small device that stores a customer's identifying information on GSM handsets. The card is easily removed and replaced. A customer with a SIM card phone can select service providers by inserting the appropriate card in the handset. The network reads the card, allows the connection, and then collects accurate billing information. With a lock in place, a different SIM card cannot be inserted into the handset.[371] AT&T and T-Mobile program their handsets with SIM locks which prevent a consumer from accessing the phone's firmware.

- System operator code locking ("SOC"). The SOC is a number assigned to a wireless carrier.[372] The code programmed into the mobile phone must match the code of the carrier providing service to the phone. When the handsets are locked, the SOC code cannot be changed, so the phone cannot be reprogrammed for use on a different network.[373] AT&T and Cingular (now AT&T Wireless) have used SOC locks in the past.[374]

- Band order locking ("BO"). BO locking restricts the frequencies on which mobile phones will operate. While mobile phones are generally capable of operating across the entire range of frequencies allocated by the FCC for mobile communications, each carrier is licensed to operate only on certain blocks within those bands. By restricting the blocks on which the handset can

---

[370] T Buerger, 5/1/09, at 133-134. Virgin Mobile stated that its MS lock is unique to each handset and is generated using proprietary algorithms embodied in software. R51 (Virgin Mobile) at 10.

[371] *Id*. at 9.

[372] SOC locks are associated with TDMA phones. R36 (Cricket) at 6.

[373] *Id.*

[374] Apart from a cursory review by the proponents, SOC or BO locking were not discussed in any detail in the current proceeding. It is worth noting, however, that SOC locks have, at least in the past, been embedded in the mobile phones sold by TracFone. "(There are two "software locks" employed in the TracFone handset, one to limit access to the TracFone software resident on the handset, and the other to prevent access to the operating system. The latter is akin to what has been referred to as the 'system operator code' (SOC) lock that prevents third parties from reprogramming the handset. On TracFone's handset, there is no specific software lock that only controls access to the carrier's wireless network.") *See* Petition for Consideration and Entry of Reply Comments of TracFone Wireless, Inc. in Docket No. RM 2005-11, at 4 (2006 anticircumvention proceeding).

operate, the carrier prevents the handset from being used on a different network.[375]

- As illustrated above, different wireless carriers use different locking measures on different phones on different networks. These locks control access to the firmware and are considered technological protection measures or "TPMs."

- These phones may be unlocked by the consumer, the wireless carrier, or by other third parties. The type of unlocking measure used depends on the phone and the wireless network on which it is used.[376]

- There are a variety of reported methods for unlocking CDMA phones with SPC locks. If a consumer knows the unlock code, then she simply calls up a series of prompt screens (directing the user to the phone's data registry) on the device and enters the correct number. Another way is to use a computer-based tool to read the data on the device, clear the existing SPC value, and/or reset it to zeros.[377] In the process, the preferred roaming list ("PRL")[378] and number assignment module ("NAM")[379] may be reconfigured and updated so that the phone can be used on a new wireless network.[380]

- Mobile phones, including CDMA phones, may also be unlocked by being "reflashed."[381] Firmware, of the kind found in a mobile phone, is designed to be changed or upgraded. In this context, when a phone is reflashed, the firmware and locking code are wiped out thereby freeing the device to be used on another wireless network. There are also more intelligent forms of reflashing that only eliminate the

---

[375] C5D (Wireless Alliance) at 8-9.

[376] Specific methods to unlock mobile phones using SOC locks and BO locks were not raised in the current record. In a comment in the proceeding three years ago that was not considered due to its untimely submission, CTIA stated that SOC locks have been seldom used by wireless carriers to lock mobile phones. It also stated that BO locking was not commonly used by major wireless carriers in the United States. *See* CTIA, Complementing Response to the Copyright Office's Request of August 14, 2006, for Further Information in Docket No. RM 2005-11, at 2 (Sept. 11, 2006). These may be the reasons why there is a lack of information in the current record on how to unlock phones with these locks. Given this circumstance, the focus of the discussion here will be on SPC, MS, and SIM unlocking.

[377] T Granick, 5/1/09, at 146-47.

[378] The preferred roaming list is a list of system identification codes of networks with which the carrier providing the service has agreements to allow the handset to be used. Each carrier has a different preferred roaming list based on its own networks and contractual agreements it has with third parties. This list is routinely changed by carriers as they establish or change relationships with third parties for roaming service. Essentially, the PRL tells your phone which towers to look for when establishing a wireless connection. *See* C5B (MetroPCS) at 7.

[379] The NAM contains files that store a device's phone number, the electronic serial number, and other firmware settings in non-volatile memory.

[380] R25 (Han) at 3.

[381] *See* the discussion *infra*, at fn. 391 and pp. 119 and 123, for additional information about "reflashing."

carrier locks, but preserve content, such as calendar information and address books, on the phone.

- Some phones with a MS lock may need to be unlocked and then reflashed in order for the device to be used on another wireless network. Once unlocked, the firmware may be reflashed via a serial port on the handset, manually changed via keypad, or changed via over-the-air communication.[382] This is the case for Virgin Mobile's phones.
- In general terms, GSM phones with SIM cards can be unlocked by inputting the correct sequence of digits. An example of unlock code for a GSM handset is: 38123134.[383]
- Some GSM phones, such as the iPhone, are more complicated to unlock. As discussed in more detail below, the methods used to unlock these devices may result in the creation of a derivative work if there is an unauthorized "adaptation" of the firmware embedded on the phone.

3. *The 2009 Proposed Classes of Works*

In the current rulemaking proceeding, the Register has received three new proposals relating to computer programs that operate wireless communications handsets. Two of the proposals were from commercial mobile phone service providers[384] and one was from a coalition of mobile phone recyclers/resellers.[385] The language of the proposed classes is as follows:

Class of Works 5B (filed by MetroPCS):

---

[382] R51 (Virgin Mobile) at 12.

[383] R25 (Han) at 3.

[384] In mid-2008, MetroPCS launched its "MetroFLASH" commercial unlocking service. Here, a customer brings her compatible CDMA handset into a MetroPCS location and, after paying a fee to unlock the phone, it is reflashed and placed in service on MetroPCS's network. *See* C5B (MetroPCS) at 6. Pocket also offers a commercial unlocking service, but uses the term "reprovisioning" for the action of unlocking a mobile phone. According to Pocket's website, "Reprovisioning a phone is a process wherein a mobile phone's program inside your phone's memory is updated or re-programmed with software updates. It actually removes the current service provider by clearing the SPC (Service Programming Code) and the PRL (Preferred Roaming List) on a mobile phone and make it compatible with a different service provider such as Pocket. Reprovisioning is only available in selected markets." *See* http://www.pocket.com/index.php/faq/6. (Last visited 4/30/10.) Pocket indicates that voice mail messages are the only type of "information" currently stored on the phone that may be lost when a phone is "reprovisioned." *Id.*

[385] MetroPCS and Pocket did not file exemption requests in the 2006 Section 1201 rulemaking proceeding.

> *Computer programs that operate wireless telecommunications handsets when circumvention is accomplished for the sole purpose of enabling wireless telephones to connect to a wireless telephone communication network.*

Class of Works 5C (filed by Pocket):

> *"Mobile Network Connection Programs." Computer programs in the form of firmware or software that enable mobile communication handsets to connect to a wireless communication network, when circumvention is accomplished for the sole purpose of lawfully connecting to a wireless communication network.*

Class of Works 5D (filed by the Wireless Alliance[386]/ReCellular[387]/Flipswap[388] (collectively referred to herein as "Wireless Alliance")):

> *Computer programs in the form of firmware that enable wireless telephone handsets to connect to a wireless telephone communication network, when circumvention is accomplished for the sole purpose of lawfully connecting to a wireless telephone communication network, regardless of commercial motive.*

As is evident from the wording, these proposed classes closely track the class designated by the Librarian in 2006. The Cellular Telecommunications Industry Association ("CTIA") and Virgin Mobile opposed these requests on several grounds. The proponents of the original three requests then collaborated and filed responsive comments proposing a new "Harmonized Class of Works" for the Register to evaluate. An in-depth discussion of the wording of the proposed classes follows the analysis of the threshold issues raised and addressed directly below.

a. The Burden of Showing an Adverse Effect on Non-Infringing Uses

MetroPCS, Pocket, and the Wireless Alliance have each stated, in various terms, that wireless carriers have the technological ability to prevent individuals from using their own mobile phones on more than one wireless network. They stated that carriers have established technological protection mechanisms which lock a mobile phone to a particular wireless network.

---

[386] C5D (Wireless Alliance) at 4-9. The Wireless Alliance stated that it is a corporation that recycles and resells used and refurbished wireless products. The Wireless Alliance further stated that it repurposes used phones and recycles those that cannot be reused.

[387] ReCellular stated that it is the world's largest recycler and reseller of used wireless phones and accessories. It further stated that it has partnered with the mobile phone industry's Wireless Foundation on the original "Donate a Phone" charitable recycling program.

[388] Flipswap stated that it is a mobile phone recycler. It further stated that its trade-in program allows consumers to reuse their phones by putting them back into the secondary market and offers cash, gift certificates, or store credit to consumers for their trade-in devices.

They specifically stated that wireless providers handcuff mobile phones to their networks using a variety of methods, including SPC locking, SOC locking, BO locking, and SIM locking.[389] They explained that these locks prevent a mobile phone consumer from accessing and instructing the firmware that directs the phone to connect to a particular network. They asserted that these locks adversely affect non-infringing uses, in this case, the ability of a consumer to use a wireless network of her own choice. They each sought the ability to use different methods to legally unlock mobile phones, such as recoding[390] or reflashing,[391] so that the consumer is free to use her device on an alternative wireless network. The proponents urged that the existing class of works be redesignated, with certain changes, so that consumers can legally circumvent the TPMs using any of a number of unlocking methods.

CTIA argued that the proponents have failed to meet their burden of proving the need for any exemption. It stated that there is a presumption in favor of the prohibition against circumvention that proponents in the rulemaking must overcome, even for previously designated classes of works. It emphasized that the assessment of adverse impacts on particular categories of works is to be determined *de novo*. It asserted that the 2006 determination regarding mobile phone unlocking firmware cannot be used to support continuation of that exemption now as proponents attempt to do by characterizing their proposals as a "renewal" or a "continuation" of the exemption. It concluded that the presumption of prohibition remains and the burden of proof must be met anew with new evidence for each category of works.[392]

Further, CTIA addressed the sufficiency of the proponents' evidence. It remarked that isolated or anecdotal evidence is not sufficient, nor is evidence of convenience or efficiency. It

---

[389] According to EFF, SPC locking is the most common kind of lock for CDMA phones. SIM locking is the most common type of lock for GSM phones. The SIM lock only controls whether the handset will accept a SIM card from another carrier; TPMs on *content* are always separate on these phones. Post-Hearing Response of EFF to Copyright Office Questions Relating to Cellphones of July 13, 2009, at 8.

[390] T Granick, 5/1/09, at 146.

[391] As noted earlier, there are two reported methods of reflashing: one method completely wipes out the binary code on the memory chip so that the mobile phone's locking program and related content is wiped out. The other method has the effect of unlocking the device, but maintains certain types of content on an embedded file so that, for example, purchased ringtones are not eradicated. *See* T Buerger, 5/1/09, at 177. ("**MR. CARSON**: Can I follow up, then? Because one thing wasn't clear to me. I heard one statement that reflashing gets rid of the software; is that right? **MR. BUERGER**: Not necessarily. So, there are two methods for a binary reflash: One that will completely wipe out all of the binary -- the code binary on the memory. There are also reflashing methods that actually keep the content in the embedded file. So, if you bought a game before or a ring tone before, you can reflash it with a new binary and keep the old ring tones that you bought..")

[392] R43 (CTIA) at 9-10.

added that evidence must be more than rhetoric, more than good policy, and more than conjecture. It argued that none of the proponents attempted to show that they have actually been harmed by the prohibition on circumvention, nor have any of the proponents "shown actual harm by the differences between the current exemption and the expansions that they seek." In the absence of any proof of actual harm, it stressed that the proponents must instead demonstrate that harm is "likely" to occur in the next three years. It noted that, in the past, proposed classes have been rejected for the very reason that there was no firm evidence to show that the predicted consequences would actually ensue. CTIA asserted that none of the proponents have adequately demonstrated the requisite "likely" adverse impact on non-infringing uses sufficient to justify their requests.[393]

Discussion. At the outset, it appears obvious that the three proposed classes outlined above are very similar to the class of works recommended to the Librarian for approval in 2006. Further, the underlying facts supporting the requests are generally the same as they were three years ago. While a proponent of a class of works is required to provide new evidence to support her request for the renewal of a class of works, such as in the case here, the Register's prior determinations have some precedential value and, unless persuaded otherwise, the Register is likely to reach a similar conclusion *when similar facts have been presented.*

On the other hand, the similar class that was designated three years ago was unopposed[394]. In contrast, this year's proposals on this topic were hotly contested, and the opponents offered serious objections, which are considered below.

As she did three years ago, the Register recognizes that the proponents' requests fall within the zone of interest subject to this rulemaking. That is, circumventing a mobile phone lock, without the authority of the copyright owner, to gain access to the protected work (*i.e.*, the firmware) is likely actionable under Section 1201(a)(1) of the Act. Further, a wireless carrier that

---

[393] *Id*. at 13. Virgin Mobile also opposed the requests on the grounds that proponents have not met their evidentiary burden. It specifically argued that proponents have failed to demonstrate with sufficient evidence that a non-infringing use is likely to be adversely affected by the prohibition in the ensuing three years, and instead, have put forth various conclusory statements with little factual support. It asserted that proponents have not provided any concrete evidence demonstrating that there are likely adverse effects of the Section 1201(a) prohibition on circumvention that outweigh the risks to the legitimate interests of its own business and that of other wireless service providers. R51 (Virgin Mobile) at 14-15.

[394] CTIA and TracFone, a wireless carrier, did make belated attempts to oppose the mobile phone exemption in 2006, but their untimely submissions were not considered. *See* 2006 Recommendation of the Register of Copyrights at 48.

is harmed by the circumvention of the software lock may bring an action for violation of Section 1201(a)(1) against anyone who circumvents such a technological protection measure.[395]

In this instance, as discussed in greater detail below, the Register finds that the proponents have presented a *prima facie* case that the prohibition on circumvention has had an adverse effect on non-infringing uses of firmware on wireless telephone handsets. The proponents had to prove that the access controls at issue, the mobile phone locks, adversely affected non-infringing uses. Here, they have shown that such locks prevent consumers from legally accessing alternative wireless networks with the phone of their choice. This is the same type of activity that was at issue when the existing class was being considered in 2006.[396]

The Register finds that there is more evidence in support of designating a class of works now than there was in 2006 when the class was first approved by the Librarian.[397] The material submitted in this rulemaking shows that the locks have a substantial adverse affect on the use of the handset. Specifically, if a consumer wishes to switch wireless providers, but keep her phone, she would have to engage in a circumventing activity. This situation would actually exist today, but for the designation of the class of works in the current regulations, and is likely to occur in the next three years unless a similar class is designated.

In determining whether the prohibition on circumvention of access controls is having an adverse effect on noninfringing uses in connection with mobile phones, the principal issue is whether the copyrights in the computer programs that operate mobile phones are infringed when the owner of a mobile phone switches to a new wireless network. The infringement might consist of the making of random access memory ("RAM") copies of the mobile phone's firmware –

---

395 *See id.* at 51 (citing similar language).

396 *See id*. at 50. ("The underlying activity sought to be performed by the owner of the handset is to allow the handset to do what it was manufactured to do – lawfully connect to any carrier. This is a non-infringing activity by the user. But for the software lock protected by § 1201, it appears that there would be nothing to stand in the way of a consumer being able to engage in this non-infringing use of a lawfully purchased mobile handset and the software that operates it.")

397 The named proponents, along with EFF, filed voluminous comments, appendices, and supplements, substantiating the need for an exemption. In addition, the Register has received comments from individuals across the country providing anecdotal evidence in support of an exemption of a type similar to the 2006 exemption which permitted them to unlock their phones. *See, e.g.*, R5 (Flerchinger), R6 (Kilpatrick), and R12 (Brenner). According to online surveys initiated by EFF, 632 individuals are on record as voicing their support for the exemptions stated in Proposed Classes 5B, 5C and 5D. R44 (Pocket) at Exhibit A, p. 3. Lincoln Han stated that he has helped thousands of people unlock their mobile phones so that they can be used on other networks. R25 (Han) at 4.

On the other hand, as noted above, substantial arguments were offered in opposition, in contrast to the situation three years ago.

something that occurs simply by turning on the device.[398] Or, it may consist of the making of a derivative work based on the computer program embedded in the firmware, which may need to be adapted in order to operate on another network. In addition to such alleged acts of infringement, opponents of the proposed class have alleged that permitting circumvention of access controls protecting the firmware will enable the unauthorized use, including possible unauthorized reproduction or distribution, of other works of authorship, such as ringtones, "wallpaper," etc., that are typically loaded onto a mobile phone.[399]

The following section addresses the specific legal arguments made by the proponents and opponents of the proposed class regarding noninfringing use with respect to the copyrights in the mobile phone firmware.

b. Circumvention in Order to Access Firmware to Switch Mobile Phone Networks

The Reproduction Right. Virgin Mobile explained that its customized mobile phone operating system, software applications, and most content reside on flash memory built into its handsets. It stated that when the operating system and/or applications are being used on the handset, instructions embodied in such software are first copied from the flash memory into a faster memory chip, namely the RAM. It added that the instructions are then loaded from RAM into the processor, where they are executed. Virgin Mobile concluded that any use of the handset necessarily requires making one or more internal copies of the operating system and/or applications. It likewise concluded that in order to use any content, such content must be temporarily copied from flash memory, whether built into the handset or removable memory, into

[398] Opponents of the proposed classes, such as Virgin Mobile, have argued that in order to use a mobile phone on another network, the owner of the phone must, at a minimum make RAM copies of the operating system whenever the owner uses the phone, and that those copies are unauthorized and therefore infringing when they are made in order to operate the phone on another network. They also have argued that it is frequently necessary to adapt the operating system software in such a way that violates the copyright owner's exclusive right to make derivative works. Proponents have responded that the making of such copies and adaptations is noninfringing under Section 117. Those arguments and counterarguments are discussed below.

[399] Issues relating to such other works of authorship are addressed, *infra*, in the discussion of the fourth statutory factor under Section 1201(a)(1)(C) (the effect of circumvention of technological measures on the market for or value of copyrighted works).

RAM. For example, it noted that in order to play a ringtone, the data representing the ringtone must be copied from flash memory into RAM.[400]

Virgin Mobile argued that its reproduction rights in the mobile phone operating system and other software are infringed when a customer unlocks the handset and uses it with another carrier. It contended that the handsets cannot be used without using the operating system, and use of the operating system entails making copies of it in RAM. It also asserted that the use of any other application or content on the handset also entails making copies. It argued that when a consumer unlocks the handset (without reflashing the entire operating system) and continues to use software on the handset, she is making reproductions that exceed the scope of her license to the software. It concluded that those reproductions are in clear violation of Virgin Mobile's Terms of Service, and, accordingly, are infringing.[401]

The Derivative Work Right. Virgin Mobile also argued that reflashing may, in some cases, modify the firmware in the mobile phone and in such cases the end result is a new derivative work.[402] CTIA noted that in some cases, unlocking involves the use of a "patched version" of the bootloader and firmware, and asserted that a patched version is "a modification … a derivative work, and I daresay an unauthorized one at that, that you need to load on the phone, in other words make a copy, in order to unlock the phone."[403]

MetroPCS came to the opposite conclusion and asserted that reflashing a handset does not change the underlying mobile phone software, but merely changes the underlying variables accessed by the program.[404] Cricket stated that no copies are made of the phone's firmware when it is unlocked. It asserted that the action of unlocking allows the individual to update the preferred roaming list and it does not affect the firmware on the phone, the bootloader, or the operating system. It commented that since the PRL is simply a file that gets updated, no infringement takes place.[405]

---

[400] R51 (Virgin Mobile) at 18-19; Response of Virgin Mobile to Copyright Office Questions relating to Cellphones of July 13, 2009, at 7-11.

[401] *Id.* CTIA also alluded to the reproduction issue. R43 (CTIA) at 30. As discussed below, CTIA also referred to copying in its discussion of Section 117. *Id* at 31. *See also* T Joseph, 5/8/09 at 131.

[402] R51 (Virgin Mobile) at 15-17.

[403] T Joseph, 5/8/09, at 131. *See also* R43 (CTIA) at 30 as well as CTIA's discussion of Section 117 at 31-33.

[404] C5B (MetroPCS) at 6.

[405] T Inglish, 5/8/09, at 82, 195.

The iPhone is a GSM device that is exclusive to AT&T's wireless network in the United States. It has a SIM card, as do most other GSM phones, but it appears that it is a more complicated task to unlock this type of phone than to unlock the average mobile phone.[406] EFF stated that in the case of the iPhone, the SIM carrier lock is enforced by the baseband system firmware on the iPhone. Utilizing unique identifiers burned into the baseband system's Infineon SGold CPU and associated memory chips, the firmware establishes an area in memory known as the "seczone" where encrypted information about the SIM lock status is kept. According to EFF, the "seczone" contains policy information about which SIMs may be used with a particular phone, and related technical information. It asserted that the only difference between iPhones tied to different carriers is the contents of this "seczone," as the firmware and hardware (other than the unique tokens burned into the SGold and associated memory chips) are identical across all same-model iPhones. EFF stated that Apple relies on a "chain of trust" between the baseband system's bootrom, bootloader, and firmware, which is enforced by cryptographic signature checking, to prevent any unauthorized software from loading on the baseband system, thereby preventing an iPhone owner from modifying the "seczone" carrier lock data.[407]

EFF asserted that, despite this design, both the "first generation" 2G iPhone and the "second generation" 3G iPhone can currently be "unlocked" by their owners using widely available and relatively easy-to use software. It stated that the most popular software for this purpose is Pwnage (for the 2G iPhone) and yellowsn0w (for the 3G iPhone). EFF commented that because the restriction framework used in the 2G iPhone differs from that used in the 3G iPhone, the corresponding unlocking techniques are different.[408]

EFF stated that for the 2G iPhone, the user installs a "patched" version of Apple's baseband firmware that does not enforce the SIM carrier lock. It commented that this is possible because the bootrom in the baseband system does not perform a signature check on the bootloader

---

[406] GSM mobile phones use a SIM card, which is a small device that stores a customer's identifying information in the handset. According to the Wireless Alliance, the card is easily removed and replaced. A customer with a SIM card phone can easily select service providers by popping the appropriate card in the handset. The network reads the card, allows the connection, and collects accurate billing information from the card. AT&T and other carriers program their handsets with SIM carrier locks to prevent them from operating if a different SIM card is inserted into the handset. C5D (Wireless Alliance) at 8-9. According to the record, all that is needed to permanently free this type of mobile phone from its original wireless network is an "unlock code." An example of a unlock code for a handset is: 38123134. After inputting that code, a consumer can use any SIM card from any compatible network to enable new service. R25 (Han) at 1-2. Han is the founder and former general manager of the UnlockCellphone.com web site and has notable experience in this subject.

[407] R49 (EFF) at 12.

[408] *Id.* at 13.

before loading it. It further commented that the Pwnage tool substitutes a "patched" version of the bootloader when the phone is turned on, which in turn, loads a "patched" version of Apple's baseband firmware that suppresses the SIM carrier lock.[409]

EFF stated that for the 3G iPhone, Apple improved the "chain of trust" in the baseband system, reengineering it to require that the bootrom perform a signature check on the bootloader before loading it. EFF asserted it is more difficult to substitute a "patched" version of the baseband firmware in place of the unaltered version. It noted, however, that an owner of a 3G iPhone can currently unlock it using an application known as yellowsn0w, which "injects" software into the baseband system memory while the firmware is operating (*i.e.*, "on-the-fly code injection"), thereby suppressing the operation of the SIM carrier lock.[410]

Joint Creators and CTIA have both argued that a patched version of the iPhone's firmware constitutes an unauthorized derivative work.[411]

c. Section 117

Proponents of the proposed class responded to the opponents' arguments regarding infringement of the reproduction and derivative work rights in the firmware by asserting that any such acts are permitted under Section 117 of the Copyright Act.[412] To reiterate, the pertinent

---

[409] *Id.*

[410] *Id.*

[411] *See* T Metalitz, 5/1/09, at 157 ("But if you look at Exhibit A, page 13, [of EFF's responsive comments] it seems pretty clear that what is happening here in installing a patched version of Apple's-based band firmware, using the Apple, for example -- and this is about unlocking, not jailbreaking, if you will; this is about access to the network, and it states that this is basically identical to Apple's code, except -- and then there are some differences. So, it seems to pretty clearly to [sic] make the case that a derivative work is being prepared, or an adaptation is being prepared."); *see also*, T Joseph, 5/8/09, at 131 (stating the same).

[412] The Register has declined to fully address the applicability of Section 117 in the case of the similar proposed class of "Computer programs that enable wireless telephone handsets to execute software applications …," because proponents of that class had made a persuasive case that the conduct in which they wished to engage constitutes fair use. In contrast, the proponents of this class did not make such a case. At most, proponents intermittently *referred* to fair use when addressing the action of unlocking a mobile phone for the purpose of using the device on another wireless network. *See* C5B (MetroPCS) at 7 (Customers who reflash their handsets are "making a noninfringing, fair use of copyrighted works that they rightfully own."). In fact, one proponent invited the Register to engage in a fair use analysis as part of the process of establishing the framework for a possible new exemption, but failed to offer any analysis of its own. R44 (Pocket) at 8 ("[W]e respectfully request that the Office attempt to clarify the intended meaning of the word 'lawfully' [to encompass] purposes that either do not infringe or are fair uses of the copyrights in the Device's programming."). *See also*, T Granick, 5/1/09, at 151 ("I could go through the fair-use factors, but I think one of the most important things to point to is there is no market for this firmware outside of the handset.") If Ms. Granick had "go[ne] through the fair-use factors," she might have made a sufficient case to permit the Register to consider whether, as argued, "fair use applies." *See id.* Opponents of the

language of Section 117(a) is as follows:

> Notwithstanding the provisions of section 106, it is not an infringement for the owner of a copy of a computer program to make or authorize the making of another copy or adaptation of that computer program provided:
>
> > (1) that such a new copy or adaptation is created as an essential step in the utilization of the computer program in conjunction with a machine and that it is used in no other manner, or
> >
> > (2) that such new copy or adaptation is for archive purposes only and that all archived copies are destroyed in the event that continued possession of the computer program should cease to be rightful.[413]

EFF asserted that "[t]o the extent that any …exclusive rights are implicated, 17 U.S.C. § 117 authorizes the owner of a copy of a computer program to make a new copy or adaptation as an essential step in the utilization of that program with a machine."[414] EFF asserted that even if reprogramming through reflashing is viewed as making an adaptation of the copyrighted work, the adaptation is non-infringing because under Section 117, the owner of a copy of a software program has the right to modify the source code of that program, including "add[ing] features to [the program that were not present at the time of rightful acquisition." It argued that in***]** *Krause v. Titleserv*,[415] the Second Circuit held that the rightful possessor of a copy of a software program can make modifications and improvements to that program. It concluded that as with the defendant in *Krause*, the consumer is the rightful possessor of the work (embedded in the phone) and simply wants to modify her copy of firmware to better meet her needs. It argued that this is a noninfringing use under Section 117.[416] EFF also asserted that the purchaser of a mobile phone is the owner of the phone; she has the right to keep and use the phone forever, and no wireless provider ever puts restrictions on the purchaser's disposal of the phone. Therefore, EFF

---

proposed class referred to fair use, but did not present any arguments as to why fair use does not apply here, presumably because proponents had not offered any case on fair use for them to rebut. Because no case has been made that fair use is applicable here, the Register cannot resolve the request to designate this class on that basis and must address the applicability of Section 117, on which issue has been joined.

[413] 17 U.S.C. § 117(a).

[414] Post-Hearing Response of EFF to Copyright Office Questions relating to Cellphones of July 13, 2009, at 7.

[415] 402 F.3d 119, 129 (2d Cir. 2005), *cert. denied*, 126 S. Ct. 622 (2005). *Krause* is also discussed *supra*, pp. 82, 89-90.

[416] C5D (Wireless Alliance) at 10, citing *Krause v. Titleserv, Inc.*, 402 F.3d 119, 125-26 (2d Cir. 2005).

* Corrected text. This line was inadvertently omitted from the memorandum delivered to the Librarian of Congress on June 11, 2010, which was originally posted on the Copyright Office website. Correction posted 8/30/2010.

concluded, the purchaser is entitled under Section 117 to continue to use the firmware on the phone even after her relationship with the wireless carrier has terminated.[417]

MetroPCS argued that even if a minor, write-only operation (resulting from reflashing) were to be construed as changing the underlying mobile phone operating system code, such changes would be permitted under Section 117 so long as they were solely for the purpose of enabling the consumer to choose the carrier's network to support use of his or her device. It asserted that Section 117(a)(1) permits the alteration of copyrighted computer programs provided that "such a new copy or adaptation is created as an essential step in the utilization of the computer program in conjunction with a machine and that it is used in no other manner." It argued that reflashing is an action permitted under the law since the changes being made to the mobile phone software are identical to the ones made routinely by the original wireless carrier to make the mobile phone operate on its network.[418]

Virgin Mobile argued that reliance on Section 117 is inapt because the handset purchasers are not owners of the software for purposes of Section 117. It argued that ownership is not determined according to whether or not one owns the device on which the software resides or on title alone, but depends on whether the party "exercises sufficient incidents of ownership."[419] It asserted that the case law makes it clear that software that is purchased with contractual limitations on its use is not sold, but is licensed.[420] It noted that in *DSC Communications Corp. v. Pulse Communications, Inc.*,[421] the Federal Circuit explained that the possessor of a copy is not an owner for purposes of Section 117 where an agreement prohibits the possessor of the copy from using the software other than as provided by the copyright holder. It asserted that in *DSC Communications*, the licensee was limited to use of the software "solely in conjunction with the

---

417 T Granick, 5/1/09, at 150-51.

418 C5B (MetroPCS) at 8. *See* 17 U.S.C. § 117(a)(1).

419 R51 (Virgin Mobile) at 23, citing *Krause*, 402 F.3d at 124. *See* T Lurie, 5/1/09, at 215 ("Under 117, the customer is not the owner of the software. They have a license to it.").

420 Post-Hearing Response of Virgin Mobile to Copyright Office Questions relating to Cellphones of July 13, 2009, at 14, citing *DSC Commc'ns Corp. v. Pulse Commc'ns, Inc.*, 170 F.3d 1354, 1360 (Fed. Cir. 1999) (agreeing with non-ownership holdings in *MAI Sys. Corp. v. Peak Computer, Inc.*, 991 F.2d 511, 518 (9th Cir. 1993) and *Advanced Computer Servs. of Mich. v. MAI Sys. Corp.*, 845 F. Supp. 356, 367 (E.D. Va. 1994)).

421 *Id.*

Material (*i.e.*, the Lifespan-2000 and related equipment) during the useful life of the Material."[422] It argued that this is exactly the case here: a customer purchasing a handset is permitted to use the software preloaded on the handset only in connection with a particular service and is not allowed to alter it in any way, among other limitations, and thus the handset purchaser is not an "owner" of the software for purposes of Section 117.[423]

CTIA also argued that the uses that proponents wish to make of the wireless handset firmware are not noninfringing under Section 117. It stated that Section 117 permits adaptation or copying of software only as an "essential step in the utilization of the computer program" and only when "it is used in no other manner." It asserted that in this circumstance, mobile phone users already are successfully using the firmware "in conjunction with a machine," with their current service provider and with authorized software, and the device is operating as intended.[424] It added that under the plain terms of the statute, circumvention is not an "essential step in the utilization of" that firmware "in conjunction with a machine." It also argued that Section 117(a)(1) insulates from copyright liability only those software modifications necessary to enable the software to operate with the purchaser's machine in the manner "for which it was both sold and purchased."

According to CTIA, Section 117 does not provide an open-ended invitation to modify already-functioning firmware to permit a handset to operate with another carrier or with other software with which it was not intended or designed to operate. CTIA stated that at least some of the proponents were seeking to apply the statute to activities that are specifically outside the scope of the statute, which limits use of Section 117(a)(1) adaptations to personal, internal use and forbids the transfer of such adaptations to third parties. It concluded that because the changes authorized by Section 117 are for personal use only, any such commercial distribution of modified firmware in and of itself removes the firmware adaptations from the scope of the law's protection.

---

[422] *Id.*

[423] CTIA characterized "whether or not the owner of the phone is the owner of the software or a licensee of the software" as an "interesting question," observing that there are "cases that suggest that where there are severe restrictions or significant restrictions on use, such as don't use the phone on a different network, that that is one indicium, at least, that you don't have ownership of the kind that Section 117 was contemplating." T Joseph, 5/8/09, at 171.

[424] R43 (CTIA) at 31-33. Virgin Mobile also stated that its customers do not need to make any copies or modifications if the handset is used as intended with Virgin Mobile's service. Post-Hearing Response of Virgin Mobile to Copyright Office Questions relating to Cellphones of July 13, 2009, at 13.

i. Ownership

As noted in the discussion of the proposed class of "Computer programs that enable wireless telephone handsets to execute software applications …,"[425] one of the key factors in determining whether Section 117 applies in this instance is whether the mobile phone consumer owns the copy of the computer program, which, in this instance, is the firmware. It is undisputed that the consumer has purchased and owns the hardware, that is, the mobile phone device. In this case, the consumer can dispose of the device in any manner she deems appropriate either by discarding it, selling it, or giving it away. Moreover, it seems apparent that ordinarily the owner of a device on which the copy of the firmware is fixed is also the owner of that copy.[426] Thus, in the absence of any additional facts, the fact that a person has purchased a mobile phone would appear to resolve the question whether that person owns the copies of any software fixed within that phone.

However, in the context of Section 117, the matter of ownership of a copy of a computer program is more nuanced, and the case law interpreting this provision is inconsistent.

Krause v. Titleserv[427] has been cited by proponents and opponents of the proposed class as key precedent in determining ownership of computer programs.[428] In *Krause*, the court stated that "it seems anomalous for a user whose degree of ownership of a copy is so complete that he may lawfully use it and keep it forever, or if so disposed, throw it in the trash, to be nonetheless unauthorized to fix it when it develops a bug, or to make an archival copy as backup security."[429] Rather than looking to formal title as an "absolute prerequisite to qualifying for § 117(a)'s affirmative defense … [i]nstead, courts should inquire into whether the party exercises sufficient

---

[425] *Supra,* p. 78.

[426] *See* 17 U.S.C. § 101 (definition of "copies": "'Copies' are material objects … in which a work is fixed by any method now known or later developed, and from which the work can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device."). When software is loaded onto a device such as an iPhone, the device itself (or some part of that device, such as a hard drive) is the material object in which the software is fixed.

[427] 402 F.3d 119 (2d Cir. 2005).

[428] T Granick, 5/1/09, at 150, 174, 216-17; T Lurie, 5/1/09, at 217. However, the witness testifying on behalf of CTIA, while accepting that *Krause* is controlling law in the Second Circuit, refused to accept "that *Krause* has settled the law." T Joseph, 5/8/09, at 175. Therefore, unlike the situation with respect to class of "Computer programs that enable wireless telephone handsets to execute software applications …," the proponents and opponents of this proposed class have not agreed that *Krause* is necessarily "good law."

[429] *Krause*, 402 F.3d at 123.

incidents of ownership over a copy of the program to be sensibly considered the owner of the copy for purposes of § 117(a). The presence of formal title may of course be a factor in this inquiry, but the absence of formal title may be outweighed by evidence that the possessor of the copy enjoys sufficiently broad rights over it to be sensibly considered its owner."[430]

The Second Circuit in *Krause* relied heavily on its decision in *Aymes v. Bonelli* ("*Aymes II*"), where the Second Circuit originally recognized that Section 117 entailed a nuanced analysis.[431] In *Aymes II*, where a computer programmer brought action against a corporation alleging that the corporation had infringed the copyright in his computer program, the Second Circuit focused on distinguishing between the copyrighted computer program and a copy of the computer program.[432] The court ultimately determined that the defendants were rightful owners of a copy of the plaintiff's copyrighted computer program and accordingly, did not infringe upon the plaintiff's copyright because the changes made to the defendants' copy of the program were necessary measures in their continuing use of the software in operating their business.[433] The court further determined that the defendants properly modified their copy of the program to suit their own needs[434] and their adaptations were essential to allow use of the program for the very purpose for which it was purchased.[435] The court noted specifically that "the modifications here fall easily within the contemplation of CONTU"[436] including the Commission's view that "a right

---

[430] *Id*. at 124.

[431] 47 F.3d 23 (2d Cir. 1995) (involving the second time the case went up to the Second Circuit, and thus referred to as *Aymes II*). The case involved computer programs written by Aymes for Island Recreation Inc. and its president Jonathan Bonelli. The programs were collectively called CSALIB and were designed to facilitate Island's inventory, record-keeping, and sales efforts in Island's business of operating a chain of retail stores selling swimming pools and related supplies. Aymes claimed, *inter alia*, that Bonelli agreed to only use the programs on one computer and agreed to grant Aymes the exclusive right to modify the programs. Also important to the case was the fact that Island paid Aymes to design a program specifically for Island's use, and for those efforts Aymes was paid in excess of $70,000.

[432] *Id*. at 25.

[433] *Id.* at 26.

[434] The court noted that "[u]ntil this lawsuit Aymes never sought to prohibit others from making modifications to the programs, although for some time he had been aware that Island had hired another programmer to convert and modify CSALIB." *See* 47 F.3d at 27.

[435] *Id.* at 27.

[436] *Aymes v. Bonnelli*, 47 F.3d 23, 26 (2nd Cir. 1995). CONTU was the "National Commission on New Technological Uses of Copyrighted Works." Congress established CONTU in 1974 to perform research and make recommendations concerning copyright protection for computer programs, and Section 117 was enacted on the recommendation of CONTU. The CONTU Report has been treated as tantamount to a legislative history of Section 117. *See Vault Corp. v. Quaid Software, Ltd.*, 847 F.2d 255, 259-61 (5th Cir. 1988). However, Congress changed

to make those changes necessary to enable the use for which it was both sold and purchased should be provided."[437] The court emphasized the right to modify and add features to a work and the internal or private nature of the adaptation.[438]

For purposes of Section 117, the distinction between the owner of the *work* and the owner of a *copy* of a work is critical. The Second Circuit in *Krause* confirmed that this determination of ownership is not based solely on formal title, but rather on "the various incidents of ownership."[439] The characterization of formal title is relevant, but not determinative here; nevertheless, its relevance is limited to formal title of the "copy" of the computer program. Even if evidence of formal title to the copy is present, courts must also assess the various incidents of ownership. In particular, the Second Circuit looked to a number of factors to determine the status of a copy of a work, including: (1) whether substantial consideration was paid for the copy; (2) whether the copy was created for the sole benefit of the purchaser; (3) whether the copy was customized to serve the purchaser's use; (4) whether the copy was stored on property owned by the purchaser; (5) whether the creator reserved the right to repossess the copy; (6) whether the creator agreed that the purchaser had the right to possess and use the programs forever regardless of whether the relationship between the parties terminated; and (7) whether the purchaser was free to discard or destroy the copy anytime it wished.[440] As noted above in the discussion of the proposed class of "Computer programs that enable wireless telephone handsets to execute software applications …," other courts have taken different approaches to what is "ownership" for purposes of Section 117.[441]

---

one word from the provision recommended by CONTU, which used the term "rightful possessor" rather than owner. *Id*. at 261 n. 11. There is nothing in the legislative history of Section 117 that explains Congress's reasons for making this change in terminology. *See Krause*, 402 F.3d at 122-23.

[437] *Aymes*, 47 F.3d at 26, citing CONTU Report at 13.

[438] CONTU Report at 13. (According to the CONTU Report, copyright laws should reflect the fact that transactions involving computer programs are entered into with "full awareness that users will modify their copies to suit their own needs." This right of adaptation includes "the right to add features to the program that were not present at the time of rightful acquisition", and was intended to apply to modifications for internal use, as long as the adapted program is not distributed in an unauthorized manner.)(citations omitted).

[439] *Krause*, 402 F.3d at 123.

[440] *Id.* at 124.

[441] *See, e.g., Wall Data Inc. v. Los Angeles County Sheriff's Dep't*, 447 F.3d 769 (9th Cir. 2006) (if "severe restrictions" are imposed on the use or transfer of the copy, then the transaction is a license, not a sale, and the purchaser of the copy is a licensee, not an "owner" within the meaning of Section 117); *MAI Sys. Corp. v. Peak Computer, Inc*, 991 F.2d 511 (9th Cir. 1993) (finding simply that "[s]ince MAI licensed its software, the Peak customers do not qualify as 'owners' of the software and are not eligible for protection under § 117"); *see also, DSC Communications Corp. v. Pulse Communications, Inc.*, 170 F.3d 1354, 1360-61 (Fed. Cir. 1999) (rejecting "the

Moreover, in *Vernor v. Autodesk, Inc.*,[442] a recent case from a district court in the Ninth Circuit interpreting that circuit's case law, the court found a conflict in Ninth Circuit cases on the question of ownership of a copy of a work. The court resolved the conflict by applying the Ninth Circuit rule that the "oldest precedent among conflicting opinions from three-judge Ninth Circuit panels" must be applied.[443] Following the oldest precedent, the court held that the "*MAI* trio" (which included *Wall Data*) cannot be reconciled with *Wise* (the earlier case), and that *Wise* was the controlling precedent that must be followed.[444] According to *Vernor*, *Wise* "establishes that even a transfer that places severe restrictions on the use and disposition of a copy of copyrighted material can transfer ownership of that copy."[445] The hallmark of a transfer of ownership was ability of the possessor of the copy to retain possession indefinitely, coupled with the failure of the copyright owner to retain the right to regain possession.[446] Although *Vernor* involved interpretation of the meaning of "owner" for purposes of Section 109 of the Copyright Act, the statutory codification of the first sale doctrine, the court concluded that "owner" has the same meaning for purposes of both provisions.[447] In fact, the conflict in Ninth Circuit caselaw that the court felt compelled to resolve was between cases addressing Section 117 (the *MAI* trio) and a case addressing Section 109 (*Wise*). *Vernor* is now on appeal to the Ninth Circuit, and it is therefore likely that the Court of Appeals will either resolve the conflict identified by the district court in *Vernor* or conclude that the cases can be reconciled with each other.

Ninth Circuit's characterization of all licensees as non-owners," but concluding that the particular contracts involved in the litigation "severely limit the rights of the RBOCs with respect to the POTS-DI software in ways that are inconsistent with the rights normally enjoyed by owners of copies of software," and that the possessors of the copies of the software were not owners of those copies).

[442] *Vernor v. Autodesk, Inc*., No. C07-1189, 2009 WL 3187613, 2009 U.S. Dist. LEXIS 90906 (W.D. Wash. Sept. 30, 2009)(finding a conflict between *United States v. Wise*, 550 F.2d 1180 (9th Cir. 1977) and what the court referred to as the "*MAI* trio," consisting of *MAI Sys. Corp. v Peak Computer, Inc.*, 991 F.2d 511 (9th Cir. 1995); *Triad Sys. Corp. v. Southeastern Express Co.*, 64 F.3d 1330 (9th Cir. 1995); and *Wall Data Inc. v. Los Angeles County Sheriff's Dep't*, 447 F.3d 769 (9th Cir. 2006)). *See also Vernor v. Autodesk, Inc.*, 555 F.Supp.2d 1164 (W.D. Wash. 2008) (earlier decision in the *Vernor* case); *UMG Recordings, Inc. v. Augusto*, 558 F.Supp.2d 1055 (C.D. Cal. 2008) (largely in accord with *Vernor*). Appeals to the United States Court of Appeals are pending in both *Vernor* (No. 09-35969) and *UMG* (08-55998).

[443] *Vernor*, slip op. at 19, *citing*, *United States v. Rodriguez-Lara*, 421 F.3d 932, 943 (9th Cir. 2005).

[444] *Id.* at 20.

[445] *Id.* at 9.

[446] *Id.* at 12.

[447] *Id.* at 20-24.

Given the variety of approaches adopted by different courts that have considered who may be the "owner" of a copy under Section 117, determining whether owners of mobile phones are also the owners of the copies of computer programs fixed in media on those phones is a difficult task. The record in this rulemaking offers evidence that some wireless carriers impose contractual restrictions on their subscribers that may well, at least in the view of some courts, be sufficient to deprive the subscribers of ownership of the copies of the software fixed on their handsets. At the same time, the record fails to contain such evidence with respect to all wireless carriers.

Virgin Mobile introduced the pertinent language from its "Terms of Purchase" and "Terms of Service." The Terms of Purchase includes the following language:

> You are permitted to use the software and content on this Virgin Mobile phone solely in connection with your use of the phone on our network expressly authorized by Virgin Mobile. Any use that exceeds this authorized use may infringe the rights of Virgin Mobile or its business partners. This phone is sold exclusively for use with service that Virgin Mobile USA provides.[448]

Virgin Mobile's Terms of Service provide:

> The software and content on the Virgin Mobile phones and devices, including the operating system, applications, data, information, music, games, images, text and other material, are owned by Virgin Mobile and/or its business partners. You are permitted to use this software and content solely in connection with your use of the Virgin Mobile phone on our network as expressly authorized under these Terms of Service. You may not distribute or upload any pre-loaded software or content to another device or transmit or broadcast the software or content, or otherwise copy or use the software or content in any manner not expressly authorized under these Terms of Service or, with respect to any downloaded content or applications, any other governing terms of use. If you violate any material term of these Terms of Service, including without limitation by using a Virgin Mobile phone or device on another network, by modifying any hardware or software on a Virgin Mobile phone or device, or by distributing, copying or otherwise using any of the software or content on a Virgin Mobile phone in a manner that is not authorized by these Terms of Service, your license to the software and content shall terminate immediately and your continued use thereof will constitute copyright infringement.[449]

These terms do appear to limit the Virgin Mobile subscriber's rights with respect to the software in ways that may be inconsistent with the rights normally enjoyed by owners of copies

---

[448] Post-Hearing Response of Virgin Mobile to Copyright Office Questions relating to Cellphones of July 13, 2009 at 9 n. 10.

[449] *Id.* at 9, n. 11; *see also* R51 (Virgin Mobile) at 9-10.

of software, most notably by permitting use of the handset only with Virgin Mobile authorized service. Under the Ninth Circuit's test as articulated in *Wall Data* and under the analysis of the Federal Circuit as articulated in *DSC Communications,* there is a reasonable likelihood that these provisions would be held to deprive the Virgin Mobile subscriber of ownership of the copies of the software residing on her phone. On the other hand, if *Vernor* correctly states the law with respect to who is the owner of a copy of software, the Virgin Mobile terms appear to fall short of retaining ownership in Virgin Mobile, since they do not appear to restrict the mobile phone owner's right to retain possession of the copy of the software. Finally, the result under *Krause* is unclear. The consideration paid for the copy most likely would not be considered "substantial," the copy is not created for the sole benefit of the purchaser, and it is not customized to serve the purchaser's use. On the other hand, the copy is stored on property owned by the purchaser (*i.e.*, the phone); the creator does not reserve the right to repossess the copy; and the purchaser is free to discard or destroy the copy any time she wishes. The record does not clearly reveal whether the creator agreed that the purchaser had the right to possess and use the programs forever regardless of whether the relationship between the parties terminated, although the provisions permitting use of the software only in connection with Virgin Mobile's service and network likely negate such an interpretation. In short, some of the *Krause* factors suggest that the owner of the Virgin Mobile phone also owns the copy of the software, while some of the *Krause* factors suggest that Virgin Mobile retains ownership.

Virgin Mobile is the only wireless carrier for which licensing terms were submitted for the record in the unlocking context. However, in connection with the proposed class for "Computer programs that enable wireless telephone handsets to execute software applications …," software licenses for Apple's iPhone were submitted for the record.[450] The iPhone is currently marketed in the United States only for use with AT&T's wireless service. According to Apple, restrictions in the iPhone software license require the conclusion that the owner of an iPhone does not own the computer software that operates the iPhone.

Apple's end-user license agreement states that the user owns the media on which the software resides, but Apple retains ownership of the software. Apple argued that this provision means that a purchaser only owns only the hardware, but is licensed to use the software in the prescribed manner. Apple contended that the license agreement demonstrates that the owner of an iPhone is simply a licensee of the copy of the computer programs on the phone and that as a licensee, Section 117(a) is inapplicable.

---

[450] Post-Hearing Response of Apple to Copyright Office Questions relating to iPhone modification of July 13, 2009, at 17-45.

Looking first to the license that Apple claims establishes that iPhone purchasers are merely licensees and not owners, it becomes clear that there is not one license, but in fact there are four versions of the license that must be examined. The critical language in all four iPhone license agreements is contained in sections 1 ("General"), 2 ("Permitted License Uses and Restrictions"), and 3 ("Transfer").

Section 1 of the first three versions of the agreement states, *inter alia*: "The software (including the Boot ROM code and other embedded software) . . . are licensed, not sold, to you by Apple, Inc. . . . .You own the media on which the iPhone Software is recorded but Apple and/or Apple's licensor(s) retain ownership of the iPhone Software itself."[451] The fourth version of the agreement omits the last sentence, and instead states: "Apple and its licensors retain ownership of the iPhone Software itself and reserve all rights not expressly granted to you."[452]

At first glance, this language might appear to resolve the issue because Apple clearly states that iPhone purchasers are licensees of the iPhone Software, and are not owners of the software; purchasers only own the media on which the iPhone Software is recorded. But with regard to the specific issue presented here, whether the iPhone purchaser is the "owner *of a copy* of the computer program," the license agreement is "not a model of clarity."[453] The license agreements (including the altered language in the fourth version) all make it abundantly clear that Apple owns the "software," but that language is ambiguous as to whether the word "software" refers to the copyrighted computer programs themselves or to the particular copies of those computer programs contained on the iPhone. Dictionary definitions of the term "software" do not clarify the meaning of this term in the contract.[454] The silence, or at least ambiguity, in the contract in relation to the meaning of this critical term is significant, because it is a maxim of contract construction that an ambiguous term in a contract is to be construed against the drafter.[455]

---

[451] *Id*. at 18, 25, and 33.

[452] *Id*. at 41.

[453] Post-Hearing Response of EFF to Copyright Office Questions relating to iPhone modification of July 13, 2009, at 10.

[454] Webster's New World College Dictionary (4th Ed.) defines "software" as "the programs, routines, etc. for a computer or computer system." Other definitions state that software can refer to anything on a computer that is not hardware.

[455] *In re Emery*, 317 F.3d 1064, 1070 (9th Cir. 2003); *Sun Microsystems, Inc. v. Microsoft Corp.*, 188 F.3d 1115, 1122 (9th Cir. 1999); see a*lso* Cal. Civ. Code § 1654. The Apple software license agreements recite that they are governed by California law.

Without more, it seems unlikely that an ambiguous provision reciting who owns the "software" is sufficient to justify the conclusion that Apple retains ownership of the copies of the software on each iPhone. Apple points out that its software licensing agreement also does not permit the sale or distribution of the software,[456] but the prohibition is subject to a significant exception permitting such a transfer in connection with a transfer of ownership of the iPhone itself. Thus, it appears that the owner of an iPhone may sell that iPhone, and that the sale may include the copy of the software that is on the iPhone.

Given those facts, it is not entirely clear whether the owner of an iPhone is also the owner of the copy of the software on the iPhone. Under the *Vernor* test, the answer would appear to be "yes." Apple argued that in another recent district court case, *MDY Industries, LLC,* the court held that no Section 117 rights existed where a license agreement provided that title to all copies of software remained with the copyright holder, the software could not be transferred except by transferring the original media along with the original packaging and manuals, and the transferee of the software had to agree to the terms of the license; provisions similar to provision in the iPhone license.[457] That case suggests that under the rule of the Ninth Circuit's "*MAI* trio," it is arguable that Apple might also retain ownership of the copy under its license. As with the Virgin Mobile license, the result in the Second Circuit under *Krause* is uncertain.

However, Virgin Mobile is only one carrier, and the iPhone is only one device (currently offered by only one carrier in the United States). The record with respect to other mobile carriers is spotty at best. CTIA has described some provisions contained in the contracts between its members and their subscribers, but with one exception, it does not identify any of the carriers. CTIA offered the following examples:

---

[456] Post-Hearing Response of Apple to Copyright Office Questions relating to iPhone modification of July 13, 2009, at 4.

[457] *MDY Industries, LLC v. Blizzard Entertainment, Inc.*, 2008 U.S. Dist. LEXIS 53988 at *26-28, 2008 WL 2757357 at *8-10 (D. Ariz., July 14, 2008). In a subsequent opinion, the same court stated that "[t]he Court recognizes that the Ninth Circuit may choose to reconsider its position on some or all of these issues during the appeal of this case." *MDY Industries, LLC v. Blizzard Entertainment, Inc.*, 2009 U.S. Dist. LEXIS 24151 at *7, 2009 WL 64971, at *2 (D. Ariz., March 10, 2009). The *MDY* case is now on appeal to the United States Court of Appeals for the Ninth Circuit, which has ordered that argument of the appeals in *Vernor* and *MDY* shall be before the same panel. Order, *MDY Industries LLC v. Blizzard Entertainment, Inc.*, Nos. 09-15932 and 09-16044, and *Vernor v. Autodesk Inc.*, No. 09-35969 (9th Cir., Dec. 23, 2009). In fact, the arguments of *MDY, Vernor* and *UMG* all took place before the same panel on June 7, 2010.

1. A pre-paid service contractually obligates the purchasers of its phones to use those phones only in connection with its service and prohibits tampering with the phone to enable use with another service.

2. Another major CTIA member's Wireless Service Agreement expressly provides: "You agree that you will not make any modifications to the Equipment or programming to enable the Equipment to operate on any other system." The agreement goes on to provide that the service provider may, in its discretion, modify the phone, and provides contact information if the customer is interested in using his or her phone on another system.

3. A third large carrier, which primarily only locks its pre-paid phones, includes in its pre-paid contract a provision that states "[y]our wireless phone . . . cannot be used with any other wireless service even if it's no longer used to receive our service."

4. T-Mobile's terms and conditions state that a "T-Mobile Device is designed to be used only with T-Mobile service; however, you may be eligible to have your Device reprogrammed to work with another carrier, but you must contact us to do so." The same Terms and Conditions prohibit "tampering with or modifying your Device," and "reselling T-Mobile Devices for profit, or tampering with, reprogramming or altering Devices for the purpose of reselling the Device."[458]

These provisions are similar in nature to the Virgin Mobile provisions. Given the uncertain state of the law relating to "ownership" for purposes of Section 117, it is difficult to predict with confidence whether a court would conclude who is the owner of the copy of the software on the phone in each of those cases.

The Register cannot and need not attempt to resolve that issue. The record does not require or, indeed, permit her to do so. The fact is that proponents of the proposed class have made a *prima facie* case that owners of mobile phones are also the owners of the copies of the software that are fixed on those phones and that as owners they are entitled to exercise the Section 117 privilege. With respect to iPhones and with respect to phones sold by Virgin Mobile and T-Mobile, opponents of the proposed class have arguably rebutted that case. But it is impossible to conclude from the record in this proceeding that the proponents' case with respect to ownership has been rebutted with respect to any other particular carrier. In other words, the Register cannot conclude that in all cases, or even in most cases, the wireless carrier retains ownership of the

[458] R43 (CTIA) at 33.

copies of the software that are fixed in the phones that they sell. Therefore, because the record requires the conclusion that a substantial portion of mobile phone owners also own the copies of the software on their phones, the Register must conclude those mobile phone owners may take advantage of the Section 117 privileges to make copies and adaptations of that software.

It is, therefore, necessary to turn to the question whether persons who use their phones on wireless networks, other than those first authorized by the wireless carriers that sold the phones, are engaging in noninfringing uses of the software on those phones when they (1) make copies of the software on their phones by turning them on, thereby causing copies to be made in the devices' RAM and (2) modify the firmware in order to enable the phone to communicate with the new network.

ii. Copies

It is not difficult to resolve whether the owner of a mobile phone who also owns the copies of software on the phone is engaging in a noninfringing use under Section 117 when she makes RAM copies of the software in order to operate the phone, even if she is operating it on another network. Section 117 unambiguously states that it is not an infringement for the owner of a copy of a computer program to make a copy when the making of that copy is an essential step in the utilization of that software in conjunction with a machine. Because the software cannot be used in the phone (a device that, for purposes of Section 117, qualifies as "machine") unless the RAM copies are made, the making of those copies clearly is an essential step in its utilization. As the CONTU Report stated:

> Because the placement of a work into a computer is the preparation of a copy, the law should provide that persons in rightful possession of copies of programs be able to use them freely without fear of exposure to copyright liability. Obviously, creators, lessors, licensors, and vendors of copies of programs intend that they be used by their customers, so that rightful users would but rarely need a legal shield against potential copyright problems. It is easy to imagine, however, a situation in which the copyright owner might desire, for good reason or none at all, to force a lawful owner or possessor of a copy to stop using a particular program. One who rightfully possesses a copy of a program, therefore, should be provided with a legal right to copy it to that extent which will permit its use by that possessor. This would include the right to load it into a computer and to prepare archival copies of it to guard against destruction or damage by mechanical or electrical failure. But this permission would not extend to other copies of the program. Thus, one could not, for example, make archival copies of a program and later sell some while retaining some for use. The sale of a copy of a program by a rightful possessor to another must be of all rights in the program, thus creating a new rightful possessor

> and destroying that status as regards the seller. This is in accord with the intent of that portion of the law which provides that owners of authorized copies of a copyrighted work may sell those copies without leave of the copyright proprietor.[459]

iii. Modifications, Adaptations and Derivative Works

As a general rule, anyone who wishes to switch her mobile phone from one network to another must alter some information embedded in the device. However, in a substantial number of cases those alterations do not appear to implicate Section 117. The principal reason for this conclusion is that the elimination and insertion of codes or digits, or completely reflashing a phone, cannot be considered an infringement of the computer program controlling the device. In the case of complete reflashing, deletion of the entire work (the firmware) and replacing it with an entirely new work does not implicate any of the exclusive rights in the deleted work. And, when specific codes or digits are altered to identify the new network to which the phone will connect, those minor alterations of data also do not implicate any of the exclusive rights of copyright owners.

When changes are made to uncopyrightable data that the computer program interacts with in order to perform a particular task (the data necessary to enable interoperability with devices, or as in this case, networks), such changes do not constitute infringement of the right to make derivative works based on the computer program. The codes that are changed are in locations that were created in order to contain variables. In other words, the computer program looks for, and interacts with, data in certain spaces or placeholders designed to contain variable information related to interoperability with mobile networks. The program will function regardless of which code is inserted. The fact that at one point a code is specified in one of these variable locations does not change the fact that these locations in the program are, and were, created to be variable. Taken out of the complexities of computer software, this situation is analogous to the song "Happy Birthday." In that song, there is a variable location in the lyrics into which a name is intended to be inserted. The name is not a part of the work, but rather the work is intended to include a variable so that alternate names can be inserted to achieve the purpose of the song. The same is true with respect to the computer programs running some mobile phones.[460]

---

[459] CONTU Report at 13.

[460] For instance, Verizon's handsets now have these variables set to zeroes solely to prevent problems for customers, however, customers may insert different variables in order to use the phone with a new provider.

Under a plain reading of the statutory language of Section 117, "adaptation" relates to changes that would, in the absence of Section 117, infringe the derivative right. This follows from the fact that adaptations that would not infringe the copyright in the computer program would not require an exemption. However, if the changes to the computer program would infringe the reproduction or derivative work right of the copyright owner of that computer program, those changes may be privileged under Section 117. This provision immunizes "a new copy or adaptation" that is created as an essential step in the utilization of the computer program in conjunction with a machine if the entity making the copy or adaptation is the owner of the particular copy of the computer program. If the firmware has been modified to a degree that it infringes the derivative work right, such an adaption may be permitted under Section 117 if it is made by the owner of the copy of the computer program and meets the other requirements of that section.

When the purchaser of a mobile phone is deemed to be the owner of the copy of the computer program contained on the phone, there are additional questions that must be answered with respect to adaptations that are necessary to use the handset with a new service provider and that affect the derivative work right. The next step in the analysis is to determine whether the adaptation comports with the statutory language in Section 117.

Despite the fact that in many cases it appears that the changes made to a computer program would not amount to an adaptation that would infringe the right to make derivative works, in some cases an adaptation of a computer program may be made in the course of altering the operating system that indeed could be considered an infringement of this right. In either situation, the question of whether or not the adaptation was noninfringing under Section 117 would depend on whether the "adaptation is created as an essential step in the utilization of the computer program in conjunction with a machine and that it is used in no other manner."[461] The question that must be resolved here is whether the adaptation is an essential step in the use of the machine.

The Second Circuit focused on the phrase "essential step in the utilization of the computer program in conjunction with a machine" in both *Aymes II* and *Krause*. Describing the analysis in *Aymes II*, the *Krause* court stated: "[w]e concluded that the modifications were essential to the defendants' utilization of the programs within the meaning of § 117(a)(1) because the adaptations were essential to allow use of the program[s] for the very purpose for which [they were]

[461] 17 U.S.C. § 117(a)(1).

purchased."[462] In assessing the case before it, the *Krause* court analyzed four types of modifications made by Titleserv in relation to the "essential step" language:

> The modifications allegedly made by Titleserv to its copy of the programs fall into four main categories: (1) correcting programming errors or "bugs," which interfered with the proper functioning of the programs; (2) changing the source code to add new clients, insert changed client addresses, and perform other routine tasks necessary to keep the programs up-to-date and to maintain their usefulness to Titleserv; (3) incorporating the programs into the Windows-based system Titleserv designed and implemented between 1997 and 1998; and (4) adding capabilities, such as the ability to print checks, and, to a limited degree, allowing customers direct access to their records, which made Titleserv's copy of the programs more responsive to the needs of Titleserv's business.[463]

The third category embraces the question of interoperability and the fourth category addresses the ability to add new features. In the case of adaptation of the copies of computer programs operating mobile phones, both categories are reasonably implicated. The interoperability at issue is not the kind that arose in cases involving personal computers on which operating systems or applications needed to be adapted for compatibility to the hardware. Rather, in the instant case, the operating system is already embedded in the "device" and works with that device as long it is used with the wireless service to which the phone is initially tethered. In order to connect to another service, it is generally necessary to change something relating to the program, and some changes may require adaptation of the program that implicates the right to make derivative works. Once connected to the new service, the reproduction of the copy or adaptation in RAM is "essential" for the operation of the device. In terms of the adaptation that may be necessary to connect to the new service, this may be considered analogous to providing new features to the existing, albeit functioning, program that only allows connection with a particular wireless network.

The *Krause* court declined to interpret the statutory language of "essential step in the utilization of the program in conjunction with a machine" narrowly. The court noted that the new features that were added "were not strictly necessary to keep the programs functioning, but were designed to improve the functionality in serving the business for which they were created."[464] The court rejected a narrow reading of "an essential step" as limited to those changes required to keep

---

462 402 F.3d at 125.

463 *Id.* at 125-126.

464 *Id*. at 126.

a program operational, finding that to read the statute so narrowly would require retreating from *Aymes II*.[465] As the court noted, the statute does not clearly indicate *for what end* modifications must be absolutely necessary. It looked at the broader context of the sentence and found that "as an essential step in the utilization of the computer program in conjunction with a machine" revealed that "essential" was related to "utilization." The court found that "utilization" might refer more broadly to "mak[ing][the program] useful" to the owner of the copy, in which case adding new program features to enhance functionality might qualify as an "essential step" in making the program useful."[466] Furthermore, the clause "utilization with a machine" was not limiting, but rather revealed that Congress might have been considering computer programs that could operate on devices other than computers, such as in automobiles, airplanes, and air conditioners.[467] Finding that the statutory language was ambiguous, the court looked to the legislative history behind Section 117.

The Second Circuit found that the pertinent passages in the CONTU Report "describe the right to modify programs in a manner that goes far beyond concern with compatibility and strongly suggests that the writers of the CONTU Report envisioned a loose concept of necessity that would encompass our very issue -- the addition of features so that a program better serves the needs of the customer for which it was created." Thus, the court found that the "right to add features to the program that were not present at the time of rightful acquisition" was consistent with an "essential step in the utilization of the computer program."[468]

The Register finds that this situation is analogous to the situation in *Krause*. Modifications to the firmware or software on the phone may be necessary to make the device functional with another service and better serve the legitimate needs of the customer. From a copyright perspective, these individual changes benefit the purchaser despite the fact that some wireless carriers would like to have complete control over the device by restricting its use to their service. But this was precisely the concern that was expressed in many parts of the CONTU Report -- that protection for computer programs had the capacity to lead to anti-competitive practices and that the use of copyright in computer programs was a means to that anti-competitive end.[469] This concern might even be greater with the advent of the DMCA and attempts to leverage the

---

[465] *Id.*

[466] *Id.* at 127.

[467] *Id.*

[468] 402 F.3d at 128, citing CONTU Report at 13.

[469] *See e.g.*, CONTU Report at 23.

copyright in largely functional computer programs in order to support anti-competitive business models in devices such as printer cartridges, garage door openers, or mobile phone services, or, in the future, in automobiles, refrigerators, and all sorts of other machines and devices.

An adaptation of the computer programs in the mobile phone, either firmware or software, may be an essential step to connecting to a new service. This use of the program increases its utility to the user and relates to the inherent need for interoperability with respect to computer programs that Section 117 intended to address, albeit in a changed and more complex technological environment from that which existed in 1980. Moreover, the reproduction of a copy or an adaptation in RAM is an essential step to the utilization of the program on the phone.

Nevertheless, in this context, it is important to recognize that the distribution of adapted software is limited by Section 117(b), which states:

> Any exact copies prepared in accordance with the provisions of this section may be leased, sold, or otherwise transferred, along with the copy from which such copies were prepared, only as part of the lease, sale, or other transfer of all rights in the program. *Adaptations so prepared may be transferred only with the authorization of the copyright owner*.[470]

Under Section 117, then, it is clear that any modifications that may be made to a computer program by an owner of a copy are limited to private use. That is, if a consumer does modify her mobile phone's firmware to such an extent that the changes implicate the derivative right, the device could not be transferred to anyone else with these adaptations. In this instance, Section 117(b) acts as a limitation on the first sale doctrine when adaptations of the software are made. In contrast, when no adaptations are made that would affect the derivative right (*e.g.*, merely changing codes in the variable sectors of the program or completely deleting or reflashing the proprietary software), there is no restriction in Section 117 on the alienation of those copies.

Based on the foregoing, the Register concludes that the proponents of this proposed class have met their burden of showing that the prohibition on circumvention has had an adverse effect on the ability of a substantial, albeit unknown, number of mobile phone owners who also are owners of the copies of firmware on their devices to engage in noninfringing uses of that firmware, specifically when they attempt to engage in the noninfringing use of connecting their phones to a new wireless network. The discussion will now turn to the factors enumerated in Section 1201(a)(1)(C).

d. The Section 1201 Factors

---

[470] 17 U.S.C. § 117(b) (emphasis added).

With one exception, the discussion of the four 1201 factors in the record was rather thin. Essentially, the Wireless Alliance argued that the four 1201 statutory factors weigh in favor of the requested exemptions. Virgin Mobile, on the other hand, argued that the four 1201 statutory factors weigh against the grant of the exemptions. CTIA's discussion of this topic centered on its assertion that the proponents of the proposed class had not made an affirmative case that the statutory factors disfavor designating the proposed class.[471] The positions of these parties are explained below.

Factor One

The Wireless Alliance asserted that there is no evidence to suggest that the availability of firmware for mobile phones would be adversely affected by the proposed exemption. In this instance, it stated, the firmware for such phones is not generally sold separately from the phones themselves.[472]

According to Virgin Mobile, the copyrighted works at issue here are the applications and content found on the mobile phone and the firmware. It contended that there is no demonstrated likely adverse effect of the Section 1201 prohibition on circumvention on the availability of software applications and content on mobile phones. However, Virgin Mobile asserted that an exemption could adversely affect the availability of proprietary applications on mobile phone handsets where it is not practical to apply separate technological measures to protect access to those works. Those assertions are addressed below in connection with the fourth Section 1201(a)(1)(C) factor, where Virgin Mobile offered similar arguments.

Factor Two

The Wireless Alliance asserted that there was no evidence to suggest that the availability (or lack of availability) of wireless phone firmware for non-profit uses would be harmed by an exemption that permits mobile phone users to unlock their phones to enable interoperability with the networks of multiple carriers. It further asserted that, in the wake of the 2006 exemption, there has been no evidence of a reduction in the availability of phone firmware for the statutorily-

---

[471] R43 (CTIA) at 24.

[472] C5D (Wireless Alliance) at 13.

specified uses. Virgin Mobile plainly stated that there is no demonstrable effect on any of these uses.

Factor Three

The Wireless Alliance asserted that there is no reason to believe that the availability (or lack of availability) of mobile phone firmware for criticism, comment, news reporting, teaching, or research purposes would be harmed by an exemption that permits mobile phone users to unlock their phones to enable interoperability with the networks of multiple carriers. Again, it claimed that in the wake of the 2006 exemption, there has been no evidence of a reduction in the availability of phone firmware for the statutorily-specified purposes.[473] Virgin Mobile repeated that there is no demonstrable effect on any of these uses.

Factor Four

The Wireless Alliance asserted that allowing customers to change networks has little to no adverse affect on the market for mobile phone-based software. It commented that a wireless carrier may claim it needs software locks because the carrier subsidizes the price of the handset and it wants to make up the differential by ensuring that the consumer stays with the carriers service. It noted, however, that every new mobile phone consumer signs a contract that provides for a minimum monthly fee and an early termination penalty. It asserted that these contracts ensure that wireless carriers will recoup, at a minimum, any subsidy provided to the consumer in her monthly fees. It concluded that a wireless carrier receives every legitimate benefit for the purchase subsidy it provides to its customers.[474]

Virgin Mobile stated that the software (including operating systems, proprietary applications and content available) on mobile phones is becoming increasingly sophisticated. It argued that the value of all of these works could be compromised if the handset is unlocked for purposes of connecting to an alternative wireless network. It also feared that stored content can be siphoned off the mobile phone and copied onto another device via a USB or serial port connection.[475]

---

[473] *Id.*

[474] *Id.*

[475] R51 (Virgin Mobile) at 36.

There was extensive discussion in the record pertaining to the substance and nature of preloaded and downloaded content (other than the firmware) such as ringtones, wallpaper, and other material typically loaded onto a mobile phone either before or after it is purchased. The main question presented was whether the access controls at issue--the locks–were necessary to protect such content. This was one subject that was not fully briefed and analyzed when the 2006 exemption was being considered.[476]

Virgin Mobile stated that its handsets are sold with content created by itself, the handset manufacturer, and an array of other developers.[477] It explained that customized software developed or acquired by Virgin Mobile includes copyrighted applications, such as Contact Vault (an address book back-up application), and several default ringtones. It further explained that the handset also may be loaded with other content, including games and background graphics created by third parties. It commented that the copyrights for such works may be held by a number of entities, but that all of these works are stored in "flash" memory on the handset.[478] Virgin Mobile was concerned that the proposed exemptions may open up such software and content to unauthorized copying.

Virgin Mobile stressed that the master subscriber lock, the TPM used to lock the mobile phone, is the same one that also protects the embedded file system where copyrighted content resides in the device. It stated that this shared TPM arrangement saves money and allows it to offer much less expensive handsets to its customers.[479] It asserted that it is not always feasible or

---

[476] *See* 2006 Recommendation of the Register of Copyrights at 53.

[477] Virgin Mobile noted that the operating system controlling its handsets may be a combination of third party software together with various programs developed by the handset manufacturer to allow the third party software to operate on the handset hardware. It added that the operating system software will also typically run a user interface that was customized and owned by Virgin Mobile, including various Virgin Mobile graphics displayed on the handsets. T Lurie, 5/1/09, at 207.

[478] Virgin Mobile explained that it sells ringtones under a licensing agreement with a music firm. It stated that it is contractually required to protect such content from unauthorized copying and distribution. It asserted that if the handset security is compromised, the security of such content may also be compromised, and Virgin Mobile would be in material breach of its contract. *Id.*

[479] Virgin Mobile noted that reflashing opens up the Preferred Roaming List and memory locations on the phone by allowing access to the embedded file system, thus exposing other copyrighted content. Ts Lurie and Buerger, 5/1/09, at 177. It added that DRM designed to protect individual content files would require significant engineering, technology, and development expenses which, in turn, would lead to increased handset costs. It asserted that an increase of just $10 in development costs necessary for a more advanced DRM system or chipset could double the retail price of a handset. Post-Hearing Response of Virgin Mobile to Copyright Office Questions Relating to Cellphones of July 13, 2009, at 3.

practical to provide additional protections on handsets for all copyrighted content and Section 1201 does not require any entity to use a particular type of TPM. Despite its protestations, and its concerns about unauthorized use, Virgin Mobile admitted that it is currently unaware of any rampant copying of the content on its mobile phones.[480]

CTIA stated that mobile phone locks foster copyright interests and protect copyrighted works. It specifically asserted that the locks help ensure that wireless carriers and manufacturers will invest in the development of new handsets, with new features and new applications. It commented that when handset locks are circumvented, the circumventer obtains access to all of the copyrighted content in a manner not authorized by the copyright owner. CTIA added that while it is possible in some circumstances to use encryption-based technology to provide additional protection for certain content, the obligation to decrypt the content each time it is accessed imposes additional power and processing burdens on the device that can degrade the consumer experience (*e.g.*, by limiting battery life).[481]

Joint Creators stated that content that comes preloaded in the mobile phone at the time of purchase, such as wallpaper, ringtones, and games, may not be the subject of concern in this context. They asserted that, in many cases, the full economic value of the licensing transaction between the content provider and the handset manufacturer and/or the network has already been liquidated. They noted, however, that there is still some concern about the use of content that was downloaded after the purchase of the phone on the initial network and certain subscription-based content that remains accessible on the new network. They were concerned that such material may be "ported" out of the phone and then shared with others on an unauthorized basis. They concluded that if an exemption is recognized, it must rule out any type of circumvention that would allow that type of activity.[482]

With regard to Virgin Mobile's claims, EFF argued that none of the carrier's exclusive rights are infringed when a customer uses her handset on another network because the content is not copied, but remains on the phone. It asserted that Virgin Mobile will only very rarely hold

---

[480] Virgin's witness was asked the following question at the May 1, 2009 hearing: "Are you aware of any cases where there has been, in fact, illicit copying of that content for perhaps redistribution to other people, apart from the use of the copy on that particular handset?" Peter Lurie responded: "I'm not aware of specific widespread trading….but it's certainly possible." T Lurie, 5/1/09, at 207.

[481] Post-Hearing Response of CTIA to Copyright Office Questions relating to Cellphones of July 13, 2009, at 2.

[482] T Metalitz, 5/8/09, at 135.

copyright in ringtones, which are almost always snippets of popular songs owned by the record labels and music publishers.[483] It further asserted that even for those few ringtones or for any user interface elements in which Virgin Mobile might own a copyright, none of its exclusive rights are infringed when a user uses her phone on a different service. EFF asserted that there is no evidence of infringement or harm to copyright interests since the 2006 exemption has been in effect. It further asserted that no party has demonstrated that copyrighted content has, in fact, been compromised.[484]

MetroPCS explained that it pays license fees for content embedded on its phones and the mobile phone consumer is entitled to make non-infringing use of that content. It asserted that whether a consumer accesses a ringtone while connected to her original wireless network or a competing network, the copyright owner has been paid the license fee for that work for use on that handset, and the consumer deserves to enjoy the benefits of that ringtone as long as she owns the handset. It further asserted that unlocking a mobile phone allows the consumer to have no greater use of the original copyrighted work than was originally licensed and she is permitted to continue to have access to the copyrighted work. It added that should copyright owners wish to add extra protection for their copyrighted works, there are no technological barriers to placing specific digital rights management tools on such works. It stated, in fact, that digital certificates are already in use on many handsets to protect copyrighted works.[485]

DRM for copyrighted content. In the discussions relating to the risks posed to preloaded and downloaded content, MetroPCS was not alone in arguing that works other than the firmware, such as ringtones, wallpapers, etc., can be protected by separate DRM. Much was said about whether the same access controls that protect the firmware ought to also protect such additional preloaded and downloaded content, or whether copyright owners or wireless carriers wishing to ensure that such content is protected should and could employ separate technological measures to protect those works.

EFF stated that almost every phone chipset sold today is hardware-capable of implementing file-specific digital rights management separate from the locks typically used to

---

[483] Post-Hearing Response of EFF to Copyright Office Questions relating to Cellphones of July 13, 2009, at 7.

[484] T Granick, 5/1/09, at 148.

[485] C5B (MetroPCS) at 16.

prevent a mobile phone user from switching carriers.[486] Because other carriers implement DRM on inexpensive chipsets, EFF stressed that there are practical and cost effective ways to control access to content (ringtones, wallpaper, etc.) while also permitting an exemption that does not interfere with carrier-switching.[487] Cricket added that copyrighted content is typically not integrated in the same fashion as the core software and utilizes standard Open Mobile Alliance ("OMA")[488] digital rights management protection methodologies.[489]

Virgin Mobile responded by stating that it does not, in fact, use such DRM on any of its low-cost handsets because of economic considerations. It further stated that its handset engineering team evaluated the established industry standard specifications for DRM to determine if any of its handsets could be said to meet any of those standards. Virgin Mobile commented that OMA has released requirements for three separate types of DRM: (1) "Forward Lock", (2) "Combined Delivery", and (3) "Separate Delivery." It stated that its low cost handsets do not meet any of the three specifications. Virgin Mobile then asserted that it does not implement Forward Lock, Combined Delivery and Separate Delivery because, among other reasons, content delivered to its handsets are not packaged in a DRM-required format.[490] It nevertheless noted that it might be possible to use DRM on its handsets if significant engineering efforts were undertaken, but nothing under the DMCA or copyright law requires it to do so.[491]

EFF asserted that other manufacturers that use chipsets identical to those found in Virgin Mobile's least expensive handset were able to practically and inexpensively protect their copyrighted works without having to resort solely to the carrier lock. It concluded that this clearly

---

[486] Post-Hearing Response of EFF to Copyright Office Questions relating to Cellphones of July 13, 2009, at 2.

[487] *Id*. at 1.

[488] OMA is the leading industry forum on developing inter-operability standards for the mobile device market. *See* http://www.openmobilealliance.org/

[489] Post-Hearing Response of Cricket to Copyright Office Questions relating to Cellphones of July 13, 2009, at 1. With respect to questions related to copyright concerns, CTIA asserted that technological protection is based on usage rules imposed by the content provider that are enforced by the phone's operating system, or by applications that are, in turn, protected by the operating system. It added that these technological protection measures often do not involve encryption, so the content remains "in the clear." Post-Hearing Response of CTIA to Copyright Office Questions relating to Cellphones of July 13, 2009, at 2.

[490] Post-Hearing Response of Virgin Mobile to Copyright Office Questions relating to Cellphones of August 28, 2009, at 4.

[491] *Id.* at 2.

demonstrates that there are practical and cost-effective ways to protect copyrighted works using DRM separate from carrier locks.[492]

Other Factors

In addition to the four enumerated factors, the statute includes an additional factor in Section 1201(a)(1)(C)(v): "such other factors as the Librarian considers appropriate." In the 2006 rulemaking, the Register stated that this "fifth factor" may be used to analyze exemption requests where the anticircumvention provisions were relied upon mainly to protect business interests rather than copyright interests.[493] In the present rulemaking, several parties filed comments raising a host of issues to consider as additional factors in the legal analysis.

Competition. Cricket asserted that mobile phone locks hurt competition because they effectively prohibit consumers from freely migrating to the wireless network of their choice. It stated that some prospective consumers are less likely to subscribe to Cricket's service if they are required to purchase a new wireless device solely for that purpose. Cricket concluded that it would be more difficult for it to attract new customers and to contend with other wireless providers in an already competitive market unless the current exemption is renewed for another three years.[494] Pocket agreed with this premise, asserting that a new exemption would foster competition in the communications industry, spur handset innovation, and lower costs for consumers.[495]

Small Business Development. eBay commented that an identified benefit of online marketplaces, like its own, is small business creation. It stated that the Internet provides entrepreneurs and small and medium-sized enterprises ("SMEs") with an opportunity to penetrate established markets and create new markets. It remarked that one of the categories on the eBay platform in which individuals and SMEs can offer goods is "Cell Phones and PDAs." It asserted that used phones have a greater chance for resale, and will appeal to a greater pool of potential

---

[492] Post-Hearing Response of EFF to Copyright Office Questions relating to Cellphones of September 18, 2009, at 2.

[493] *See* 2006 Recommendation of the Register of Copyrights at 52.

[494] R36 (Cricket) at 8-9.

[495] R44 (Pocket) at 4-5.

purchasers, if they are sold in an "unlocked" mode since the auction winner is then able to select the carrier of her choice. It believed that renewing the exemption will continue to foster competition in the wireless marketplace, continue to create opportunities for SMEs, and benefit consumers without adversely affecting copyrighted works. It concluded that a failure to renew the exemption will work the opposite result of harming consumers, eBay, and SMEs.[496]

Communications Law and Policy. The Public Interest Spectrum Coalition ("PISC") submitted that granting the proposed exemptions would promote open access policies considered by the Federal Communications Commission ("FCC").[497] PISC asserted that to deny the exemption would frustrate communications policy by allowing wireless carriers to violate consumer rights the government finds important. It concluded that in the absence of an exemption, the DMCA would undermine policies designed to promote innovation, consumer choice, and competition in the wireless industry. [498]

Skype, as a software-based communications service, supports open access policies that permit consumers to attach devices of their choice ("no locking") to any wireless network and use software applications of their choice on such devices ("no blocking"). It submitted that the proposed exemptions (*i.e.*, jailbreaking along with mobile phone unlocking) will ensure that copyright laws do not interfere with the "no blocking" and "no locking" open access principles. It argued that enabling a consumer to use her unlocked mobile phone on any compatible network and to use any legally-obtained software applications on her handset will ensure that she enjoys the benefits of consumer choice and wireless competition.[499]

---

[496] R27 (eBay) at 2.

[497] R41 (PISC) at 3. In an effort to preserve consumer rights, the FCC imposed open access conditions on the "C block" portion of the wireless spectrum sold at the 700MHz auction. These open access conditions require service providers who operate wireless networks in the spectrum to permit consumers and businesses to develop and use the devices and applications of their choice on those networks. PISC stated these open device and open application requirements benefit consumers by empowering innovation and consumer choice. *Id.* at 2-3. CTIA responded by stating that PISC has mischaracterized the FCC's current position. It asserted that the Commission has only applied the open access rules in very limited circumstances. It added that, in any event, it is unclear that the FCC's policies are inconsistent with the wireless industry's current subsidy-based business model. T Joseph, 5/8/09, at 163-164.

[498] *See also* Post-Hearing Response of EFF to Copyright Office Questions relating to Cellphones of July 13, 2009, at 1 (noting that the issue of phone portability continues to be of timely concern to the FCC and Congress, especially with regard to handset exclusivity deals).

[499] R52 (Skype) at 2-5.

Environmental and Global Concerns. The Wireless Alliance stated that thousands of mobile phones have been discarded every year because consumers are unable to use them if they switch wireless carriers. It asserted that the proposed exemptions would mitigate this "massive environmental waste problem" because more mobile phones will be re-used or recycled.[500] Finally, it asserted that the proposed exemptions could bridge the "digital divide" as unlocked handsets can be exported to impoverished nations for the poor to use.

CTIA argued that the alleged benefits advanced by the proponents, such as phone recycling, are being provided by wireless carriers regardless of an exemption.[501] It commented that the proponents point out the following benefits: (1) increased competition; (2) improved consumer choice; (3) consumer cost savings; (4) a cleaner environment; (5) revenue earning opportunity for charitable organizations; and (6) aid to developing nations. It asserted that none of these alleged "benefits" have anything to do with copyright, but instead "evidence a kitchen sink attempt to promote free-riding business models." It argued that such claims were irrelevant to the exemption analysis and should be disregarded. CTIA claimed that consumer choice and affordable wireless service were best promoted by ensuring that wireless carriers continue to have the incentive to subsidize and promote the development of diverse handsets.

Trademarks. On the other hand, CTIA claimed that circumvention violates a wireless carrier's trademark rights. It stated that when the protection measures on a device are circumvented and the device is altered to connect to a different service, the trademarks of the original service provider remain; as a result, anyone using the device is likely to be misled about the identity of the service being provided.[502]

Subsidies. Virgin Mobile asserted that the proposed exemptions, if approved, would have an adverse effect on the prepaid mobile phone business that provides subsidized, moderately

---

[500] C5D (Wireless Alliance) at 7. MetroPCS, as well as Pocket, also argued that reusing wireless handsets would also result in a cleaner environment.

[501] R43 (CTIA) at 34-39. CTIA stated that, with or without an exemption, wireless carriers would be engaged in recycling efforts. It asserted that there are thousands of retail establishments that accept all makes and models of wireless phones and accessories for authorized recycling. It claimed that the proponents' issue is not whether circumvention is needed to foster handset recycling; it is whether circumvention is needed to help proponents create a business out of recycling. *Id.* at 34. Virgin Mobile added that an exemption may preempt specific recycling conditions that wireless carriers often desire, such as the removal of any trademarks or copyrighted content from the phones subject to recycling. T Lurie, 5/1/09, at 163-64.

[502] R43 (CTIA) at 34.

priced handsets to lower-income, low-credit customers.[503] It asserted that without effective mobile phone locks, wireless carriers in this market niche cannot protect their reasonable investment. To put the matter into context, it explained that its wireless handsets are provided at a "highly subsidized retail price that is well below the per-unit cost"of acquiring the handsets from manufacturers.[504] It stated that this subsidy allows it to provide wireless service to lower-income customers, who otherwise may not be able to afford the significant capital outlay to begin wireless service or who may not have the credit history necessary to subscribe to other wireless plans. It commented that the subsidized phone, in combination with the prepaid wireless plan, allows many individuals to obtain a handset for emergency uses.

Virgin Mobile further stated that other carriers who provide wireless service under postpaid plans with contractual term commitments may be able to provide unsecured handsets upon purchase. It asserted that these wireless carriers have more flexibility as to whether and when to unlock various handsets; if a customer elects a longer term contractual plan, these providers can then adjust the subsidy applied for the handset. Virgin Mobile commented that unlike those carriers who have the built-in ability to adopt various pricing plans, it still must rely on locks as a means of supporting its subsidized mobile phone business model.[505]

EFF asserted that wireless carriers have locked both subsidized and non-subsidized phones they sell. It argued that this practice illustrates that locking is part of a business strategy, and not merely a matter of the carrier recouping subsidies on handsets it sells.[506]

---

[503] R51 (Virgin Mobile) at 8-9.

[504] Virgin Mobile stated that it pays manufacturers between $70 and $100 per handset, but sells them for as little as $15 to $20 per handset. It asserted that if the company were forced to sell its handsets without their current locks, the retail prices of such devices would at least quintuple. T Lurie, 5/1/09, at 125.

[505] R51 (Virgin Mobile) at 10-12. The subsidies issue was also addressed at the Copyright Office's hearing in Washington, D.C. In response to questions raised about whether the existing exemption reduced the industry's incentive to offer subsidized phones, CTIA counsel responded: "I don't think you can conclude one way or the other with respect to the past three years, and I do not have any specific evidence." He then stated that mobile phone locks are "one of the tools in the arsenal of the carrier to protect the subsidy and if the protection is weakened sufficiently, you can expect that it would follow as a logical matter that they would reduce the amount that they are willing to subsidize." T Joseph, 5/8/09, at 145.

[506] Post-Hearing Response of EFF to Copyright Office Questions relating to Cellphones of July 13, 2009, at 9.

Alternatives. CTIA argued that the availability of alternative means of access to competing wireless networks obviates the need for any exemption.[507] It pointed out that, under the law, an exemption will not be granted if there are alternatives that will allow the consumer to pursue the requested activity without circumvention. It stated that in this circumstance, the specific purpose of the consumer is to connect a phone to a particular network. It asserted that this purpose can be achieved without resorting to circumvention of access controls. In support of its assertion, it stated the following: (1) CTIA members, such as T-Mobile and AT&T, will unlock the phones of bona fide customers in appropriate circumstances; (2) in many cases, no "key" is needed because there are carriers, such as Verizon Wireless, that do not lock the majority of the mobile phones it offers to the public;[508] and (3) a third (unnamed) major carrier will unlock a customer's phone at the end of the customer's contract term and in certain other circumstances.[509] CTIA added that if a consumer seeks to connect to a wireless carrier of her choice, there are hundreds of phones that she can purchase in the marketplace.

EFF stated that CTIA's statements about alternatives are misleading because they obfuscate the facts. To counter the industry's assertions, EFF provided the following information on the current state of unlocking activities by various wireless carriers: (1) Verizon, due to a court settlement, sells all its post-paid phones with SPC in "unlocked" mode and freely distributes information about how to connect these devices to its wireless network; (2) Sprint is subject to an identical settlement, but it has not gone into effect because all appeals are not yet resolved (it will now unlock a phone at the end of the two year contract or upon payment of an early termination fee); (3) T-Mobile provides unlock codes to customers that have had 90 days of active service and meet a variety of unspecified requirements (but customers are not informed of this policy); and (4) AT&T (combined with Cingular) does not unlock its handsets (although class action

---

[507] R43 (CTIA) at 26-29.

[508] CTIA stated, for example, that Verizon Wireless does not lock the majority (96%) of its postpaid phones. Post-Hearing Response of CTIA to Copyright Office Questions relating to Cellphones of July 13, 2009, at 4. EFF noted that carriers in some instances implement SPC not to prevent customers from switching carriers, but to ensure that customers do not inadvertently change these settings since, if such settings are changed, the handset may not work on the original carrier's network. EFF stated that is why Verizon Wireless sets its SPC code to all zeros and advertises the code rather than have no code at all; in this way, post-paid Verizon handsets are sold "unlocked," but customers are protected from accidently modifying important network settings. Response of EFF to Copyright Office Questions relating to Cellphones of July 13, 2009, at 3.

[509] Post-Hearing Response of CTIA to Copyright Office Questions relating to Cellphones of July 13, 2009, at 4.

challenges regarding its practices have been pending for more than six years).[510]

Cricket implied that CTIA ignores the needs and desires of most mobile phone consumers. First, it stated that many consumers cannot afford to purchase a new phone, no matter how inexpensive the handset. Second, it asserted that a consumer has a vested interest in keeping her phone with all of her personal data and presets programmed in. Finally, it commented that consumers like to keep their existing telephone numbers on the phone that they already have, rather than switch phones and attempt to port their existing numbers to the new device.[511]

Conclusions regarding the Section 1201(a)(1)(C) factors. As was the case in 2006, the Register finds that the four factors enumerated in Section 1201(a)(1)(C)(i)-(iv) are neutral in this context. First, with respect to the second and third factors, nothing in the record indicates that the decision whether to designate the proposed class, in this context, would affect the availability of works for nonprofit archival, preservation, and educational purposes or impinge upon the ability to engage in criticism, comment, news reporting, teaching, scholarship, or research. With respect to the first and fourth factors, there was extensive discussion concerning whether permitting circumvention of software locks under the circumstances presented here would adversely affect the availability of and the market for preloaded and downloaded content. For the reasons that follow, the Register cannot conclude that there would be such an adverse effect.

While Virgin Mobile claims that the value of proprietary applications and downloaded content could be compromised if this class of works is once again designated under Section 1201(a)(1)(C) and (D), it does not adequately substantiate how this might be the case, and there is reason to be skeptical.

First, there is absolutely no evidence demonstrating that copyright owners of content found on mobile phones have been harmed by the current regulation designating this class of works. No mobile phone provider could clearly articulate how the exclusive rights granted to

---

[510] Response of EFF to Copyright Office Questions relating to Cellphones of July 13, 2009, at 8-9. AT&T has recently settled these pending class action suits. The settlement provides that AT&T agrees to give its eligible current and former customers codes that unlock all AT&T Wireless, Cingular, and AT&T mobility handsets, except for the iPhone and any handset that AT&T mobility introduces or has introduced for sale pursuant to a contract with a handset manufacturer that provides for an exclusivity period of 10 months or longer. Unlock codes for AT&T handsets will be provided to eligible postpaid customers who have completed a minimum of 90 days of active service and who are in good standing and current in their payments at the time of the request. *See* http://www.attlockinglawsuits.com/pdf/meolinot.pdf

[511] T Inglish, 5/8/09, at 85.

copyright owners for such content have been infringed because of the regulation. If the existing regulation has had deleterious effects on the availability of, or market for, the kinds of copyrighted content discussed above, presumably there would be examples to support such claims. Opponents of the proposal presented no such examples.

Moreover, the case has not been made that granting the proponents' requests will likely lead to infringing uses. CTIA and Virgin Mobile did not make a persuasive case that consumers are engaged in an infringing activity when they use or access content found on their existing phones after switching to a new carrier. As noted by the proponents, it is unlikely that infringement occurs when a mobile phone owner simply uses her phone, embedded with authorized content, on another wireless network. In this instance, the content has not been copied to a new device and the copyright owner has realized the economic benefit of the original license for use of such works. The mobile phone consumer, then, having already paid for and incurred the benefit of the license, can continue to use such copyrighted works on the mobile phone she owns. The same can be said of post-sale downloads. The mobile phone user has purchased such content, thus remunerating the copyright owner for her creation, and may use it on the device regardless of which mobile carrier the mobile phone owner uses.

Nor is there any evidence to suggest that the current regulation has impeded or will impede technological innovation and the creation of new content. Mobile phone providers, including Virgin Mobile as well as Apple with its iPhone, have broken new ground by providing consumers thousands of new applications since 2006. Competitive pressures and consumer demand will likely lead to even more novel applications in the future.

The record evidence also demonstrates that digital rights management software, apart from carrier locks, is available to protect discrete content found on, or downloaded to, mobile phone devices. Virgin Mobile apparently has made a conscious decision not to include separate security for content found on the phones it sells to the public. Virgin Mobile may have had sound business reasons for this decision and it certainly is not obligated to protect such content separately. However, in light of the availability of the alternatives discussed above and in light of the fact that Virgin Mobile has, for the past three years, operated while the existing regulation has been in place, the consequences of that decision, if any, appear to be of Virgin Mobile's own making and Virgin Mobile has apparently concluded that it can live with those consequences.

On this point, it is noteworthy that other wireless carriers have chosen to implement two separate technological protection measures, one for copyrighted content and another for the phone's operating system. Such separate measures would appear to be sensible in situations

where permitting a user to circumvent a technological protection that prevents the user from switching networks may also have the effect of removing protection from other content on the device. Taking such action would be particularly prudent where there is concern about access to particular works and an exemption currently exists, as is currently the case. Given that Virgin Mobile has freely chosen not to separately protect content on its devices despite the existence of the 2006 exemption, its actions appear to speak louder than its words. Under these circumstances, it is not credible to argue that permitting circumvention for purposes of using a mobile phone on another network puts other copyrighted content on the mobile phone seriously at risk.

It is important to emphasize again that wireless providers, like Virgin Mobile, have not demonstrated that they have been in any way harmed by the existing exemption.[512] In fact, CTIA stated that at least 55 lawsuits have been successful against resellers based on causes of action other than violation of Section 1201(a)(1). Although copyright owners are not required to prove harm, the absence of any cognizable harm where an exemption has been in place for the preceding three years is relevant to the overall balancing of interests. Speculation about future harm must be reconciled with the absence of any documented harm in a situation where the requested exemption is already in place.[513]

In any event, the four factors enumerated in Section 1201(a)(1)(C) do not weigh either in favor of or against designating the proposed class of works. The software locks do not appear to be deployed to protect the interests of the copyright owner or the value or integrity of the copyrighted work; rather, they are used by wireless carriers to limit the ability of subscribers to

---

[512] R43 (CTIA) at 5. Between June 2005 and June 2009, the wireless industry grew from 194.4 million subscribers to 276.6 million subscribers. Wireless penetration, measured by percentage of the total U.S. population over the same time period, increased from 66% to 89%. *See* CTIA, 100 Wireless Facts, http://www.ctia.org/advocacy/research/index.cfm/AID/10323. (Last visited 5/5/10.) The existing exemption has not stunted the growth of the wireless industry nor has it otherwise had an adverse effect on the wireless phone business model.

[513] In past proceedings, the Register has considered the lack of evidence that an existing exemption harmed rights-holders or affected the market for the relevant class of works as "instructive" or "informative" factors militating in favor of renewing the exemption. Such an evaluation has occurred in those circumstances where rights-holders have opposed the renewal of the exemption. *See* 2003 Recommendation of the Register of Copyrights at 30 ("In assessing the likelihood of harm to filtering software that would result from an exemption, the absence of any identifiable harm that resulted from the previous exemption is informative. While there is no burden on the opponents of exemption to show that a similar preexisting exemption has caused harm, silence on the issue may raise inferences."); *see also*, 2006 Recommendation of the Register of Copyrights at 35 (with regard to renewing the exemption concerned with computer programs protected by dongles, the Register stated: "It remains instructive that an exemption has been in place for the past six years, but opponents did not cite any evidence of harm resulting from that exemption, despite the proponent's evidence that the exemption has been put to use.").

switch to other carriers, a business decision that has little to do with the interests protected under copyright law.[514]

As was the case three years ago, because it appears that the opposition to designating the proposed class is based primarily on the desires of wireless carriers to preserve an existing business model that has little if anything to do with protecting works of authorship, it is appropriate to address the additional factor set forth in Section 1201(a)(1)(C)(v). However, the arguments made by the commenters and discussed above under the heading of "Other Factors" are unrelated to copyright interests. As such, they are not germane to the matters Congress was concerned with when it drafted Section 1201(a)(1) over a decade ago. Consumer choice and enhanced competition in the wireless marketplace, along with the other noted benefits, may be valid arguments to make before other administrative agencies, such as the FCC, but are inapt here, in a proceeding conducted by the Copyright Office and the Librarian of Congress, which have no responsibilities for, and no particular expertise in, such matters, and where the purpose of the proceeding is to address copyright law and policy concerns.

Speaking of other factors, the wireless industry has raised the possibility of trademark infringement as a reason to deny the exemption requests. Trademark violations are a valid concern, especially in the bulk reseller context, but this is not the forum in which to litigate or otherwise address such claims. Moreover, wireless carriers have obtained relief for trademark infringement against bulk resellers of their mobile phones.[515] As such, trademark concerns will not stand in the way of granting the exemption requests.

Moreover, the impact an exemption may have on the mobile phone subsidy model is not a proper factor that should be taken into account in the analysis. Here, Virgin Mobile has cogently explained how device locks protect its investment in the mobile phones it sells to the public. It is certainly understandable for wireless carriers to implement a variety of measures to retain their customer base and protect their profit margin. It may well be that, as Virgin Mobile asserts, the subsidy permits wireless carriers like itself to facilitate wireless service to low-income consumers.[516] But in this context, it is apparent that the main function of the software lock is to

---

[514] These are essentially the same conclusions the Register reached in 2006. *See* 2006 Recommendation of the Register of Copyrights at 50-51.

[515] *See, e.g., Virgin Mobile USA, LLC* v. *Blue Oceans Distrib., LLC,* No. CV06-511-S-EJL, 2007 U.S. Dist. LEXIS 10783 (D. Idaho Feb. 14, 2007); *TracFone Wireless, Inc.* v. *Dixon,* 475 F. Supp.2d 1236 (M.D. Fla. 2007); *TracFone Wireless, Inc.* v. *Bitcell Corp.*, No. 0722249- Civ., 2008 U.S. Dist. LEXIS 41955 (S.D. Fla. 2008) [all cited in R51 (Virgin Mobile) at 25 fn. 54]. *See also* T Lurie, 5/1/09, at 168, 170-73.

[516] *See* T Lurie, 5/1/09, at 124.

support a business model. The purpose of this rulemaking is not to protect such an interest or to maintain the profitability of a particular corporation or industry. Instead, the task here is to ascertain whether the use of access controls in this manner has an adverse effect on the ability of users of the proposed class to make non-infringing uses of works in that class, while also avoiding harm to copyright owners insofar as the prohibition is protecting their copyright interests in their works of authorship. As noted throughout, the ability of a mobile phone consumer to use her phone on alternative wireless networks, a noninfringing act, is indeed adversely affected. And, no opponent of the proposal has persuasively argued that the prohibition on circumvention is, in this context, protecting a copyright owner's interest in a work of authorship and that permitting circumvention for the purposes of switching mobile networks poses a serious risk to copyright owners' interests in protecting their works.

Finally, the record evidence demonstrates that there are no real alternatives for the relief an exemption would provide. First, wireless industry unlocking "efforts" do not adequately permit the non-infringing use desired by the proponents. The fact that Verizon now sells its postpaid mobile phones in unlocked mode hardly resolves the issue. There are still legacy phones connected to the Verizon wireless network that are locked and cannot be used on an alternative wireless network. Further, according to the record, AT&T, a major wireless carrier with millions of subscribers, still sells its phones in locked mode. Moreover, the evidence in the record suggests that most mobile phone carriers make it difficult for customers to switch networks. It seems clear that the primary purpose of the locks is to keep consumers bound to their existing networks. This observation is not a criticism of the mobile phone industry's business plans and practices, but simply a recognition of existing circumstances.

e. Defining the new class of works

Having concluded that the prohibition on circumvention of access controls does have an adverse effect on the ability of an owner of a wireless telephone handsets to engage in noninfringing uses of firmware in order to connect to a wireless telephone communication network other than the network of the wireless carrier that sold the handset to the owner, and having concluded that on balance, the factors set forth in Section 1201(a)(1)(C) favor the designation of a class of works that would permit handset owners to circumvent access controls in order to engage in such noninfringing uses, it is now necessary to determine how that class of works should be defined.

In assessing the proper scope of the class of works, it is appropriate to consider various formulations offered by both proponents and opponents of the proposed class, as well as concerns expressed about bulk resellers. NTIA's positions on the issues are explained and addressed as well. The language of the new class is then presented. The discussion ends with an examination of the relationship between contractual obligations, Section 1201(a)(2), and designation of the new class.

i. CTIA's Proposed Class of Works

CTIA asserted that the proper focus of the Section 1201(a)(1) rulemaking is on individual, noncommercial conduct. It added that the mobile phone industry's most significant concern is circumvention by phone traffickers and services that are attempting to free-ride on handset subsidies. It stated that its members do not foresee a situation in which they would bring a Section 1201 action against a bona fide individual customer who circumvented a handset lock solely in order to use his or her own phone on another service. For that reason, CTIA commented that it would not object to a narrowly targeted exemption to permit such circumvention.[517]

CTIA further commented that "it is essential that the exemption be carefully limited so that it cannot be used to foster destructive free-riding commercial activity, undermine exclusive distribution agreements, or facilitate bulk theft of handset subsidies through trafficking in new subsidized phones."[518] On this point, it asserted that certain parties have attempted to misuse the existing exemption to argue that the circumvention of handset locks is federal policy, preempting all other possible claims. It noted, for example, that MetroPCS has sued Virgin Mobile for a declaratory judgment, claiming that the 2006 exemption has broad effect and import, protecting its MetroFLASH service from a variety of causes of action.[519] It added that any such exemption should not condone breach of contract or allow circumvention that gives access to copyrighted works, beyond the works needed to allow use of the phone on the chosen network.

---

[517] *See* R43 (CTIA) at 44.

[518] *Id.*

[519] *Id.*, citing Complaint, *MetroPCS Wireless, Inc. v. Virgin Mobile USA, L.P.*, Case No. 08CV1658-D (N.D. Tex. Filed Sept. 19, 2008) According to CTIA, MetroPCS argued that the purpose of the 2006 exemption "is to ensure that customers have the freedom to switch wireless communications service providers" and that Virgin Mobile's user contracts "are thus pre-empted by the exemption in the DMCA." *Id*. ¶¶ 39, 40. It added that MetroPCS made a similar preemption claim with respect to tortious interference with contractual relations and prospective business advantage. *Id*. ¶¶ 47, 53.

CTIA submitted the following language as an alternative to the proponents' exemption proposals:

> *Computer programs in the form of firmware in wireless telephone handsets that restrict the handset from connecting to a wireless telephone communications network, when circumvention is accomplished by an individual customer of a wireless service provider for the sole noncommercial purpose, and with the sole effect, of lawfully connecting to a wireless telephone communications network or service other than that of the service provider, provided that (i) the individual complies with all of his or her contractual obligations to the service provider, and (ii) the individual does not thereby obtain access to works protected under this title beyond those necessary to connect to such a network or service*.[520]

EFF stated that CTIA has tacitly admitted that an exemption is warranted. It then opined that the only open question here is the scope of the new exemption. In this context, it believed that CTIA's narrow noncommercial language, as proposed above, would frustrate the intent of the exemption the Wireless Alliance originally proposed. It asserted that CTIA's formulation likely would not help mobile phone recyclers or the average consumer who would like to switch wireless providers using their existing device.[521]

EFF also voiced concerns about CTIA's contractual obligations clause. It stated that it would be difficult to enforce against mobile phone recyclers because, as firms taking phones given to them by individual consumers, they are not privy to a contract with a wireless carrier. It further stated that it would be difficult for courts to analyze Section 1201 claims to determine whether to grant motions to dismiss without performing fact-finding on the contractual issues. It added that such issues related to CTIA's proposal are not the interests that the copyright law seeks to vindicate; rather, they are related to business model interests that the Register recognized are separate from the Section 1201 stated interests.[522]

Discussion. The Register finds that the exemption language proposed by CTIA is too limiting to be adopted in its present form. Its dense wording is overly restrictive and imposes too many caveats for it to be of much use to its intended beneficiaries. For example, it is inappropriate to require the owner of the handset to have complied with all of his or her

---

[520] R43 (CTIA) at 44. Virgin Mobile stated that it would not oppose an exemption like the one proposed by CTIA even though it still believed that no exemption is warranted because the proponents have not met their burden of proof. Post-Hearing Response of Virgin Mobile to Copyright Office Questions relating to Cellphones of July 13, 2009, at 16.

[521] T Granick, 5/1/09, at 141-42.

[522] *Id*. at 142.

contractual obligations to the service provider; the focus in this rulemaking is on the ability to engage in noninfringing uses, not on whether a person otherwise qualified to take advantage of the exemption has breached any contractual obligations. Moreover, the proposed requirement that the individual "does not obtain access to works protected under this title beyond those necessary to connect to such a network or service" is overbroad and could render the exemption useless. A wireless carrier that chooses to use the same access controls both to deny users the ability to switch carriers and to protect other copyrighted works stored on the device would place the user in a situation whereby the mere act of circumvention in order to switch carriers would automatically give that person access to the other works as well. Moreover, the proposed language would not permit a person who has purchased a ringtone or a copy of some other copyrighted work that is stored on her mobile phone to continue to gain access to that work after she has changed carriers. The opponents of the proposed class have not presented a persuasive case that someone who has switched carriers should be denied access to copies of copyrighted works that she had purchased prior to switching carriers.

However, to the extent that CTIA is attempting to address concerns about bulk reselling of new subsidized phones, the Register supports language in an exemption that would exclude such activity from its ambit. As is discussed below, bulk resellers would not be able to take advantage of the new class of works because it would be restricted to cover only *used* wireless telephone handsets. This limiting language is explained in more detail below. Based on the preceding, the Register declines to adopt CTIA's alternative language.

To further allay the concerns expressed by CTIA, and to address its comments about the characterization of the 2006 exemption by MetroPCS in its litigation with Virgin Mobile, some clarification is in order. Here, the Register notes that the 2006 class, and the new one recommended herein, are both narrow, apply only to claims under Section 1201(a)(1), and do not establish a general federal policy of ensuring that customers have the freedom to switch wireless communications service providers. The designation of the classes, both new and old, simply reflect a conclusion that unlocking a mobile phone to be used on another wireless network does not *per se* constitute copyright infringement and that Section 1201(a)(1), a statute intended to protect copyright interests, should not be used to prevent mobile phone owners from engaging in such non-infringing activity.

On the other hand, the Register does not accept the proposition that the exemption should be available only when it is used for "noncommercial purposes." A person or entity that engages in the commercial activity of purchasing or obtaining by donations used mobile phones from actual users of those phones and "recycling" them for reuse by other persons should not be

precluded from taking advantage of the designation of this class of works merely because there is a "commercial purpose." As long as the other requirements of the class are met (*i.e.*, as discussed below, as long as the handset is used, the person engaging in the circumvention is the owner of the handset because she has purchased or otherwise acquired it from the original owner, and the circumvention is performed solely to connect to a wireless telephone communication network), there is no reason why such activity should be excluded from the scope of the class.[523]

However, one significant limitation on the activities of such "recyclers" should be noted. As discussed above, in order to permit the use of certain handsets on another network, it is necessary (in some cases) to modify the firmware to the extent that what is created may amount to a derivative work. Such activity would violate the copyright owner's exclusive right "to prepare derivative works based upon the copyrighted work."[524] As discussed above, the making of a derivative work is privileged in certain circumstances under Section 117's privilege for making "adaptations" of computer programs. However, that privilege includes a significant limitation: such adaptations may be transferred only with the authorization of the copyright owner.[525]

Thus, a recycler who prepares such an adaptation may not transfer ownership of the copy of the adapted computer program to anybody else without the authorization of the copyright owner. As a practical matter, that means that the recycler cannot transfer ownership of the handset, which contains the copy of the adapted computer program, to anybody else without the copyright owner's authorization. Such a transfer would be an act of infringement, disqualifying the recycler from taking advantage of the designation of this class of works.[526] Therefore, the designation of this class offers no benefit to recyclers who make and distribute adaptations of the computer program itself if those adaptations implicate the derivative work right.

---

[523] In addition, as in the past, the regulation designating the classes of works includes the general qualification that the prohibition against circumvention "shall not apply to persons who engage in *noninfringing* uses of the following … classes of copyrighted works." As discussed below, some "recyclers" may be excluded from the scope of the class if they modify the firmware in such a fashion that they are creating derivative works and then transfer it to anyone else without the permission of the copyright owner.

[524] 17 U.S.C. § 106(2).

[525] 17 U.S.C. § 117(b).

[526] The recycler would be disqualified because the proposed regulation, like the existing regulation, provides that "the prohibition against circumvention of technological measures that effectively control access to copyrighted works set forth in 17 U.S.C. 1201(a)(1)(A) shall not apply to persons who engage in noninfringing uses of the following six classes of copyrighted works." 37 C.F.R. § 201.40(b). Thus, a person who engages in an infringing use – such as the transfer of a copy of an adaptation of a computer program without the authorization of the copyright owner – of a computer program within the class of works would not be sheltered from liability for circumvention under § 1201(a)(1)(A).

ii. Proponents' proposed exemptions and the new class of works

In their initial comments filed with the Office, the proponents proposed the following class of works

MetroPCS (5B):

> *Computer programs that operate wireless telecommunications handsets when circumvention is accomplished for the sole purpose of enabling wireless telephones to connect to a wireless telephone communication network.*

Pocket (5C):

> *"Mobile Network Connection Programs." Computer programs in the form of firmware or software that enable' mobile communication handsets to connect to a wireless communication network, when circumvention is accomplished for the sole purpose of lawfully connecting to a wireless communication network.*

The Wireless Alliance (5D):

> *Computer programs in the form of firmware that enable wireless telephone handsets to connect to a wireless telephone communication network, when circumvention is accomplished for the sole purpose of lawfully connecting to a wireless telephone communication network, regardless of commercial motive.*

Upon a review of the initial exemptions proposed by the proponents, Pocket realized that the proposed classes of works regarding mobile phone unlocking were similar in many respects. Pocket conferred with the parties who had proposed exemptions 5B and 5D in an effort to harmonize these classes. Based on a common agreement and understanding, Pocket and the other Class 5 parties then submitted the following proposed class of works (the "Proposed Harmonized Class") for approval by the Register and Librarian:

> *Computer programs that enable wireless communications devices to connect to wireless communications networks when circumvention is accomplished for the purpose of enabling such devices to lawfully connect to wireless communications networks.*

This, they stated, is different from the existing exemption as illustrated by the following redline comparing the new proposed exemption with the 2006 exemption:

> Computer programs ~~in the form of firmware~~ that enable wireless communications devices ~~telephone handsets~~ to connect to ~~a~~ wireless

~~telephone~~ communication<u>s</u> network<u>s</u>, when circumvention is accomplished for the ~~sole~~ purpose of <u>enabling such devices</u> to lawfully connect to a wireless ~~telephone~~ communications network<u>s</u>.

According to Pocket, the Proposed Harmonized Class does not fundamentally change the scope of the 2006 exemption. It added that most of the differences between this Proposed Harmonized Class and its initial Class 5C proposal were intended to eliminate ambiguity and reduce the possibility of unintended consequences.[527] Pocket, however, remained cautious about some of the differences, and stated its belief that it is imperative that the resulting Proposed Harmonized Class be given the proper interpretation. It stated the following in support of the proposed exemption's new phraseology.

The phrase "in the form of firmware or software." Pocket commented on the deletion of this phrase as reflected in the Proposed Harmonized Class. It stated that while a device's "computer programs" are essentially the same as its "firmware or software," one or the other of these phrases should be deleted from the Class in order to eliminate repetition and promote clarity of scope. Pocket stated that it is worth repeating that the words "or software" had been proposed previously in light of the recognition that removal of a device lock does not always require access to what is generally understood as the firmware of a device.[528]

The phrase "wireless communication devices." According to Pocket, it had recommended that the term "wireless communication" be used in the Proposed Harmonized Class because it is common nomenclature in the wireless device marketplace. With regard to the term "devices," rather than telephone handsets, it stated that the clarification is intended to ensure that consumers can still seek out unlocking solutions despite the fact that their particular hardware may not technically qualify as a handset. It also stated that the majority of wireless devices would likely qualify as handsets in the strictest sense, but this understanding has been rapidly changing with

---

[527] R44 (Pocket) at 2-3. MetroPCS, who has joined with Pocket in advocating the revised language, stated that the "Proposed Harmonized Class" is intended to: (1) take into consideration some of the changes proposed by the other proponents; (2) clarify the language of the proposed exemption based upon the experience of MetroPCS in the wireless industry; (3) reduce ambiguity surrounding the Class; and (4) reduce the possibility of unintended consequences that may arise. R31 (MetroPCS) at 6-7. Cricket submits that the proposed language provides added clarity while continuing to capture the core elements of the exemption adopted by the Copyright Office in 2006. R36 (Cricket) at 12.

[528] R44 (Pocket) at 2, 6. (noting that "Handset locking measures are included not just by a handset's manufacturer [hence, in what is classically considered the firmware], but also in programs utilizing more volatile memory such as software added in the handset flash memory. The broader, more accurate wording is intended to capture all types of programming in the class of literary works where locks are included to control access to the programs that operate the handset.")

the evolving nature of wireless technology in recent years. It commented that several basic electronic devices, such as pagers, are now incorporating modules that exchange data through a wireless network. It further commented that laptop computers remain at the forefront of this trend, with a number of carriers now providing continuous data links via wireless broadband cards that are locked to a given carrier. Pocket concluded that because the wireless communications industry is quickly changing to address unmet needs, the recharacterization of "mobile communication handsets," in its initial exemption request, to "wireless communication devices," in the Proposed Harmonized Class, would allow the exemption to evolve as the industry continues to innovate.[529]

The word "sole." Pocket stated that the word "sole" in the 2006 Exemption has been a source of unintended consequences, as district courts have occasionally held that mobile phone unlocking would not be exempt if a financial motive was present in the pursuit of connecting a device to an alternative wireless network. It explained that unlocking will involve some financial incentive in addition to the motive of connecting to another network. It argued that it was never intended that the word "sole" be interpreted to defeat the 2006 Exemption just because financial motives exist in addition to other lawful motives. Pocket asserted that deletion of the word "sole" addresses this concern.[530]

The word "lawfully." Pocket has sought clarification of the term "lawfully" as it is used in the Proposed Harmonized Class. Specifically, it sought a determination from the Register and the Librarian that "lawful" purposes encompass all activities that either do not infringe or are fair uses of the copyrights in the device's programming.[531]

NTIA's Comments. The Assistant Secretary of Commerce for Communications and Information has advised the Register that NTIA believes the Librarian should extend the current exemption for the next three year cycle. In support, NTIA noted that consumers have filed

---

[529] *Id.* at 7. Joint Creators neither opposed nor supported renewal of the existing class. However, they opposed efforts to expand the existing class. They stated, for example, that any class should continue to explicitly state that it is only applicable to "wireless *telephone* handsets" and "wireless *telephone* communication networks" rather than the broader terminology proposed. R46 (Joint Creators) at 41.

[530] R44 (Pocket) at 8.

[531] *Id.* In response to the parties' original proposed classes, Joint Creators argued that the proponents did not adequately justify the removal of the term "lawful." They commented that the legislative history of Section 1201(a)(1)(B) makes clear that "the focus must remain" on only granting exemptions for "*lawful uses*" of copyrighted works. R46 (Joint Creators) at 40. The Register finds that this matter is now moot as the parties have now re-inserted the term in their revised language.

comments requesting that the current exemption be renewed.[532] It then noted, in agreement with the Register's 2006 recommendation, that "the software locks are access controls that adversely affect consumers to make non-infringing use of the software on their cell phones."[533]

NTIA did not support any of the proposed changes to the existing exemption. It stated that it was persuaded by opponents' argument that the narrowly tailored language recommended by the Register in 2006 prevents unlawful practices by those that would misuse the exemption for commercial purposes.[534] NTIA also asserted that the underlying purpose of the current exemption is to permit consumers adversely affected by the access control to unlock their phone and switch networks.[535] It then noted that its endorsement of extending the current exemption should not be construed as support for commercial application of this exemption. It stated that it only supports the opportunity for consumers to switch networks once contractual obligations are met with current wireless carriers or where the consumer has purchased the phone outright.[536] NTIA concluded by stating that to "the extent service providers resist unlocking phones for these consumers, the continuation of this exemption is encouraged."[537]

The Register's staff had further discussions with NTIA and inquired whether the Assistant Secretary would support an exemption permitting businesses and other entities that engage in recycling and resale to legally circumvent TPMs so that mobile phones may be used on different

---

[532] NTIA Letter of November 4, 2009, at 9, citing comments of Jonathan Flerchinger, at 1.

[533] *Id*., citing 2006 Recommendation of the Register of Copyrights at 76.

[534] *Id.*, citing comments of CTIA at 8. It also referenced current case law on this point. *Id*., citing *TracFone Wireless, Inc. v. Dixon*, 475 F. Supp. 2d 1236, 1238 (M.D. Fla. 2007) (holding that the "exemption does not absolve the Defendants of liability for their violations of the DMCA . . ." and that the narrowly tailored language of the exemption was intended for the "sole purpose of lawfully connecting to a wireless telephone communications network."). NTIA then stated that this reasoning was adopted by a subsequent court on a similar set of facts raised by the same plaintiff. NTIA letter of November 4, 2009, at 9, citing *TracFone Wireless, Inc. v. GSM Group, Inc.*, 555 F. Supp. 2d 1331 (S.D. Fla. 2008).

[535] NTIA noted that "adhering to this principle more closely aligns the process to the purpose for which DMCA was enacted. " NTIA Letter of November 4, 2009, at 9, citing comments of CTIA at 5-9.

[536] NTIA noted the wireless carriers' prediction that inexpensive subsidized phones would disappear if the exemption remained in place. NTIA stated that it is not persuaded that this will occur as it has not happened in the last three years with the current exemption in place. NTIA Letter of November 4, 2009, at 9.

[537] NTIA also noted that within one month of the establishment of the original exemption in 2006, several of the major carriers announced that they each would unlock their phones to be used on other networks. *See id.* at 9, citing *A Cellular Sea Change*, N.Y. TIMES, Dec. 1, 2007, at A14; Leslie Cauley, *AT&T Cellphone Network Wide Open*, USA TODAY, Dec. 5, 2007, at 7A; Carolyn Y. Johnson, *Big Wireless Carriers Get Set to Free the Phone*, BOSTON GLOBE, Mar. 28, 2008, at A1. But, it noted, popular smartphones that have been introduced since the 2006 exemption have remained locked. NTIA Letter of November 4, 2009, at 9-10, citing Cauley, at 7A. NTIA supports the exemption as long as it benefits consumers.

wireless networks. NTIA then followed up its earlier correspondence with an additional letter to the Register on this and other points related to the scope of the class of works for mobile phone unlocking.[538] NTIA recognized the broad desirability of making it easier for not-for-profit entities to provide used mobile phones to aid workers and the U.S. military and for certain green uses, such as recycling. NTIA then recommended that the Register provide a more detailed analysis emphasizing the intended scope of the class of works to include noninfringing uses of the exemption, but specifically exclude bulk resellers and other similar commercial uses. It stated that the use of the term "used," as distinct from "new" products in the proposed exemption would help clarify the Register's position and prevent abuses of the exemption by bulk resellers. NTIA also stated its concern about the inclusion of the phrase "by the owner of the copy of the computer program" in the language of the new class of works.[539] NTIA believed that consumers could misunderstand what rights the possessor of the used handset would have under the exemption. Therefore, NTIA recommended deleting this language from the text of the proposed class of works.[540]

Discussion. The Register recommends that the Librarian adopt a reformulation of the existing class of works, as embodied below. The Register makes this recommendation because a strict application of the statutory language of Section 1201 would result in a finding that one who circumvents the software lock on a mobile phone in order to connect to an alternative wireless network is engaging in unlawful circumvention of an access control. However, that Moreover, the act of circumvention is made in order to engage in conduct which cannot reasonably be understood to be an infringing activity. Finally, copyright interests, generally, do not appear to be adversely affected when such circumvention takes place.[541]

The Register recommends the following regulatory language to describe the class of works:

---

[538] Letter from Lawrence E. Strickling, Assistant Secretary for Communications and Information, United States Department of Commerce, to Marybeth Peter, Register of Copyrights, April 16, 2010 ("NTIA Follow-up Letter").

[539] For an explanation of that language, see the discussion *infra* at pp. 167, 169-170.

[540] *Id.*

[541] *See* 2006 Recommendation of the Register of Copyrights at 51.

> *Computer programs, in the form of firmware or software, that enable used wireless telephone handsets 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.*

The proposed new language would modify the original class approved by the Librarian in 2006 by introducing new terms that address concerns expressed by various parties and attempts to strike a careful balance. Approval of the new class will still permit circumvention of mobile phone locks in order to switch to another wireless carrier, but it should also curtail the commercial exploitation of the exemption by bulk resellers of new cellphones.

This new language differs from the language of the 2006 class of works as follows

> Computer programs***,*** in the form of firmware ***or software,*** that enable ***used*** wireless telephone handsets to connect to a wireless telephone communication network, when circumvention is ***initiated by the owner of the copy of the computer program*** ~~accomplished for the~~ sole***ly in order to*** ~~purpose of lawfully~~ connect~~ing~~ to a wireless telephone communication network ***and access to the network is authorized by the operator of the network.***

The Register has considered the specific modifications proposed by the participants in this proceeding and has reached the following conclusions. First, the Register does not believe that the formulation "Computer programs, in the form of firmware or software," is unduly repetitious or unclear. "Computer programs" are generally understood to be a subset of the class of literary works protected under Section 102 of the Copyright Act, and therefore "computer programs" is an appropriate starting point in defining the class of works. The existing class is confined to computer programs in the form of firmware; however, the proponents expressed concern that in some instances the pertinent computer programs may not be stored in what is "part of the classic firmware of a Device" and that a "trend to store locks in software that is not part of the firmware is expected to continue."[542] While the solution offered by the proponents was to remove the reference to firmware, the same result can be accomplished – and arguably with more clarity – by simply adding the words "or software" to make clear that the computer program may be in the form of firmware or software.

---

[542] R 44 (Pocket) at 6-7. *See also* C5C (Pocket) at 1; R31 (MetroPCS) at 7.

Second, the Register recognizes that the term "wireless communications devices" may be a more current descriptor of the hardware subject to the exemption than the term "telephone handsets" that has been part of the 2006 exemption. It does reflect the advances in technology over the course of the last three years and is comparable to language used in industry conversations[543] and at the Federal Communications Commission.[544] However, the proponents have not made an adequate evidentiary showing as to why the sweeping change is necessary at this point in time.

In any event, the objective of the exemption, from the Register's standpoint, is to permit a consumer to use a phone on a network other than the network of the wireless carrier that originally sold the phone. The principal function of the phone that is of concern here is "voice" communication and the exemption should facilitate this use.[545] A case has not been made that other devices, such as laptops or beepers, should be brought into the scope of the exemption because it has not been demonstrated that they are used primarily for this purpose.[546] Nor has it been shown that similar access controls have been placed on such devices. However, the exemption would apply to smartphones, such as Apple's iPhone and RIM's Blackberry, because they provide access to "voice" service, even though they also offer a penumbra of other useful functions (*i.e.*, mobile broadband data service, downloadable applications, and e-mail). As such, the language of the exemption should refer only to "telephone handsets" as the term has been stated and understood in this context. Nevertheless, the phrase "wireless telephone communications network" has been shortened to "wireless telecommunications network" in recognition of the fact that virtually all current wireless *networks* handle more than just voice service, and to avoid any implication that a network that offers more than telephone communications is beyond the scope of the class. While this change was not explicitly proposed by any party, it makes sense for the current exemption to reflect the modern telecommunications landscape.

---

[543] *See, e.g.*, http://www.fcc.gov/pshs/docs/advisory/jac/pdf/pcia-jac.pdf (Last visited 5/5/10.) (Comments of PCIA/The Wireless Infrastructure Association at 2, filed with the FCC).

[544] *See, e.g.*, https://esupport.fcc.gov/form1088/consumer.do (Last visited 5/6/10.) (The FCC uses the term "wireless communications devices" in its Form 1088 which concerns "Junk Faxes and Telemarketing.").

[545] The wireless telecommunications industry generates revenue from two principal services: phone calls ($116 billion) and text messaging (roughly $12 billion). *See* Scott Woolley, *Big Talk*, FORBES, November 16, 2009, at 96.

[546] On this point, the Register agrees with CTIA when it stated that "Pocket never bothers even to assert that beepers and text devices contain firmware or software that directs them to a particular wireless carrier, or that the prohibition on circumventing such locks has harmed or will harm anyone." *See* R43 (CTIA) at 19.

Third, the Register cannot approve of the removal of the language "sole purpose" in the new class of works. The use of that language in the 2006 exemption was purposefully intended to ensure that it would not extend to cases where the circumvention is accomplished not only in order to permit the handset to be used on another network, but also in order to remove restrictions on other copyrighted content stored on the handset, that is, to permit redistribution of copies of such content. Such a "dual purpose"circumvention would not be within the scope of the designated class. However, the "sole purpose" language was not intended to address whether the person engaging in circumvention might be acting in a commercial capacity. The discussion in the Register's 2006 recommendation was silent with respect to commercial motivation.

To clarify the intended scope of the class, the Register recommends that the "sole purpose" language be altered and that the appropriate limitation be that the circumvention was "*solely in order to* connect to such a wireless telecommunications network." This properly shifts the emphasis to the objective of the activity rather than whether the person engaging in the activity is doing so with an expectation of profit. While it would have the result, in some cases, of permitting circumvention of access controls by companies that purchase used handsets from consumers in order to make those handsets usable on other networks, the requirement (discussed below) that the handsets must be "used" would prevent the abuses singled out by the opponents of the proposed class as their principal grounds for objection: the bulk purchase of unused handsets that are offered for sale at low prices and the resale of those handsets after removing the technological restrictions that limit the use of the handsets to a single network.[547]

[547] As the NTIA stated, the proposed exemptions "raise interesting issues at the intersection of competition, communications, and copyright law." It noted that the FCC and others are "currently reviewing the issues related to competition and communications law and policy that may be linked" to exemption requests. NTIA Letter of November 4, 2009, at 9. Here are some open proceedings at the FCC examining handset availability and other developments in the wireless industry: *Petition for Rulemaking Regarding Exclusivity Arrangements Between Commercial Wireless Carriers and Handset Manufacturers*, RM-11497, FCC (rel. Oct. 23, 2008); *Fostering Innovation and Investment in the Wireless Communications Market*, GN Docket No. 09-157, and *A National Broadband Plan For Our Future*, GN Docket No. 09-51, Notice of Inquiry, FCC 09-66 (rel. Aug. 27, 2009). Congress has held hearing on the subject as well. *See also, The Consumer Wireless Experience*, hearing before the U.S. Senate Committee on Commerce, Science, and Transportation, June 17, 2009; *An Examination of Competition in the Wireless Industry*, hearing before the House Subcommittee on Communications, Technology, and the Internet, May 7, 2009. There has even been legislation introduced that would prohibit the unlocking of pre-paid wireless devices. *See The Wireless Prepaid Access Device Enforcement Act of 2009*, H.R. 2449, introduced on May 14, 2009 ("To amend title 18, United States Code, to prohibit fraud and related activity in connection with purchases of certain wireless prepaid access devices.")

The term "lawfully" is not part of the new exemption. The original rationale for including this term was to ensure that individuals or firms could not use the exemption to illegally connect to a wireless network, that is, to connect to a network without the permission of the operator of that network. However, as Pocket pointed out, the use of the word in this context is ambiguous.[548] In order to more accurately state the purpose that was originally behind the use of that word, and which remains valid in this proceeding, the Register proposes that the description of the class include the following qualification: "*and access to the network is authorized by the operator of the network.*" This language clarifies the scope of the restriction. On the other hand, the mere fact that the person who takes advantage of the exemption to connect to a new network may still be contractually obligated to continue to use her original network would not be the kind of "unlawful" connection that is outside the scope of the exemption. The original carrier's remedy for such activity would be an action for breach of contract.[549]

The Register has added the phrase "the owner of the copy of such a computer program" to emphasize that the exemption is intended to benefit the owner of the mobile phone and the firmware embedded in it. As discussed above, the state of the law with respect to who may be an "owner" of a copy of a computer program under Section 117 appears to be in flux, and the determination whether the owner of a handset is also the owner of the copies of computer programs contained in that handset may depend on an evaluation of a number of circumstances. However, because the basis for finding that the prohibition on circumvention has adversely affected the ability of users to engage in noninfringing uses was the conclusion that those uses are privileged under Section 117, and because the Section 117 privilege may be exercised only by the owner of the copy of the computer program, the users who may benefit from the designation of this class must necessarily be confined to "the owner of the copy of such a computer program." The Register understands the NTIA's position on the issue of ownership, but the state of the law and the variety of contractual or licensing arrangements in the marketplace make it impossible to include any bright line rules within the language of the regulation. The most that can be said at this point is that if the owner of the handset also happens to be the owner of the copy of the computer program that is contained in the handset, then the designated class applies to her (assuming all the other requirements in the description of the class have been satisfied).

---

[548] R44 (Pocket) at 8.

[549] *See* H.R. Rep. No. 94-1476 at 79. (discussing the first sale doctrine) ("This does not mean that conditions on future dispositions of copies or phonorecords, imposed by a contract between their buyer and seller, would be unenforceable between the parties as a breach of contract, but it does mean that they could not be enforced by an action for infringement of copyright.") However, as discussed above, contractual restrictions may determine whether the owner of the handset is in fact the "owner of the copy of such a computer program."

The Register finds that it is necessary to address one grievance the wireless industry has put forth in the record. Over the course of this proceeding, and through the comments filed by CTIA and Virgin Mobile, it has become evident that one of their main concerns about the proposed exemption requests centers on bulk resellers that would be able to purchase low cost mobile phones, legally unlock them without activating them on a wireless network, and then sell the devices for a profit in other countries. This concern shines through in the comments of the opponents of the proposed class.

CTIA specifically argued that including the proposed class in the new triennial regulations will foster bulk unlocking and unauthorized reselling of mobile phones. It remarked that there appears to be general agreement in the industry that the bulk purchase and subsequent circumvention of new phones for resale purposes is "wrong and destructive."[550] It argued that "the result is no less than the theft of the phone subsidy by a profit-seeking free-rider."[551] It concluded that such "theft" destroys the ability of a service provider to subsidize its phones, resulting in higher costs and less choice for consumers. Virgin Mobile was in agreement with CTIA and argued against any exemption that would permit anyone to "free ride" on the subsidized phones it provides to the public and unfairly profit from its low cost mobile phone offerings.

EFF stated that it understands the wireless industry's concerns about bulk purchasers and legitimizing certain outfits that would facilitate unlocking for dubious reasons. But, it added, the industry's concern is related more to abrogation of contracts, trademark infringement, and unfair competition, and not so much with copyright protection.[552]

In addition, EFF argued that Virgin Mobile's business model of selling highly subsidized inexpensive mobile phones is the direct cause of the problems it has encountered with third parties reflashing and selling their phones in overseas markets for a profit. It argues that Virgin Mobile and other wireless carriers faced this situation before 2006 and, therefore, the existing mobile phone exemption cannot be blamed for the situation. It commented that instead of opposing the new requests, Virgin Mobile should instead invest in higher quality TPMs that make it more difficult and expensive for bulk purchasers to do business.[553]

---

[550] R43 (CTIA) at 39.

[551] *Id.*

[552] T Granick, 5/1/09, at 149-150.

[553] *Id.* at 168.

Based on the record evidence, the Register finds that bulk reselling of new mobile phones by commercial ventures is a serious matter. There is no justification for the result of this rulemaking proceeding to condone, either expressly or implicitly, the illegal trafficking of mobile phones. Such illicit practices raise the cost of doing business, which in turn affects the marketplace for mobile phones and the prices consumers pay for such devices. The Register finds that the exemption should be limited to include only "used" mobile phones. The term "used," as applied in this context, refers to a mobile phone that has been activated with the carrier or provider that sold the phone at a subsidized price and that the person activating the phone must actually have used on that carrier's network. This additional language would likely promote continued usage of the phone on that network because a consumer would be unlikely to switch wireless networks immediately after activating the phone.[554] This new language would also prevent bulk resellers from taking advantage of the exemption after purchasing new mobile devices *en masse* at retail establishments and immediately unlocking them to be sold outside the United States.

f. Limitations on the new class of works

It must be pointed out that the new exemption is limited by existing law in two important respects. First, the exemption is cabined by Section 1201(a)(2) which strictly prohibits an entity from offering a circumvention service. Second, a wireless carrier's "Terms of Purchase" and "Terms of Service", which are binding contracts, still impose use restrictions on consumers even with an exemption in place. These legal constructs are explained in more detail below.

i. Section 1201(a)(2)

Joint Creators and Copyright Owners asserted that what the proponents are implicitly seeking is to have an exemption that covers the sale of circumvention devices by third party resellers, or the provision of circumvention services to others, both of which are prohibited by

---

[554] Virgin Mobile expressed an openness to such an approach. *See* T Lurie, 5/1/09, at 186-187 ("What you could do, you could allow the exemption -- and we would submit something in writing later. But for legitimate customers who previously used the service for which the device was intended, could themselves reflash the phone.") Ultimately, however, Virgin Mobile continued to assert that no exemption is warranted and made clear that it would continue to object to any exemption that did not include restrictions at least as stringent as those that were suggested by CTIA. *See* Post-Hearing Response of Virgin Mobile to Copyright Office Questions relating to Cellphones of July 13, at 16-17.

Section 1201(a)(2).[555] They argued that Congress has already clarified when Section 1201(a)(2) is inapplicable, and the Register cannot recommend additions to that list. CTIA asserted that Congress limited the scope of the rulemaking to the Section 1201(a)(1) prohibition on individuals engaging in the act of circumvention. It argued the rulemaking expressly does not apply to those who provide circumvention services or technology.[556]

In response, Cricket maintained that an exemption under Section 1201(a)(1) is independent of 1201(a)(2) and suggested that granting the exemption for mobile phone unlocking will not affect a wireless carrier's ability to use Section 1201(a)(2) in a private cause of action against the illegal trafficking of mobile phones.[557]

The Register does not agree that the proponents' proposed classes of works are aimed solely or even principally at bringing circumvention services under the umbrella of a Section 1201(a)(1) exemption. In fact, the main business of certain supporters of the exemption, such as Pocket, is to sell new phones to new wireless subscribers, not to unlock and resell old mobile phones. MetroPCS also concentrates on selling new handsets and services to new customers, and only offers to reflash phones under certain conditions.[558] The recyclers who are part of the Wireless Alliance do not sell new phones; rather, they obtain old handsets from a variety of sources, repurpose them, and redistribute them to others.[559]

Nothing in this rulemaking can or is intended to insulate such activities from liability under Section 1201(a)(2) to the extent that they fall within its scope. If any of the proponents of

---

[555] R46 (Joint Creators) at 41. *See* 17 U.S.C. § 1201(a)(2)(A) ("No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or parts thereof, that [ ] is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title….").

[556] R43 (CTIA) at 39-40.

[557] T Inglish, 5/8/09, at 194-95.

[558] In litigation against Virgin Mobile, MetroPCS asserted that it reflashes handsets only at a handset owner's request and only when a customer establishes wireless service with MetroPCS and agrees to various terms. For example, customers requesting the reflashing service must affirm that they (1) do not have a contract with any other wireless service provider, (2) are not participating in a scheme to acquire bulk quantities of subsidized handsets to resell at higher prices, and (3) will not use the original provider's trademarks in selling, offering for sale, distributing, or advertising their handsets. *MetroPCS Wireless, Inc. v. Virgin Mobile USA L.P.*, C.A. No. 3:08-CV-1658-D, (N.D. Tex. Sept. 25, 2009), at 4-5, n. 4.

[559] The Register agrees with the Wireless Alliance that its members' activities, "the recycling and resale of used handsets, differs markedly from the business of the bulk purchasers and resellers of new phones that Tracfone has sued" under Section 1201(a)(2). *See* C5D (Wireless Alliance) at 11.

the proposed class are offering the service of unlocking software locks, they most likely are in violation of Section 1201(a)(2).[560] To the extent that they are acquiring used handsets, unlocking them and then reselling them, it seems unlikely that such activity falls within the scope of Section 1201(a)(2), but that is not a matter to be resolved in this rulemaking

ii. Contracts

As discussed above,[561] wireless service providers often sell their mobile phones with contractual provisions prohibiting the use of the devices on other wireless networks. CTIA asserted that circumvention often violates those contracts.

Virgin Mobile added that courts have already found its contractual terms to be enforceable. It commented that it conspicuously notifies customers in all-capital letters on the handset packaging that the purchase and use of Virgin Mobile-branded wireless handsets are subject to certain restrictions, including that (1) the customer may not alter any hardware or software in the handset and (2) the customer may use the handset only on the Virgin Mobile service. It further commented that the first page of the "Terms of Service" booklet provided inside the packaging reiterates the prohibition against reflashing; moreover, those customers who purchase and/or activate their handsets on Virgin Mobile's website must affirmatively click a box acknowledging that they agree to be bound by the "Terms of Service." It asserted that consumers have at least two, and in some cases three, opportunities to either not purchase or to return the phones if they object to the "Terms of Purchase" or "Terms of Service." Virgin Mobile thus concluded these "terms" are enforceable agreements.[562]

MetroPCS asserted that it is inappropriate for carriers to insert into their agreements that handsets may not be used on third party networks, or similarly limit the use of the software to provision the use of services on the carrier's network. It argued that such a limitation would be similar to a car manufacturer inserting a provision in the sales contract that a car may only be serviced at a dealer's service locations. It further argued that this would be an inappropriate restraint of trade and the Register should consider whether to pre-empt state law to the extent

---

[560] *See* 17 U.S.C. § 1201(a)(1)(E); *see also*, http://www.metropcs.com/metroflash (Last visited 5/6/10.) (describing the steps necessary to get a mobile phone reflashed at a MetroPCS store). The Register takes no position as to whether MetroPCS is actually violating Section 1201(a)(2); the observation is merely offered to illustrate that while Section 1201(a)(2) may be implicated in some of the activities identified by the Joint Creators, it does not appear to be implicated in all such activities.

[561] *See*, *supra*, for a discussion of Virgin Mobile's Terms of Service and Terms of Purchase.

[562] *Id*. at 11.

carriers try to use contract provisions to eliminate the rights being sought here. Otherwise, it concluded, wireless carriers could attempt to make any relief granted here a hollow right easily defeated.[563]

On the other hand, EFF stated that even if the exemption were granted, the contractual relationship between the wireless carrier and its customers would remain.[564] It further stated that consumers who abrogate existing agreements would still be subject to contractual conditions and remedies, such as the requirement to pay early termination fees. In short, it is only asking that an exemption from the Section 1201 anticircumvention requirement be granted so that a customer would be permitted to unlock a mobile phone to use it on another network without being subject to the remedies provided for violation of Section 1201(a)(1).[565]

Contracts, and the conditions that they may impose on mobile phone consumers, play an important role in this context. It is commonly understood that "Terms of Purchase" and "Terms of Service" are types of contracts, the conditions of which vary from carrier to carrier. These agreements are recognized as valid under state law and may contractually bind users to usage of the wireless phone on a particular network or place other limitations on the use of the handset. However, the Register is in no position to, and has no authority to, judge the merits of the dozens of "Terms of Purchase" or "Terms of Service" in the marketplace today, especially in a rulemaking proceeding such as this.

That being said, courts have recognized that contractual obligations stand apart from the copyright law.[566] The rights and obligations established by contract are different from the

---

[563] C5B (MetroPCS) at n. 21.

[564] When queried on the contracts issue at the hearing, EFF questioned the enforceability of Virgin Mobile's "Terms of Service" and "Terms of Purchase", but did not clearly articulate the reasoning behind its suppositions or provide support for its position. T Granick, 5/1/09, at 214-15.

[565] *Id.* at 179-80.

[566] To demonstrate that contract rights are preempted by the Copyright Act, a party must show that the state law claim (1) "falls within the subject matter of copyright," as defined by 17 U.S.C. § 102, and (2) "protects rights that are equivalent to any of the exclusive rights of a federal copyright, as provided in 17 U.S.C. § 106." *Carson v. Dynegy, Inc.*, 344 F.3d 446, 456 (5th Cir. 2003). The test for evaluating the equivalency of rights is commonly referred to as the "extra element" test. *Id.*, citing *Alcatel USA*, 166 F.3d at 787. This test requires that if one or more qualitatively different elements are required to constitute the state-created cause of action being asserted, then the right granted under state law does not lie within the general scope of copyright, and there is no preemption. *See MetroPCS Wireless, Inc. v. Virgin Mobile USA L.P.*, C.A. No. 3:08-CV-1658-D, (N.D. Tex. Sept. 25, 2009) at 45.

exclusive rights granted by copyright.[567] Breach of contract claims still may be brought by Virgin Mobile and other carriers in the courts. This rulemaking proceeding, and the designation of this class of works, apply only to the Section 1201(a)(1) prohibition on circumvention of access controls and have no effect whatsoever on the validity or viability of such breach of contract claims.

g. Conclusion

Based on the foregoing, the Register recommends that the Librarian of Congress consider and approve the following class of works for an exemption to the prohibition on circumvention found in Section 1201(a)(1) of the Copyright Act:

> *Computer programs, in the form of firmware or software, that enable used wireless telephone handsets 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.*

The proposed class recommended by the Register goes somewhat beyond the class recommended by NTIA. As noted above, NTIA recommended that the class designated three years ago remain in place, but it did not support any of the proposed expansions of the current class. NTIA also remarked that "the triennial DMCA exemption rulemaking is an inappropriate forum to debate the larger policy issues," such as competition and communications policy issues currently under review by the Federal Communications Commission and other agencies.[568] The Register agrees with that observation, and her recommendation is based only on application of copyright law and policy to the facts presented in the proceeding.

---

[567] *See ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447, 1454 (7th Cir. 1996) (Rights "equivalent to any of the exclusive rights within the general scope of copyright" are rights established by law--rights that restrict the options of persons who are strangers to the [copyright holder]. Copyright law forbids duplication, public performance, and so on, unless the person wishing to copy or perform the work gets permission; silence means a ban on copying. A copyright is a right against the world. Contracts by contrast, generally affect only their parties; strangers may do as they please, so contracts do not create "exclusive rights."); *see also Taquino v. Teledyne Monarch Rubber*, 893 F.2d 1488, 1501 (5th Cir. 1990) ("A right is equivalent if the mere act of reproduction, distribution, or display infringes it. This action for breach of contract involves an element in addition to mere reproduction, distribution or display: the contract promise made by Taquino, therefore, it is not preempted." (citations omitted)). *See MetroPCS Wireless, Inc.* at 45-46.

[568] NTIA Letter November 4, 2009, at 8.

Specifically, NTIA cautioned that its "endorsement of continuing this exemption should not be construed as support for commercial application of this exemption," and stated that it was "persuaded by opponents' argument that the narrowly tailored language used in 2006 prevents unlawful use by those that would misuse the exemption for commercial purposes."[569] NTIA also proposed a dichotomy where non-profit entities could take advantage of the exemption while commercial users could not. The Register's recommendation, in contrast, would permit some commercial activity, so long as it (1) involves only used handsets, (2) is done by the owner of the copy of the computer program, and (3) is done "solely in order to access such a wireless telecommunications network and access to the network is authorized by the operator of the network." The Register believes that these limitations ensure that the designation of this class will not benefit those who engage in the type of commercial activity that is at the heart of the objections of opponents of the proposed exemption: the "bulk resellers" who purchase new mobile phone handsets at subsidized prices and, without actually using them on the networks of the carriers who market those handsets, resell them for profit.[570] The type of commercial activity that would be permitted would be the resale of used handsets after the owners of the handsets have used them and then given or sold them to somebody else, who then resells them just as a used bookstore sells used books. The Register acknowledges that NTIA's general view that the class should not extend to any commercial activity is inconsistent with aspects of the Register's recommendation, but believes that to the extent her recommendation goes beyond what NTIA was willing to endorse, it does so in a way that, in NTIA's words, "prevents *unlawful* use by those that would misuse the exemption for commercial purposes."[571]

D. Video games accessible on personal computers and protected by technological protection measures that control access to lawfully obtained works, when circumvention is accomplished solely for the purpose of good faith testing for, investigating, or correcting security flaws or vulnerabilities, if:

1. The information derived from the security testing is used primarily to promote the security of the owner or operator of a computer, computer system, or computer network; and

---

569 *Id.* at 9.

570 *See* R43 (CTIA) at 21-22, 39-40 (referring to "bulk commercial reflashers" who engage in "subsidy theft").

571 *See* NTIA Letter of November 4, 2009, at 9 (emphasis added).

2. The information derived from the security testing is used or maintained in a manner that does not facilitate copyright infringement or a violation of applicable law.

Background. Professor J. Alex Halderman proposed two classes of works relating to investigating and correcting security flaws or vulnerabilities created or exploited by technological measures protecting certain kinds of works.[572] The first proposed class includes three categories of works as its starting point: (1) literary works, (2) sound recordings; and (3) audiovisual works. The proponent then qualified the scope of the proposed class by restricting it to lawfully obtained works within those categories protected by access control measures that create or exploit security flaws or vulnerabilities that compromise the security of personal computers. The class is further refined by reference to particular uses—when circumvention is accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities.

The precursor for this proposal is a class that the Librarian designated in 2006:

> Sound recordings, and audiovisual works associated with those sound recordings, distributed in compact disc format and protected by technological protection measures that control access to lawfully purchased works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities.

The 2006 exemption was largely based on the facts arising out of the distribution, by Sony BMG Music Entertainment, of compact discs ("CDs") that employed certain digital rights management software that created security vulnerabilities on computers on which the software

---

[572] The two classes are:

> Literary works, sound recordings, and audiovisual works accessible on personal computers and protected by technological protection measures that control access to lawfully obtained works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities; and
>
> Video games accessible on personal computers and protected by technological protection measures that control access to lawfully obtained works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities. C8A (Halderman) at 3.

was installed. Specifically, SunnComm's MediaMax content protection software and First4Internet's XCP copy protection software program were alleged to create significant security vulnerabilities on personal computers. The proponents of the 2006 exemption, Edward W. Felten and J. Alex Halderman, proposed the class of "sound recordings and audiovisual works distributed in compact disc format and protected by technological measures that impede access to lawfully purchased works by creating or exploiting security vulnerabilities that compromise the security of personal computers."

The evidence in the record of the 2006 proceeding demonstrated that MediaMax and XCP controlled access to the sound recordings (as well as some related audiovisual works, such as music videos) on a number of CDs distributed in 2005 and, as a consequence, ended up being installed on perhaps half a million computer networks worldwide. The evidence also established that these access controls created security vulnerabilities on the personal computers on which they were installed. For example, XCP included a "rootkit" which cloaked the existence of other aspects of the XCP digital rights management software (a music player application and a device driver).[573] The rootkit created security vulnerabilities by providing a cloak that concealed malicious software, a cloak that, in fact, was exploited by disseminators of malware within days of the discovery of the XCP rootkit.

Copyright owners were opposed to the proposed exemption primarily on the ground that they believed that a statutory exemption already exists that permits circumvention of access controls for the purpose of "security testing" under Section 1201(j) ("accessing a computer, computer system, or computer network, solely for the purpose of good faith testing, investigating, or correcting, a security flaw or vulnerability, with the authorization of the owner or operator of such computer, computer system, or computer network.") After extensive review and analysis of the legislative history, the Register concluded that while it appears possible that the statutory exemption in Section 1201(j) may permit certain acts of circumvention in cases such as those involving MediaMax and XCP, it was not clear from either the statutory language or the legislative history whether that provision extends to the circumvention of an access control *on a copy of a copyrighted work* (as opposed to "accessing a computer, computer system or computer network"). In light of that uncertainty and the seriousness of the problem, the Register recommended that the Librarian designate a class of works consisting of sound recordings, and

[573] A rootkit is a kind of computer code that is able to command and control an operating system and is capable of hiding its presence from spyware blockers and similar system management utilities. *See*, *infra*, for a further discussion of rootkits.

audiovisual works associated with those sound recordings, distributed in compact disc format and protected by technological protection measures that control access to lawfully purchased works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities.

Class of works rejected–literary and/or audiovisual works. In the current proceeding, Professor Halderman did not introduce any evidence that the prohibition as applied to sound recordings, or audiovisual works associated with such sound recordings, is adversely affecting or is likely, in the next three years, to adversely affect the ability to engage in noninfringing uses. There is no information in the record that would justify again exempting the class designated three years ago. In this *de novo* review, the absence of a record in relation to sound recordings requires that the default rule established by Congress should apply and that no exemption should issue.

Similarly, there is nothing in the record of this proceeding that creates a record relating to a class based on literary and/or audiovisual works, except to the extent that video games constitute literary works or audiovisual works. There is some speculation in the record that other digital rights management measures "are likely" to implicate other types of copyrighted works (*e.g*., ebooks and streaming video), but the evidence to support this claim is either unverifiable, contradictory, or speculative.[574] Moreover, while it may be that digital rights management measures are increasingly used on new types of digital works, there is no evidence that such measures are likely to create security flaws or vulnerabilities.

While Professor Halderman may have offered compelling policy arguments in favor of an exemption that covers such works, those arguments are more properly addressed to Congress than to the Register and the Librarian. This rulemaking is restricted in its scope; it can address only particular classes of works with respect to which noninfringing uses are being adversely affected or, in the next three years, are likely to be adversely effected by the prohibition on circumvention. This inquiry is primarily fact-based, although of course legal analysis, to determine whether the

[574] C8 (Halderman) at 7-8, nn. 30 and 31. Footnote 30 contains speculation about the possibilities for DRM on e-books in the next five years, but there is no evidence that DRM on e-books causes, or is likely to cause, security flaws or vulnerabilities. The blog entry cited in footnote 31 tends to refute the claim that Adobe creates security flaws or vulnerabilities, and explains that Adobe simply encrypts streamed content in order to protect access and prevent reproduction of streaming content. Similarly, another article cited discusses Microsoft's Silverlight streaming technology, but does not reveal any evidence of security flaws or vulnerabilities caused by that technology.

affected use is noninfringing, also plays a key role. It focuses on the marketplace as it is at the time the rulemaking takes place, and not on broader policy concerns that are within the province of the legislature. While Professor Halderman's concerns relating to sound recordings and to literary and audiovisual works other than video games may be well-founded, he has not presented a record upon which the Librarian can act in this regulatory setting. Indeed, similar policy concerns presumably could be articulated with respect to any works of any kind that are distributed in digital formats and protected by technological measures.

Accordingly, the Register cannot recommend that the Librarian designate the first of the two classes proposed by Professor Halderman. However, Professor Halderman has presented a record relating to the second proposed class involving certain video games.

Class of works accepted–video games. For purposes of categorization under Section 102(a) of the Copyright Act, video games are "hybrid" in that they fall within two statutory classes of works.[575] Video games typically are, in part, computer programs,[576] which are a subset of the statutory category of "literary works." But other aspects of video games, and increasingly the predominant authorship, are comprised of audiovisual elements. Thus, while the categories of literary works and audiovisual works are implicated in a record relating to video games, those categories encompass an enormous range of works that are not addressed in the factual record. The only evidence introduced in relation to particular alleged problems relates to two types of access controls applied to video games.[577] Given the evidentiary record before the Register, the starting point in this analysis is limited to video games on personal computers protected by technological protection measures that control access to lawfully obtained works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers.

Professor Halderman conceded that focusing on such a class "should be adequate to mitigate the harms caused by TPMs [technological protection measures] that control access to PC-accessible video games because it will remove the chilling effect of the anti-circumvention measures, thereby encouraging independent researchers to investigate and correct security flaws

---

[575] 17 U.S.C. § 102(a).

[576] 17 U.S.C. § 101 (A "computer program" is a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result.)

[577] C8 (Halderman) at 5.

in these TPMs and allowing users to stay informed and take appropriate measures to protect themselves."[578]

The record relating to the adverse effects on security research and investigation of technological measures applied to video games is primarily limited to two distinct security measures: (1) Macrovision's SafeDisc software and (2) Sony's SecuRom software.[579] Professor Halderman asserted that the measures constitute access controls because, in both cases, the measures authenticate discs and enforce access policies.[580]

The alleged underlying noninfringing use involved is two-fold. First, purchasers of video games (including researchers) are engaged in noninfringing use when they install, access, and play authorized copies of such video games while further seeking to protect the security of their computers. Second, researchers in lawful possession of copies of games are engaged in noninfringing uses when they seek solely to research and investigate whether a video game, or the technological measure protecting it, creates security vulnerabilities or flaws. Professor Halderman asserted that such good faith research that does not cause or promote infringement generally fits squarely within the fair use factors.[581]

In support of his conclusion that such activities constitute fair use, Professor Halderman argued that the purposes of the intended use are research, scholarship and teaching, conduct expressly mentioned as illustrative fair uses in the preamble of Section 107.[582] He further stated that "the discovery and disclosure of security vulnerabilities is analogous to criticism and commentary, two other model fair uses listed in the preamble."[583] He asserted that the creative nature of the work is not particularly significant in the context of video games (*i.e.*, creative games expressed as computer programs), because they generally "contain unprotected aspects that cannot be examined without copying."[584] Although the entire work may be installed and

---

[578] *Id.* at 7.

[579] *Id.* at 5-6.

[580] *Id.* at 8.

[581] *Id.* at 12-13.

[582] *Id.* at 13.

[583] *Id.*

[584] *Id.* at 14, citing *Sony Computer Entm't, Inc. v. Connectix Corp.*, 203 F.3d 596, 603 (9th Cir. 2000); *Sega Enters. v. Accolade, Inc.*, 977 F.2d 1510, 1526 (9th Cir. 1992).

reproduced in the course of this research, he argued that the installation of a lawful copy is generally within the scope of the license.[585] Moreover, the use of the copyrighted work is incidental to the purpose of investigating the protection measure itself. To the extent the copyrighted work is used, it is either used minimally or not at all.[586] Professor Halderman also argued that security research is likely to increase market demand rather than adversely affect the market for or value of the works, because research will ameliorate consumer uncertainty. Moreover, he argued that to the extent that research harms the market for the work, it would only do so as successful criticism, which is not relevant market harm for purposes of copyright.[587] In conclusion, he found that all of the factors weigh in favor of fair use.[588]

Professor Halderman alleged that Sony's SecuROM may create security flaws or vulnerabilities. In support, he referred to a number of articles and class action lawsuits suggesting that SecuROM may contain flaws or cause vulnerabilities. He claimed that "anecdotal contentions of harm, speculations about causes, and contradictory assessments of risk have run wild on the Internet."[589] He further stated that a single definitive scientific study might quell the "panic, protests, and litigation" to "what may turn out to be nonexistent or easily reparable faults."[590]

Professor Halderman further alleged that harm is caused by Macrovision's SafeDisc, "one of the most widely used copy-protection systems for PC-accessible video games."[591] He alleged that SafeDisc was preinstalled on "nearly every copy of the Microsoft Windows XP and Windows 2003 operating systems, [and that] the vulnerability affected nearly one billion PCs, two thousand times more than the [Sony] rootkit."[592] He claimed that the security flaw created by SafeDisc was "much more dangerous" than the Sony rootkit flaw, because the flaw allowed attackers to

---

585 *Id.* at 14.

586 *Id.*

587 *Id.*

588 *Id.* at 15.

589 C8 (Halderman) at 6.

590 *Id.* at 7.

591 *Id.* at 5.

592 *Id.*

"execute unrestricted 'kernel-level' code and read or write to any area of the hard disk or memory of the PC, thus facilitating the complete compromise of the security of the PC."[593]

Opponents raised three principal arguments against Halderman's proposal. First, they argued that he provided little concrete or documented evidence that any security flaws or vulnerabilities associated with access control mechanisms used in connection with video games exist. Second, they argued that there is no evidence that research has been chilled. They alleged that Professor Halderman completely ignored "the development of a robust ecosystem within which security experts routinely identify such flaws, collaborate on remedies, and disseminate information to alert computer users of the problems and point them to solutions."[594] Third, they argued that Professor Halderman failed to establish that the conduct at issue is prohibited by Section 1201(a)(1), since a statutory exemption might apply to the security research.[595]

In support of their first point, opponents stated that the vulnerability identified in SafeDisc was resolved and a patch made available to consumers. They also noted that a remote user could not exploit this vulnerability, and that the driver included with Windows was inactive until invoked by a game. In response to the allegations relating to SecuROM, the opponents argued that the allegations of various bloggers, many of them anonymous, are completely unsubstantiated. Moreover, opponents argued that a closer examination of many of the class action complaints reveals that most address performance issues, licensing restrictions, disclosure questions, and activation limitations, all of which are unrelated to security threats.[596] The security concerns are "the spindly tail being wagged by a much more robust dog of unrelated consumer complaints."[597]

With respect to Professor Halderman's second argument, the opponents agreed that independent security research and testing should be encouraged to identify and correct any security flaws or vulnerabilities that access controls might contain. However, they asserted that this research is occurring and that the claims that the prohibition is chilling research are

---

[593] *Id.* at 5, n. 19.

[594] R46 (Joint Creators) at 47. The Joint Creators also argued that there was no showing in relation to the categories of literary, sound recording, and audiovisual works.

[595] *Id.* at 47 and 53-54.

[596] *Id.* at 49.

[597] *Id.*

ungrounded. They claimed that this alleged chilling effect is contradicted by the two examples cited by the Professor Halderman. In the case of SafeDisc, they stated that Symantec researchers identified the problem and that there have been no reports of legal threats as a result of this research. Similarly, they claimed that Symantec and other independent researchers have explored and debunked some of the security allegations surrounding SecuRom without any reports of legal threats.[598] Opponents further argued that research is encouraged by the industry and that the online resources and attribution given to researchers provides evidence of the "robust and collaborative ecosystem" that exists.[599]

In relation to the opponents' argument that Section 1201(j) may apply, the opponents state that the proponent of an exemption has the burden of proving that an existing statutory exemption does not apply. Notwithstanding the acknowledgment that the Register and the Librarian concluded in the last rulemaking that an exemption in this rulemaking process may be granted when "it is not clear whether [a statutory exemption] extends" to the conduct in question," the opponents contended that when a proponent fails to prove that the activity falls outside of the scope of the exemption, "the burden has not been met, and the proposal must be rejected."[600] In particular, the Joint Creators contend that Section 1201(j) "could apply."[601]

The Assistant Secretary of Commerce for Communications and Information has advised the Register that he believes that the record supports granting the requested exemption for video games and other works accessible on personal computers.[602] NTIA believed that the proponents have "persuasively argued that without a research exemption, research into all current and future vulnerabilities will be and is chilled now,"[603] and concurred with the Librarian's conclusion in 2006 that the research may not be covered completely by the existing statutory exemptions.[604]

---

598 *Id*. at 51.

599 *Id*. at 52.

600 *Id.* at 53.

601 *Id.*

602 NTIA Letter of November 4, 2009, at 11-12.

603 *Id.* at 11.

604 *Id.* at 12.

NTIA further believes that although the Sony Rootkit vulnerability no longer exists, "it seems to be a certainty that new vulnerabilities *will* emerge in the next three years."[605]

NTIA urged the Register to resist focusing solely on the limited protection measures identified by the proponents, because vulnerabilities are certain in the future in relation to other technological protection measures.[606] NTIA did not accept the opponents' attempts to narrow the exemption,[607] but rather believed that the exemption should permit research by academic, government, and private entities and individuals.

a. The nature of the underlying use of the copyrighted work by researchers

The only limitation to the copyright owner's exclusive rights that is clearly relevant to the reproductions of the copyrighted work in the course of investigation and research is fair use.[608] In order to determine whether a particular use of a copyrighted work is fair, the four mandatory statutory factors must be considered.[609]

Factor One

The purpose and character of the use of the video game is to investigate and identify, in good faith, whether security flaws and vulnerabilities in the technological measures protecting a video game exist. In order to do that, the researcher typically must purchase and install the video

---

[605] *Id.* (emphasis in original).

[606] *Id.* at 12.

[607] In response to post-hearing questions, opponents had asserted that if the Librarian were to designate a class to address security flaws and vulnerabilities, "the exemption should be limited to an identifiable category of credentialed qualified experts engaged in verifiable security research." Post-Hearing Response of Joint Creators to Copyright Questions relating to Security Flaws of July 10, 2009, at 2.

[608] Professor Halderman offered two legal theories as to how the conduct in which he wished to engage is noninfringing: fair use and Section 117. There could be an argument that Section 117 is relevant to the analysis, but it is unclear whether the technological protection measure or the video game may be classified as a "computer program" for purposes of this statutory provision, and the parties have not raised the issue. Moreover, the law is unsettled with respect to the circumstances under which one is the "owner" of a copy of a computer program entitled to invoke Section 117. *See*, *supra*. In any event, while Professor Halderman offered a legal analysis in support of his fair use claim, he did nothing more than refer to Section 117 without offering any explanation as to how it is applicable. Given his failure to offer any reasons why Section 117 is applicable and given the conclusions here concerning fair use, the Register finds no reason to assess the relevance of Section 117.

[609] 17 U.S.C. § 107.

game on the computer. It should be noted that the proposed class is applicable only to good faith testing, investigating, or correcting of security flaws or vulnerabilities and not to circumvent for other purposes. Moreover, not only does this activity involve research and, at least in some cases, teaching and scholarship, but like all of the activities listed in the preamble of Section 107, it involves a broader socially productive activity. The goal of the research is to yield rigorous and accurate criticism or comment about the technological measure attached to a work. This criticism or comment may reveal problems or dispel unfounded rumors. In either case, the purpose is socially productive and provides the public with an objective assessment of publicly distributed measures that control access to video games.

The character of the use is also typically noncommercial and the purpose of the use is transformative. Security researchers do not typically seek direct monetary reward for investigating mass-marketed security measures. Although researchers may receive indirect benefits from successful scholarship (*e.g.*, tenure and publicity), the same may be said for any scholarly research. Moreover, security research is transformative because it serves an entirely different purpose from the entertainment purpose of the copyrighted work and the measure protecting that work. Indeed, the particular work itself is essentially irrelevant to the use, except that the work must be reproduced in order to understand how the protection measure attached to the work operates. The goal of security research is analogous to reverse engineering for the purpose of achieving interoperability. Like reverse engineering, the intermediate copying of the work is a means to another end, that is, to understand the functioning of the security measure in order to assess potential vulnerabilities the measure creates on a personal computer. The product of the research does not generally contain any of the copyrighted work, but only locally reproduces the work as needed to investigate the operation of the measure in conjunction with the work and the computer's operating system. Any reproduction of the copyrighted work typically does not extend beyond the researcher's computer on which the researcher was already entitled to reproduce the entire work as a consequence of its being a lawful copy of the work. These noncommercial, socially productive, transformative uses performed solely for good faith testing, investigation, or correcting of security flaws or vulnerabilities weigh heavily in favor of fair use under the first factor.

Factor Two

Turning to the nature of the copyrighted works, video games are creative and thus would ordinarily be entitled to a broad scope of protection in a fair use analysis. However, video games

made for personal computers, as opposed to proprietary game systems, are necessarily also partly computer programs. These types of programs contain many functional elements necessary for interoperability with a personal computer operating system. The security research at issue here focuses on functionality, rendering the creative aspects of the video games irrelevant. Therefore, for purposes of a fair use analysis on the facts presented here, the video games actually should be considered functional works entitled to lesser consideration.[610] Moreover, the focus here is not even so much on the video games themselves as it is on the technological protection measures that control access to the video games, measure that are purely functional. Because these functional elements cannot be investigated or assessed without some intermediate reproduction of the creative work, whatever significance there might be in the creative nature of a video game in this context is diminished.[611] In addition, to the extent that the purpose of the use is transformative (*i.e.*, a different purpose from the entertainment purpose or reasonable derivative markets), this factor does not offer a great deal of assistance.[612]

Factor Three

The amount and substantiality of the portion used in relation to the copyrighted work as a whole tends to favor fair use. Although the entire work may be reproduced in the course of testing and investigating a measure used to protect access to a video game, these reproductions are intermediate copies, at least in part, consistent with authorized use of a lawfully acquired video game. The amount of the copyrighted work that is actually used by the security researcher's end-product will likely none at all. That is not surprising since the copyrighted work itself is not the focus of the research, but rather an ancillary necessity in the course of studying the technological protection measure attached to the work. Given likely nonexistent use of the copyrighted work in any results the researchers provide to the public, this factor tends to weigh in favor of fair use; in any event, it certainly does not weigh against fair use.

Factor Four

---

[610] *See Sega Enters. Ltd. v. Accolade, Inc*, 977 F.2d at 1524 (reaching a similar conclusion regarding a different kind of research that involved making copies of video games).

[611] *Id.* at 1510.

[612] *Campbell v. Acuff-Rose Music, Inc.* 510 U.S. 569, 586 (1994); *see also*, *Bill Graham Archives v. Dorling Kindersley Ltd.*, 448 F.3d 605, 612 (2d Cir. 2006)("We recognize, however, that the second factor may be of limited usefulness where the creative work of art is being used for a transformative purpose.")

Turning to the fourth factor—the effect of the use upon the potential market for or value of the copyrighted work—good faith research would be unlikely to adversely affect the potential market for or value of a work in a manner cognizable under the Copyright Act. First, because the research copy would have to be lawfully obtained and no copies of the work are distributed as a result of the study, the research would not have a direct effect on the market for the copyrighted work. To the extent that the research results in unfavorable or critical findings, any resulting harm to the market for that work would not be relevant harm to Section 106 rights.[613] Moreover, research that failed to uncover any security flaws or vulnerabilities would tend to foster the market for or value of the work. There is a social benefit in objective analysis that dispels rumors and speculation about the vulnerabilities created by a technological protection measure. Scholarly research is capable of certifying the safety of protection measures in the marketplace and may foster cooperation between researchers and the creators of technological protection measures early in the process to ensure the integrity of protection systems.

Overall, the factors tend to strongly support a finding of fair use in this context. The socially productive purpose of investigating security and informing the public do not involve use of the creative aspects of the work and are unlikely to have an adverse effect on the market for or value of the copyrighted work itself. The proponents have therefore established an underlying noninfringing use that may be affected by the prohibition.

b. The evidence of existing or likely adverse effects on noninfringing uses

The next step in the analysis is to determine whether the prohibition is adversely affecting, or is likely to adversely affect, noninfringing research. In particular, it is necessary to determine whether the record provides verifiable and measurable evidence that security flaws or vulnerabilities exist, whether the prohibition has adversely affected the ability to engage in security research, or whether there is sufficient evidence that such vulnerabilities are likely to exist with respect to either of the technological measures that have been used in relation to this class of works. Such evidence is necessary in order to determine whether an exemption is warranted for a particular class of works during the next three year period.[614]

---

[613] *Id.* at 591-592.

[614] Security research is, as a general proposition, a socially beneficial pursuit. However, this rulemaking is not intended to provide prescriptive indemnification for socially beneficial noninfringing uses without a showing that harm has occurred or is likely to occur. Moreover, the scope of permissible exemptions is limited to particular classes of works. Therefore, present or likely harm in a particular class must be established to support an exemption.

The record is essentially limited to two specific technological measures used on a wide variety of video games: SecuRom and SafeDisc. While it is undisputed that the evidence relating to SecuRom tends to be highly speculative, Professor Halderman asserted that "this situation has been crying out for an investigation by reputable security researchers in order to rigorously determine the nature of the problem that this system cause[s], and dispel this uncertainty about exactly what's going on." [615] He believed that the prohibition on circumvention is at least partially to blame for the lack of rigorous, independent analysis.[616] Professor Halderman submitted a research plan into the record to explain exactly what he proposed to examine in order to determine whether SecuROM does in fact contain security flaws or create security vulnerabilities.[617] A close inspection of the articles and websites cited by Professor Halderman in his submissions reveals little more than conjecture about whether SecuROM creates vulnerabilities. Moreover, even though a number of class action suits have been filed, including allegations that the SecuROM program cannot be completely uninstalled, other software developers dispute these allegations.[618] Critics of the allegations of vulnerabilities (found from the sources cited by Professor Halderman) have gone so far as to say that "people with no real knowledge of SecuROM are deliberately and systematically creating and then perpetuating absolutely unverifiable, often patently false claims against such protection systems, more to debase and undermine the protection system's credibility in the eyes of the public than anything else."[619] There is no clear evidence in the record that tends to prove that SecuROM is creating, or is likely to create, security flaws or vulnerabilities.

The evidence offered by Professor Halderman simply proves that suspicion exists. He alleged that further proof can only be obtained through research, and that such research is being chilled by the prohibition. It is not clear from the record whether research is in fact being chilled by the threat of the prohibition on circumvention, but a number of the activities cited in Professor Halderman's research plan appear to constitute prohibited conduct.[620] Thus, a researcher abiding by the prohibition might reasonably avoid activity that could create legal liability. It appears

---

[615] T Halderman, 5/7/09, at 186.

[616] *Id.*

[617] R29 (Halderman).

[618] *See* Tweakguides, PC Game Piracy Examined, http://www.tweakguides.com/Piracy_9.html. (Last visited 5/6/10.)

[619] *Id.*

[620] R29 (Halderman) at 3.

reasonable to conclude that in the absence of an applicable limitation on the prohibition, security research to determine the facts, without regard to the ultimate conclusion that might be reached, could be adversely affected by the prohibition.

If the evidence relating to SecuRom were the sole factual basis for the exemption, the existence of such speculation alone would be insufficient to support the recommendation of an exemption for the ensuing three-year period. As noted above, the object of this rulemaking proceeding is to designate specific classes of works with respect to which the prohibition against circumvention is actually having an adverse effect on noninfringing uses (or is likely to do so in the next three years). Such findings have always required evidence that a problem actually exists (or is more likely than not to exist in the next three years) with respect to the particular class of works.

The unsubstantiated allegations about SecuROM do not, however, serve as the sole evidentiary basis for the proposed exemption. Professor Halderman has also identified SafeDisc as another technological measure that controls access to video games. In contrast to SecuROM, SafeDisc has created a verifiable security vulnerability on a large number of computers.

Opponents of Professor Halderman's proposal do not dispute that SafeDisc created a security vulnerability, but they argue that the security flaw was patched by Microsoft in 2007, without the need of an exemption.[621] However, the evidence demonstrates that Macrovision's SafeDisc was pre-loaded on nearly every copy of Microsoft's Windows XP and Windows 2003 operating systems. It was on the market for over six years before a security researcher discovered malware exploiting the security.[622] The vulnerability had the capacity to affect nearly *one billion* PCs.[623]

The SafeDisc situation demonstrates that there have, since the previous rulemaking proceeding concluded, been verifiable and measurable security vulnerabilities in the class of video games. The concerns about SecuROM, while insufficient in and of themselves, and whether accurate or erroneous, may lend additional weight to the conclusion that security researchers are adversely affected by the prohibition on circumvention in their ability to lawfully assess whether

---

[621] C8 (Halderman) at 5, n. 17.

[622] *Id.* at 6-7.

[623] *Id.* at 5.

or not SecuROM poses security vulnerabilities on computers. Within the class of video games, the proponents have demonstrated that substantial vulnerabilities existed for a significant period of time with respect to SafeDisc. Within the same class of works, security researchers have proposed investigation of unconfirmed allegations of security vulnerabilities on another technological protection measure (SecureROM) that controls access, but have expressed unwillingness to do so without clear legal authority. Aggregating the evidentiary record, the proponents have shown that they need to be able to fix flaws that are identified in this class of works and they need to be able to investigate other alleged security vulnerabilities in this class, one that SafeDisc demonstrates is subject to such vulnerabilities.

The opponents of the exemption argue that the evidence with respect to SafeDisc must be balanced with the fact that the vulnerability was discovered and fixed without the need of an exemption. In their view, the existing market was capable of adequately resolving the problem without requiring an exemption.

The opponents' testimony that the "ecosystem in place…relies on people in the field to identify and bring to the attention of the developers the flaws that may exist" [624] demands closer scrutiny to determine whether it is borne out by the facts. The incentives of a company to fix its own problems, incentives that the opponents claim exist,[625] are not necessarily sufficient to publicize, investigate or remedially address flaws or vulnerabilities found to exist in a protection measure in all cases. The opponents asserted, but have not demonstrated, why those who created the protection measure containing the flaws will always have good reason to discover, publicize and repair them. [626] They also did not adequately address the benefit to copyright owners or the public that result from expressly permitting independent research into security flaws.

---

[624] T Metalitz, 5/7/09, at 207.

[625] *Id.* at 229.

[626] Moreover, a news report quoting a Macrovision spokesperson suggests otherwise. See *UPDATE - Buggy game DRM puts Windows users at risk*, http://www.thestandard.com/news/2007/11/08/update-buggy-game-drm-puts-windows-users-risk. (Last visited 5/6/10.) The fact that Macrovision and Microsoft "worked together during the development of Windows Vista RTM [release to manufacturing] to review the security of the Vista version of the [secdrv.sys] driver" but failed to address the vulnerability on Windows XP and 2003 until after a Symantec employee discovered the vulnerability being exploited tends to undermine the assertion that the creators of measures have sufficient incentive to discover, disclose and repair flaws and vulnerabilities in a timely manner.

The opponents of the exemption also argued that the proponents' evidence does not rise to the level of the problem established in 2006 regarding the Sony rootkit issue.[627] In the case of SafeDisc, they argued that the "vulnerability was identified and resolved, and a patch made available to consumers…."[628] They also pointed out that this vulnerability could not be exploited by a remote user; 'an attacker must convince a user to run an executable or must have valid logon credentials to exploit this vulnerability.'"[629] In testimony, they also stated that:

> the researchers, for whatever reason, apparently did not discover this problem until after some bad guys discovered it. But they were able to very quickly do the research that was needed to generate a fix and have that widely distributed. Professor Halderman paints this episode in apocalyptic terms of the millions of computers that were infected, and how much worse this was than the Sony rootkit. I don't want to underscore the obvious, there was no rootkit involved here. And, if you look at the normal channels adapted to this, to identify the problem, develop a fix and distribute a fix, we give two examples of that in our submission. And neither of them thought this was a world-ending problem. It was a problem. There's no question the fix was important. But the system worked. The research was done, and the security problem was fixed.[630]

Thus, both proponents and opponents of an exemption appear to have agreed that a problem existed with respect to SafeDisc. Moreover, despite some dispute about the scale of that vulnerability, given that the vulnerability had the potential of affecting a billion personal computers, the scale of the problem was significant. In addition to the scale of the problem, the nature of the problem is also an important factual consideration. In order to understand the nature of the problem and compare it to the evidence presented in the 2006 rulemaking relating to the Sony rootkit, an examination of additional information from the record is warranted.

c. The nature of the vulnerability

The record indicates that the PC-accessible video game market has undergone gradual change. Initially, serial numbers and passwords contained in manuals were used by copyright

---

627 *See* R46 (Joint Creators) at 48-49; T Metalitz, 5/7/09, at 197. *See also* 2006 Recommendation of the Register of Copyrights at 54-64.

628 R46 (Joint Creators) at 48.

629 *Id.*

630 T Metalitz, 5/7/09, at 197-198.

owners to ensure that users were installing authorized copies of video games before access to the games would be granted.[631] With the rise of the Internet, some copyright owners began to use remote authentication, with the user's copy being verified for authenticity by a central server of the copyright owner.[632] When such measures proved ineffective at preventing unauthorized copies to be accessed, some copyright owners pursued more aggressive strategies to control access to video games. As in the case of the Sony rootkit employed on CDs containing sound recordings, a new strategy involved installing the video game on the computer and, at the same time, surreptitiously installing a third party program along with the game. This third party program is typically installed with elevated privileges on the computer operating system, giving the program unfettered access to the rest of the PC in order to carry out tasks for the copyright owner, such as authenticating discs, enforcing access policies, and taking countermeasures against circumvention tools.[633]

Rootkits are a form of malicious code or malware that may include viruses, spyware or trojans that attempt to hide their presence from spyware blockers, antivirus, and system management utilities.[634] Rootkits come in many forms,[635] but they are only one form of malicious code.[636] As Professor Halderman stated:

> Both the Sony rootkit and the flawed SafeDisc software are so−called "device drivers." Device drivers have effectively unrestricted access to PC hardware and software, so attackers can often leverage security flaws in the drivers to bypass other security mechanisms on the PC. The flaw in the Sony rootkit grants attackers only the limited power to conceal their own files and programs; the SafeDisc flaw is much more dangerous, allowing attackers to execute unrestricted "kernel−level" code and read or write any area of the hard disk or memory of the PC, thus facilitating the complete compromise of the security of the PC. The flaws in both the rootkit and SafeDisc are exploited by so−called "privilege escalation attacks" and require the attacker to first gain some access to the PC.[637]

---

631 C8 (Halderman) at 8.

632 *Id.*

633 *Id.*

634 *See* Bryce Cogswell and Mark Russinovich, *Rootkit Revealer v.1.71*, http://technet.microsoft.com/en-us/sysinternals/bb897445.aspx. (Last visited 5/6/10.)

635 *Id.*

636 C8 (Halderman) at 5, n. 19.

637 *Id.*

A key feature of both device drivers is that they install deep within the operating system of the computer. This feature has advantages for copyright owners by providing increased control over changes that a user can make to a computer's hardware, software, settings, or interactions between these elements. Such control may prevent, for instance, the user's ability to access a work in any manner beside the secure manner chosen by the copyright owner.

This feature also has fundamental disadvantages. When a control is placed at the kernel-level of the operating system, it enables an outside source to take advantage of that high-level control, or Ring 0 access, of the computer's operating system.[638] Privilege escalation attacks, one of many forms of malicious attacks on a computer, computer system, or computer network, enable a "bug" in an application to gain access to resources which normally would have been protected from an application or user with lower privileges. [639]

Opponents of the proposed exemption stated that SafeDisc is not a rootkit. The significance of that distinction, however, is not explained and does not prove to be particularly helpful. If both rootkits and SafeDisc are device drivers that install at the kernel level and provide the potential for privilege escalation from an outside source, although potentially different in some characteristics, both have the potential to create security vulnerabilities. The fact that with SafeDisc, these vulnerabilities existed for six years before they were patched is a significant concern in a time when the news is filled with stories about cybersecurity, security threats, malicious worms, and denial of service attacks.[640] Indeed, President Obama recently stated that "cyberspace is real. And so are the risks that come with it." The President went on to state that:

---

[638] Most emulation programs, some of which are used to bypass technological protection measures, also install Ring 0 drivers at the kernel level. These emulators, and many circumvention tools, also create security vulnerabilities. For instance, Daemon Tools or Alcohol 120, which have been used by some to bypass SecuROM protection, have been reported to install Ring 0 drivers. *See Tweakguides' PC Game Piracy Examined*, http://www.tweakguides.com/Piracy_9.html. Mark Russinovich states that: "[t]here's no proof that Alcohol and Daemon Tools use rootkits to evade DRM, but the evidence is compelling. If they do their usage is clearly unethical and even potentially runs afoul of the US Digital Millennium Copyright Act (DMCA). In any case, there's no reason for these products, or any product as I've stated previously, to employ rootkit techniques." Mark's Blog : *Using Rootkits to Defeat Digital Rights Management*, http://blogs.technet.com/markrussinovich/archive/2006/02/06/using-rootkits-to-defeat-digital-rights-management.aspx. (Last visited 5/10/10.)

[639] *See, e.g.*, Port80 Blog, *You Can't Catch What You Can't See* at http://blog.port80software.com/tag/buffer-overflow-attacks/. (Last visited 5/10/10.)

[640] *See, e.g.*, Elinor Mills, *Botnet Worm in DOS Attacks Could Wipe Data Out on Infected PCs* http://news.cnet.com/8301-1009_3-10284281-83.html (Last visited 5/10/10.); John Sutter, *No Joke in April Fool's Day Computer Worm*, http://www.cnn.com/2009/TECH/03/24/conficker.computer.worm/index.html. (Last visited 5/10/10.)

"America's economic prosperity in the 21st century will depend on cybersecurity."[641] When the fact that almost one billion personal computers were potentially at risk due to the vulnerability created by Macrovision's SafeDisc is combined with the evidence asserting that the nature of this vulnerability was more profound than that which existed with the Sony rootkit situation, concern is indeed warranted.

While it is true that the security vulnerability created by SafeDisc was discovered and fixed relatively quickly even though there was no applicable exemption to the prohibition on circumvention, a full examination of the facts reveals further cause for concern. First, there is no dispute that the vulnerability existed for six years before it was discovered. Second, there is no dispute that the vulnerability was pre-installed (although dormant until access to a game using SafeDisc was loaded) on a vast number of personal computers.[642] Third, it was apparently first discovered by a malicious entity, and only after the vulnerability was being "actively exploited" did a Symantec researcher discover that the source of the problem was Macrovision's SafeDisc.[643]

Opponents of the proposed exemption highlighted that the SafeDisc "vulnerability could not be exploited by a remote user; 'an attacker must convince a user to run an executable or must have valid logon credentials to exploit this vulnerability.'"[644] While this distinguishes the SafeDisc vulnerability from other vulnerabilities, this distinction does not minimize the actual risk created. As society has learned from the clever trickery involved in phishing and surreptitious executables involved with "worms," it is not difficult to deceive some number of people, particularly if warnings are not issued *before* the vulnerability is exploited.

---

[641] REMARKS BY THE PRESIDENT ON SECURING OUR NATION'S CYBER INFRASTRUCTURE at May 29, 2009, http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/. (Last visited 5/10/10.) "(This new approach starts at the top, with this commitment from me: From now on, our digital infrastructure -- the networks and computers we depend on every day -- will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy and resilient. We will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage.") The Register does not suggest that the President was specifically referring to rootkits or similar phenomena, but they certainly relate to cybersecurity.

[642] Some reports state that in addition to being pre-installed on computers running Windows XP and Windows 2003, it was also pre-installed on computers running Windows Vista. *See UPDATE - Buggy game DRM puts Windows users at risk*, http://www.thestandard.com/news/2007/11/08/update-buggy-game-drm-puts-windows-users-risk. (Last visited 5/6/10.) However, the same report claims that Vista was immune from the vulnerability due to a pre-release security review. This fix in Vista does not appear to have resulted in further investigation regarding the source of the problem.

[643] *Id.*

[644] R46 (Joint Creators) at 48.

The opponents concluded that "the system worked. The research was done, and the security problem was solved."[645] But these claims of success do not resolve the issue. Is a vulnerability affecting potentially a billion personal computers that went undiscovered for six years and was only discovered *after* bad actors were actively exploiting the flaw evidence that the "system worked"? While it is obvious that a relatively quick fix to an identified vulnerability is beneficial, the security researcher's goal is to identify potential vulnerabilities *before* the flaw has been exploited. The opponents fail to find significance in the fact that the Symantec researcher who discovered the flaw, found it only after someone was exploiting it. Moreover, while the record does not reveal whether the Symantec researcher had to engage in an act of circumvention in order to discover the flaw, Professor Halderman could not think of any way to identify and fix the problem discovered that would not involve circumvention.[646]

The fact that Professor Halderman does not allege that SafeDisc was a "world-ending" vulnerability mischaracterizes the burden on proponents of an exemption. While anecdotal evidence, isolated occurrences, and inconveniences will not be sufficient to support an exemption, the adverse effect of the prohibition need not be devastating in order for an exemption to be warranted. The statute requires only that the proponents prove that the prohibition causes more than an insubstantial adverse effect on noninfringing uses. Moreover, the significance of the problem may affect the degree of evidence necessary to support an exemption.[647] Preventing security vulnerabilities is a significant socially-beneficial endeavor. The evidence of the existence of a potentially severe vulnerability affecting up to one billion computers that went unidentified for six years and was only discovered after being exploited demonstrates a verifiable problem, not an isolated instance and certainly not a mere inconvenience. When the record demonstrates a recent problem of such magnitude, and when it demonstrates that the prohibition on

---

[645] T Metalitz, 5/7/09, at 197-198.

[646] T Halderman, 5/7/09, at 267-268.

[647] *See* 2003 Recommendation of the Register of Copyrights at 26-27 ("The case made by Mr. Finkelstein for this exemption is also instructive for the manner in which it met the requisite showing. The evidence produced did not prove that a substantial number of people have utilized or were likely to utilize an exemption. On the contrary, the evidence tended to prove that very few people have had the motivation or technological ability to circumvent this technological measure, to investigate the lists of blocked sites in filtering software or to report on, comment on or criticize such lists. Although there was little need for an exemption in quantitative terms (*i.e.*, in terms of the number of persons likely to take advantage of it directly), it was the qualitative need for an exemption that was controlling in this case; absent the ability of a few to carry out their noninfringing efforts notwithstanding the prohibition set forth in section 1201, the many would not reap the fruits of such efforts – the information, analysis, criticism and comment enabled by the quantitatively small number of acts of circumvention.").

circumvention has had or is likely to have an adverse effect on noninfringing activities that could discover such flaws and vulnerabilities and prevent the harm likely to result from them, a case for an exemption may well have been made. However, it is necessary to consider whether the research activity can be accomplished without an exemption.

d. The risk of liability and the applicability of statutory exemptions

Even the opponents of Professor Halderman's proposal, who suggest that he does not need to circumvent as much as he says he does, acknowledge that some degree of circumvention is probably necessary in order to engage in the research that Professor Halderman has proposed to do.[648] How much research has been chilled by the prohibition on circumvention may be difficult to ascertain, but Professor Halderman's comments and testimony provide support in the record to show that some legitimate research has been, or is likely to be, adversely affected. The mere fact that legal action has not been brought against legitimate security researchers, or that permission may be available to some researchers from some companies, does not diminish the fact that legitimate researchers seeking to obey the law may understandably feel compelled to refrain from research that involves circumvention.

The opponents argued that it is possible that one of the statutory exemptions in Section 1201 might apply. Opponents pointed primarily to Section 1201(j), but they also referred in passing to Section 1201(g) (encryption research) and Section 1201(i) (protection of personally identifiable information) as providing a possible limitation on liability for researchers, such as Professor Halderman.

Opponents suggested that Section 1201(j) is the statutory exemption that most closely addresses security research, and they asserted that Professor Halderman has not demonstrated that Section 1201(j) does not apply.[649] They also stated that other statutory exemptions may apply to certain activities of security researchers.[650] They further contended that in the absence of proof

---

[648] T Metalitz, 5/7/09, at 202-203.

[649] R46 (Joint Creators) at 53.

[650] *Id.* (referring to Sections 1201(g) (encryption research) and 1201(i) (protection of personally identifiable information). The opponents do not explain why these two exemptions might be applicable here, apparently believing that merely by mentioning the two provisions, they have shifted the burden to the proponent. That is not the case. A proponent of an exemption need not catalog each and every conceivable statutory exemption that might possibly apply, and then explain why it does not apply. Nor can an opponent cast doubt on a proponent's case by mere incantation of a statutory provision when the opponent does not bother to explain why that provision

that an applicable statutory exemption does not apply, no exemption should be granted.[651] Following from this reasoning, opponents argued that the existence of a statutory exemption that may apply precludes a finding that the noninfringing use has been adversely affected by the prohibition.

But the Register's recommendation of 2006 reveals the flaw in this reasoning.[652] There are many good policy reasons why Section 1201(j) *should* be interpreted to extend to this type of security research in relation to measures placed on all works, but there is a complete lack of clarity in the statutory language or the legislative history, either preceding the introduction of Section 1201(j) into the bill or after its inclusion in the various legislative drafts of the bill, to provide a comfortable fit between the statutory language and this factual manifestation of the security vulnerability issue. Congress did not appear to anticipate this precise scenario involving access controls creating vulnerabilities. Had Congress foreseen the problem, it is reasonable to conclude that it might have addressed the issue in more precise terms. But it appears that Congress did not envision protection measures themselves becoming the source of a security flaw or vulnerability. Rather, Congress appeared to be addressing firewalls and antivirus software that were used on computers, computer systems and networks to protect their respective contents. The legislative history suggests that Congress wanted to encourage independent evaluation of such security systems as long as such research was done with the authority of the owner of the computer, system or network that they are protecting.

It is true that in many cases, security research might involve reverse-engineering or encryption research, activities addressed in the statutory exemptions found in Sections 1201(f) and (g). But the goal of security research is not congruent with those particular activities. It may also involve additional forms of circumvention in order to investigate and research security flaws or vulnerabilities. Indeed, Congress appeared to recognize that fact between the publication of the Commerce Committee Report's analysis[653] of the bill (when Section 1201(j) did not exist) and the Conference Report,[654] which sparingly explained the justification for the new Section 1201(j).

---

would apply.

[651] *Id.* at 53-54.

[652] *See* 2006 Recommendation of the Register of Copyrights at 59.

[653] Commerce Comm. Report at 36, 44-45.

[654] Report of the Committee of Conference on the Digital Millennium Copyright Act ("Conference Report"),H.R. Rep. No. 105-796, at 66-67 (1998).

At the time of the Commerce Committee Report, July 22, 1998, Section 1201(j) did not exist. In the discussion of what was then Section 102(g) of the House Commerce Committee's version of the proposed WIPO Treaties Implementation Act (now Section 1201(g) of title 17), the Commerce Committee stated that:

> In addition, network and web site management programs increasingly contain components that test systems security and identify common vulnerabilities. These programs are valuable tools for systems administrators and web site operators to use in the course of their regular testing of their systems' security. The testing of such "firewalls" does not violate Section 102 because in most cases the firewalls are protecting computer and communications systems and not necessarily the specific works stored therein. Accordingly, it is the view of the Committee that no special exception is needed for these types of legitimate products.[655]

Thus, at that point in time, there was a view that computer security did not relate to protection of copyrighted works, but rather to the protection of computers and systems. Computer security was believed to be limited to network management tools and firewalls protecting the computer, computer system or computer network as a whole. A statutory exemption was not deemed necessary because testing or circumvention of a firewall was not seen to affect a copyrighted work. In the discussion of Section 1201(g), the House Manager's Report stated:

> Today, network and web site management and security tools increasingly contain components that automatically test a system's security and identify common vulnerabilities. These programs are valuable tools for systems administrators and web site operators, to use in the course of their regular testing of their systems' security. Again, because these devices are good products put to a good use, they do not fall within the scope of the statute.[656]

Thus, both of these important components of the legislative history of the DMCA apparently assumed that computer and system security would be unaffected by the prohibition.

By October 8, 1998, the Conference Report expressed a different understanding. By that time, Section 1201(j), relating to security testing, had been added to the list of statutory exemptions. Section 1201(j)(1) defines "security testing" as:

---

[655] Commerce Comm. Report at 44-45.

[656] House Manager's Report at 17.

> Accessing a computer, computer system, or computer network, solely for the purpose of good faith testing, investigating, or correcting, a security flaw or vulnerability, with the authorization of the owner or operator of such computer, computer system, or computer network.

The Conference Report stated:

> Subsection (j) clarifies the intended effect of the bill with respect to information security. The conferees understand this act to prohibit unauthorized circumvention of technological measures applied to works protected under title 17. The conferees recognize that technological measures may also be used to protect the integrity and security of computers, computer systems or computer networks. It is not the intent of this act to prevent persons utilizing technological measures in respect of computers, computer systems or computer networks from testing the security value and effectiveness of the technological measures they employ, or from contracting with companies that specialize in such security testing.

Thus, in addition to the exception for good faith encryption research contained in Section 1201(g), the conferees adopted Section 1201(j) to resolve the additional issues related to the effect of the anti-circumvention provision on legitimate information security activities. First, the conferees were concerned that Section 1201(g)'s exclusive focus on encryption-related research does not encompass the entire range of legitimate information security activities. Not every technological means that is used to provide security relies on encryption technology, or does so to the exclusion of other methods. Moreover, an individual who is legitimately testing a security technology may be doing so not to advance the state of encryption research or to develop encryption products, but rather to ascertain the effectiveness of that particular security technology.

The conferees were also concerned that the anti-circumvention provision of Section 1201(a) could be construed to inhibit legitimate forms of security testing. It is not unlawful to test the effectiveness of a security measure before it is implemented to protect the work covered under title 17. Nor is it unlawful for a person who has implemented a security measure to test its effectiveness. In this respect, the scope of permissible security testing under the Act should be the same as permissible testing of a simple door lock: a prospective buyer may test the lock at the store with the store's consent, or may purchase the lock and test it at home in any manner that he or she sees fit, for example, by installing the lock on the front door and seeing if it can be picked.

What that person may not do, however, is test the lock once it has been installed on someone else's door, without the consent of the person whose property is protected by the lock.[657]

Congress recognized that Section 1201(g) addresses only one form of technological protection measure -- encryption. However, computer, system and network security often extends beyond encryption, and Congress also recognized that there is value in testing the effectiveness of security measures applied to computers, computer systems and computer networks. Therefore, Congress added a new provision encompassing security research in Section 1201(j). What Congress apparently did not foresee is that measures that protect copyrighted works may create vulnerabilities in computers, computer systems and computer networks. Even the analogy of door locks seems to support this understanding of Congress's view at the time of introduction of Section 1201(j)—once the lock, or firewall, was placed on a computer system, the only way to test it was with the consent of the computer owner or operator. Absent here is any discussion of the interaction between measures that protect access to works and measures that protect computers. Also absent is express language that allows circumvention of measures on copyrighted works installed on a computer that, in themselves, create security vulnerabilities.

Thus, Congress did not anticipate the manner in which technological measures that protect copyrighted works would develop in the marketplace. The legislative history of Section 1201(j) suggests that Congress was concerned about the robustness of security measures placed on computers, computer systems and computer networks. Congress, at the time of enactment, had no reason to be concerned about flaws or vulnerabilities that might be introduced into the computer, system or network ecosystem by a technological protection measure itself, because the forms of technological protection measures which create security flaws or vulnerabilities had not been introduced into the market for copyrighted works until after the enactment of the DMCA.

The optimal solution for the proponents of the proposed exemption would be to apply Section 1201(j) to cover such situations. Section 1201(j) has the benefits of potentially applying to all classes of works, existing perpetually, and exempting development, production, distribution and employment of technological means for performing the acts of security testing that might be prohibited under Section1201(a)(2) (the anti-trafficking provision).[658] The Librarian in this

[657] Conference Report at 66-67.

[658] 17 U.S.C. § 1201(j)(4) limits the trafficking provision in Section 1201(a)(2) by allowing a person to develop, produce, distribute or employ technological means for the sole purpose of performing acts of security testing. If Section 1201(j) was clearly applicable to the proponents' intended uses of security testing, this subsection would also allow the proponents to develop, produce and distribute the means for others to test their computers. This

rulemaking proceeding lacks the authority to resolve any problem in a comparably robust manner. The Librarian is limited to exempting particular classes of works; any exemption issued is limited to a three-year period; and the rulemaking has no effect on Section 1201(a)(2). This is the case despite the fact that the statutory exemption in Section 1201(f) would, if applicable, more fully resolve the overall concern raised by the proponents. As the Register stated in 2006:

> Witnesses testifying in favor of the proposed exemption also asserted that § 1201(j) is of insufficient scope because it addresses accessing computers, not access to works, and that the proponents seek access to works. As noted above, the exempted act of "security testing" involves "[a]ccessing a computer, computer system, or computer network, solely for the purpose of good faith testing, investigating, or correcting, a security flaw or vulnerability." The question is whether such activity includes circumventing an access control that protects a sound recording or audiovisual work that is stored on a computer or on removable media that may be accessed through a computer. Proponents of an exemption in this proceeding argued that § 1201(j) "appears to permit the ethical hacking into a computer system for the purpose of detecting security flaws in the firewall protecting the system. It is not clear that it permits the permanent disabling of a technological measure on a specific work when the measure causes a vulnerability."[659]

Precisely the same question is raised in the present situation, except that "sound recording" is replaced by the class of "video games." The Register's conclusion is similarly congruent:

> The language in § 1201(j) has not been construed by any court. While there is a reasonable argument that its reference to "accessing a computer, computer system, or computer network solely for the purpose of good faith testing, investigating, or correcting a security flaw or vulnerability" would include the case where correcting the security flaw involves circumventing access controls on a computer that protect a sound recording or audiovisual work rather than the computer itself, it is not clear whether it extends to such conduct. Because of the uncertainty whether § 1201(j) addresses the situation presented by this proposal, the Register cannot conclude that it is unnecessary to consider an exemption for the proposed class of works. Under the circumstances, the proposed class must be considered on its merits.[660]

---

provision might be improved by clearly allowing not only the means to test, but also *to fix* or correct identified security flaws.

[659] 2006 Recommendation of the Register of Copyrights at 59.

[660] *Id.*

Although Congress envisioned a somewhat different factual scenario at the time it drafted the statutory provision, the general concern expressed by the legislature at the time convinces the Register that the present situation warrants handling under Congress's established fail-safe mechanism, which is embodied in this rulemaking. The Register finds that a security vulnerability has been proved with regard to the class relating to video games and that an exemption is warranted. The Register is also persuaded that the means of tailoring the class of works should be guided by Congress's general approach to the problem in Section 1201(j). Accordingly, in formulating this particular class of works, the Register recommends following the congressional model, as such:

> Video games accessible on personal computers and protected by technological protection measures that control access to lawfully obtained works, when circumvention is accomplished solely for the purpose of good faith testing for, investigating, or correcting security flaws or vulnerabilities, if
>
> (1) the information derived from the security testing is used primarily to promote the security of the owner or operator of a computer, computer system, or computer network; and
> (2) the information derived from the security testing is used or maintained in a manner that does not facilitate copyright infringement or a violation of applicable law.

This formulation of the exemption differs from the language proposed by Professor Halderman in a number of respects. The recommended language avoids the conjunctive language "and create or exploit security flaws or vulnerabilities that compromise the security of personal computers," because, upon reflection, such language would appear to require a security researcher to know that a technological protection measure creates a security flaw or vulnerability prior to investigation. If a security researcher discovered that there were no problems with the measure protecting the video game, then he or she would fall outside the exemption. The goal of security research is to discover *whether or not* a measure protecting a video game contains a security flaw that creates vulnerability. As Professor Halderman stated in his comment about SecuROM, "SecuROM reportedly may interfere with the operation of a PC's CD and DVD burners and several software programs; some users even claim that SecuROM can even interfere with virus and firewall protection software, opening a serious hole in the defenses of the PC. . . ."[661] "And the ongoing uncertainty over SecuROM's safety could probably be settled by a single definitive scientific study; instead, a regime of panic, protests, and litigation has taken hold over what may

[661] C8 (Halderman) at 8-9.

turn out to be nonexistent or easily reparable faults."[662] The evidence presented was not solely the interest in confirming known security flaws or vulnerabilities, but rather to investigate whether such flaws or vulnerabilities exist at all, and if they do exist, identify what they are. The ability to objectively perform a scientific investigation can be both noninfringing and socially beneficial when the investigation reveals that the technological measures are safe. Such a finding, for instance with respect to SecuROM, would dispel concerns and offer marketplace stability for such a measure. This would assist not only the public, but copyright owners as well, by offering them objective verification whether a measure is safe for use on an array of copyrighted works.

The opponents pointed out that Professor Halderman "very carefully" did "not make any assertions about any security vulnerabilities about SecuROM. He simply notes accurately that there are class-action lawsuits pending, that a lot of allegations have been made, there's a lot of furor, there's a very toxic atmosphere surrounding it."[663] But the opponents did not argue that security researchers should not be able to discover whether or not a measure creates security flaws or vulnerabilities. Instead, opponents argued that there is no evidence that researchers have been chilled by the prohibition in their ability to engage in research, and, *inter alia*, that various statutory exemptions in Section 1201 could apply.[664] The opponents admitted that "[o]f course there's no way to guarantee that there are [no flaws or vulnerabilities], but we also have an ecosystem in place … that relies on people in the field to identify and bring to the attention of the developers the flaws that may exist."[665]

These arguments and statements by the opponents of the exemption do not deny that security flaws or vulnerabilities may well exist in video games or that there may be sound reasons to investigate whether a vulnerability exists. The opponents simply argued that such necessary investigation is going on without an exemption through amorphous means by entities contained in the "ecosystem" of "people in the field." However, as explained above, the opponents did not show that vulnerabilities identified in SafeDisc were disclosed or rectified in a timely manner or that questions about SecuROM have been adequately investigated. Good faith security researchers reasonably desire to play a role in the security ecosystem. Professor Halderman provided direct testimony that his research is being adversely affected by the prohibition and his

---

662 *Id.* at 7.

663 T Metalitz, 5/7/09, at 199.

664 *Id.* at 199-206.

665 *Id.* at 207.

testimony was credible. The proponents have demonstrated that the nature of the problem is socially significant and that good faith, reasonable investigation is a noninfringing and prudent activity. The Register therefore recommends adopting the proposed exemption in order to clarify that good faith investigation will be exempted even when the investigation fails to identify a security flaw or vulnerability. It is believed that permitting such good faith noninfringing research will serve copyright owners, the security industry and the public.

The Register also believes that the inclusion of the conditions attached to the exemption, which are modeled on the conditions Congress included in Section 1201(j), will eliminate any potential abuse of this exemption that would harm the copyright interests of the owner of a work. The language in the first condition, the information derived from the security testing is used *solely to promote the security of the owner or operator of a computer, computer system, or computer network*, is intended to encompass the activities of good faith researchers even when no flaws or vulnerabilities are discovered. If a researcher verifies that a technological protection measure does not compromise the security of a computer, computer system, or computer network, the information derived from that testing will nevertheless promote the security of the owner or operator of such systems. An objective evaluation of a protection measure may be the only way to dispel concerns raised about a measure. The independent verification of the safety of a technological protection measure will help promote the security of the owner or operator of a computer, computer system, or computer network.

The second condition in the exemption ensures that the information derived from good faith security testing, whether positive or negative, will be used in a responsible manner that does not facilitate infringing or otherwise unlawful activity.

These two conditions are based on the factors set forth in Section 1201(j)(3), reflecting the Register's judgment that the Section 1201(j) exemption demonstrates Congress's judgment as to the conditions under which circumvention for the purpose of security testing should be permitted.[666]

[666] As noted above, it is unclear whether the exemption for security testing in Section 1201(j) applies to cases such as this, because it appears that Congress may not have anticipated that security testing issues would arise in the context of research involving access controls that protect a specific work of authorship, as distinguished from a computer, computer system or computer network. The Register recommends that the Librarian designate this class of works because of that lack of clarity, but in fashioning the class of works she has tried to remain faithful to Congress's judgment that the propriety of circumvention for the purpose of security testing should be judged based on the factors set forth in Section 1201(j)(3).

e. The application of the statutory factors

In applying the statutory factors of Section 1201(a)(1)(C), the Register finds that the case has been made for designation of a class of works.

Factor One

Under the first factor, the availability of use of copyrighted works, the exemption recommended will encourage the use of copyrighted video games on personal computers by allowing access controls applied to games to be inspected by legitimate, third-party security researchers. Such good faith research will promote trust in video games protected by technological protection measures that control access, and will provide facts that may offset rumors and speculation about such measures that are propagated online. Conversely, there is no reason to believe that the exemption will in any respect make copyrighted works less available.

Factor Two

The second factor, the availability for use of works for nonprofit archival, preservation, and educational purposes, does not appear to be implicated by the proposal or the exemption.

Factor Three

The third factor, the impact that the prohibition on circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research, is central to the recommended exemption. The prohibition is having an impact on criticism, comment, teaching, scholarship and research. The crux of the exemption relates to security research that currently cannot take place without implicating the prohibition on circumvention. The proponent of the exemption seeks to engage in scholarship on the issue, but at least part of his research plan is adversely affected by the prohibition. Although not directly implicated by the exemption, to the extent that research and scholarship is enabled by the exemption, such research and scholarship will presumably facilitate criticism, comment, news reporting, and teaching on the findings of this research and scholarship.

Factor Four

The fourth factor, the effect of circumvention of technological measures on the market for or value of copyrighted works, also tends to support the exemption. Increasing the computer security of the public will foster trust in well-tested protection systems and digital works themselves. The restrictions on the purpose of the research and the use and maintenance of the results will serve to prevent activity that enables infringement, while at the same time allowing legitimate researchers to engage in research on equal footing with malicious researchers.

In relation to other factors that the Librarian considers appropriate, it is essential to stress the heightened concerns for computer and network security that the country faces generally, and the recognition of cybersecurity in particular. While the Librarian's authority is limited in this rulemaking, the ability to promote legitimate security research within that authority cannot be overlooked. No one knows what security flaws or vulnerabilities will be exploited in the future, but the identification of flaws or vulnerabilities by legitimate researchers before they are discovered by wrongdoers is a significant concern.

Given the limited scope of the rulemaking proceeding, it is beyond the Librarian's authority to exempt all classes of works from the prohibition on circumvention when circumvention is accomplished for the purpose of good faith testing, investigating, or correcting security flaws or vulnerabilities. Designation of a class of works must be based on a record that demonstrates that users of *that particular class of works* are being or in the next three years are likely to be adversely affected by the prohibition on circumvention. While it may be socially beneficial to permit security testing and research in relation to all classes of works, neither the record nor the statute provide the Librarian with any basis to do so. It is worth asking whether it makes sense to require security researchers to rely only on a regulatory exemption that depends on which particular classes of works have been, or are likely to be, adversely affected in a particular three-year period. As demonstrated by the records and results in the 2006 proceeding, and in the current proceeding, the problem is a moving target, with no ability to predict which class will suffer harm in the next three years.

The Register is sympathetic to the views of the Assistant Secretary of Commerce for Communications and Information that this problem may arise in other classes. However, the Register is constrained by the statute and the record in this rulemaking to recommend exemptions for classes of works for which noninfringing uses are, or in the next three years, likely to be

adversely affected by the prohibition on circumvention. The only class of works for which such an existing or likely adverse effect has been demonstrated is the class of video games. The Register supports Congressional review of the problem to determine whether a statutory exemption should be enacted.

E. Computer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete. A dongle shall be considered obsolete if it is no longer manufactured or if a replacement or repair is no longer reasonably available in the commercial marketplace.

Background. In each of the preceding rulemakings, requests were made to designate classes of works involving dongles (*i.e*., hardware locks attached to a computer that work with software to prevent unauthorized access to that software). In the course of those rulemakings, evidence was presented showing that damaged or malfunctioning dongles can prevent authorized access to protected software. The records in those proceedings demonstrated a genuine problem for authorized users of expensive computer programs given that software vendors may have gone out of business or have otherwise been unresponsive. The concern centered on those who lose their ability to gain access to their lawfully acquired copies of those computer programs due to malfunctioning or damaged hardware that cannot be replaced or repaired.

Three years ago, an request to designate a class relating to dongles was again before the Copyright Office. In making the recommendation whether it should be renewed, the Register found that the legal and analytical rationale for designating this class remained unchanged. The key question then was whether there was evidence in the record that supported the new request. The Register concluded that a sufficient factual showing was made in the 2006 proceeding to designate the class. However, she stated that for purposes of clarity and consistency, the description of the class should be refined to include an explanation of what constitutes an "obsolete" dongle.[667] The Register noted that this conclusion was consistent with the existing exemption for "computer programs and video games distributed in formats that have become obsolete and which require the media or hardware as a condition of access."[668] She concluded that similar language should be part of the description of the dongle class.[669] After consideration of the

---

[667] *See* 2006 Recommendation of the Register of Copyrights at 33-34.

[668] In that case, the class of works included a second sentence describing when a format is obsolete: "A format shall be considered obsolete if the machine or system necessary to render perceptible a work stored in that format is no longer manufactured or is no longer reasonably available in the commercial marketplace." *Id.*

[669] *Id.* at 36.

facts and the law, the Register recommended the following class:

> Computer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete. A dongle shall be considered obsolete if it is no longer manufactured or if a replacement or repair is no longer reasonably available in the commercial marketplace.[670]

Comments. Joseph V. Montoro, Jr., on behalf of Spectrum Software, Inc., has proposed the following class of works related to dongles:

> "Computer programs protected by dongles that prevent access due to malfunction or damage *or hardware or software incompatibilities or require obsolete systems or obsolete hardware as a condition of access.*"[671]

The italicized text represents language that departs from the language used to describe the class designated in 2006.

At the outset, Montoro explained that a dongle is a type of hardware that attaches to either the printer port or the USB port of a computer in order to make secured software function. He stated that dongles are sold along with certain types of software and are necessary for the user to access that software on a computer. He further explained that in order for the dongle to operate properly, the operating system must support the hardware and the required device driver must be installed.[672]

Montoro stated that there are four situations where an exemption is necessary to rectify actual harm: (1) when dongles become obsolete; (2) when dongles fail; (3) where there are incompatibilities between the dongle and the operating system, and (4) where there are incompatibilities between the dongle and certain hardware.[673] He asserted that a software user

---

[670] *Id.*

[671] C6 (Montoro) at 1.

[672] A device driver is software that links certain types of hardware or peripherals to the operating system of a computer. *See* http://www.pctechguide.com/glossary/WordFind.php?wordInput=Device%20Driver. (Last visited 5/6/10.)

[673] Mr. Montoro filed exhibits, attached to his initial comment, in support of these four categories. (1) Exhibits 1-6 were filed in support of the "obsolete" claim; (2) Exhibits 7-14 were filed in support of the "failure" claim; (3) Exhibits 15-25 were filed in support of the "incompatible operating system" claim; and (4) Exhibits 26-32 were filed in support of the "incompatible hardware system" claim.

must be able to circumvent the dongle when a software company is no longer in business and cannot offer support for its product. He commented that such "obsolete" dongles may leave hundreds of customers stranded without a backup to access protected software. Second, he asserted that circumvention of access controls is necessary when a dongle malfunctions, is damaged, or otherwise fails. He commented that obstacles arise when a defunct software company can no longer offer support for the software and/or dongle. He specifically stated that in such cases, users cannot receive maintenance or a replacement dongle if there is a malfunction or a failure. Third, he explained, that in some cases, the dongle has not been damaged but it is unworkable on a current operating system. He stated that an updated or new operating system may render a perfectly functioning dongle useless, thereby preventing access to protected software. He specifically pointed out that Microsoft has listed certain dongle incompatibilities with its operating systems. Fourth, he explained that a dongle is rendered useless when hardware changes render the dongle useless. Montoro noted that the most prominent example is when printer port[674]-compatible dongles cannot be used because many newer computers do not have a printer port.[675] In addition, Montoro had stressed that the issue is as much about the computer ecosystem as it is about dongles, in particular. He commented that the Register must realize that the dongle, the operating system software and the computer hardware work in tandem and that his request necessarily covers all of these parts.[676]

---

[674] A printer port is sometimes referred to as a parallel port. "In the computer world, a *port* is a set of signal lines that the microprocessor, or CPU, uses to exchange data with other components." J. Axelson, *Parallel Port Complete 1-2* (1996). In 1996, a book on parallel ports observed that they were "found on just about every PC, or IBM-compatible personal computer," and described them as "a workhorse of PC communications. On newer PCs, you may find other ports, such as SCSI, USB, and iRDA, but the parallel port remains popular because it's capable, flexible, and every PC has one." *Id.* at 1-2. The book noted that "The parallel port was designed as a printer port, and many of the original names for the port's signals … reflect that use. But these days, you can find all sorts of things besides printers connected to the port." *Id.* at 2. Eleven years later, a book on "Upgrading and Fixing PC's observed that "For years, all printers attached to a standard printer port (also known as a *parallel port*) on your PC. Today, many plug straight into the USB port." A. Rathbone, *Upgrading and Fixing PCs for Dummies* 49 (2009).

[675] As noted above, Mr. Montoro provided several points of evidence that he said supported his request. In May 2009, he sent along several additional documents, noting that they related to obsolete hardware and operating systems and would be referenced in his testimony before the Copyright Office at the May 8, 2009, hearing on Section 1201. E-mail from Joseph Montoro to Robert Kasunic, May 6, 2009.

[676] In his testimony before the Office, Mr. Montoro stated the following: "You can't simply have a dongle and run a program without an operating system. You can't run a program without a computer. . . . So to answer the question again, is it a question that the dongle malfunctions or is it the operating system or is it the hardware, and I really submit that it's all of these combined because nothing works by itself." T Montoro, 5/8/09, at 54.

The Software & Information Industry Association ("SIAA") commented that it does not oppose renewing the existing class of works, but objects to expanding it beyond its current terms.[677] SIIA specifically disagreed with the addition of the phrase "hardware or software incompatibilities or require obsolete systems or obsolete hardware as a condition of access," when this phrase does not even relate to the dongle itself. It asserted that an incompatible dongle is an interoperability issue and is thus not related to access controls. Nevertheless, SIIA stated that it believes that an exemption is necessary when a dongle malfunctions or is damaged and no replacement is reasonably available.

Like SIIA, Joint Creators submitted a comment opposing an expansion of the existing class. They believed that the Register's prior statements on the necessity of an exemption are just as valid today as they were three years ago; that is: (1) the record does not support an exemption for computer software protected by dongles that are working properly and (2) an exemption is not warranted simply when a dongle is malfunctioning or damaged, but where a replacement is reasonably available.[678] They also commented that software or hardware issues associated with dongles may be resolved through industry cooperation.

On the other hand, commenter Lincoln Han supported the proposed class because: (1) dongles have not gained market acceptance and are only used among niche market software developers; (2) customer usage will outlive the dongle and/or the software company; and (3) changes in computer hardware and software will make many dongles unusable. NTIA has advised the Register that, to the extent she finds that the record supports the continued designation of this class, it would support it as well as long as it is not expanded.[679]

Discussion. The record supports the continued designation of a class relating to dongles. A proponent in this rulemaking must show by a preponderance of the evidence that there has been or is likely to be a substantial adverse effect on noninfringing uses by users of copyrighted works. Montoro has effectively met his burden of proof regarding dongles that are malfunctioning or damaged and which are obsolete, a point on which there is no disagreement among the commenters and the witnesses at the hearing. When the dongle no longer functions

---

[677] SIIA is a trade association representing the software and information industry. It represents approximately 500 high-tech companies that develop market software and electronic content for business, education, consumers, the Internet, and entertainment.

[678] *See* R46 (Joint Creators) at 43.

[679] *See* NTIA Letter of November 4, 2009, at 13.

and is obsolete, there is a substantial adverse effect on non-infringing uses because there is no other means to access a lawfully acquired software program on a computer without resorting to such a device. As Montoro has demonstrated in the last three rulemakings, as well as in the current record, when a dongle malfunctions or becomes obsolete, a person lawfully entitled to access it should be able to rely on self-help if remedial measures are not reasonably available in the commercial marketplace.[680] Moreover, the record reveals no evidence of harm to the market for, or value of, copyrighted works protected by dongles since the issuance of the original exemption in 2000.

The class, however, should not be expanded to include situations in which a replacement dongle is reasonably available or can be easily repaired. Some copyright owners legitimately use dongles to protect access to a program by unauthorized users and are entitled to the full benefit of the prohibition as long as reasonable accommodations are offered for malfunctioning or damaged dongles. Montoro has not demonstrated that the standard applied when crafting previous classes – reasonably available in the marketplace—is insufficient to meet the needs of users of copyrighted works whose dongles malfunction or are damaged.

Montoro also argues that the current class should be expanded to reach situations involving incompatibility between the dongle and a new or upgraded version of an operating system. He states:

> These dongles do not operate on their own. Beginning with Windows NT, hardware and software programs could not "talk" to each other directly. Instead they must communicate through a device driver. Some of these products are not compatible because the driver for the operating system is not available. This is an issue that needs to be addressed because the physical piece is intact. It has not been damaged; technically it has not even had the opportunity to malfunction. However it is obsolete on a current operating system.[681]

---

[680] Among other unopposed factual bases for the continuing need for the existing exemption, Mr. Montoro cites the acquisition of two of the largest dongle manufacturers—Rainbow Technologies and Aladdin Knowledge System—by SafeNet, "leaving a boatload of dongles that would be discontinued and no longer supported." T Montoro, 5/8/09, at 43.

[681] C6 (Montoro) at 5-6.

In his testimony, Montoro went on to explain that "Dongles can cause incompatibilities with hardware or software. A dongle that works perfectly well may suddenly experience problems following a major operating system upgrade or a driver patch."[682]

Montoro makes a compelling point: dongles are hardware, but they necessarily interact with software by means of communication to the application being protected via the operating system on the computer. Changes to an operating system, whether in the form of an update or upgrade, may interfere with that communication between the dongle and the operating system in such a way that legitimate access to the application is prevented. Moreover, Montoro also posits that because particular applications often work as a component part of more a more complex system of applications, interactions between applications may also lead to communication problems between the dongle and the operating system.

Opponents respond that this problem is unrelated to the dongle itself and instead relates to interoperability and not access.[683] In some cases, this may be true. It is difficult to see why creating a driver for a dongle to enable it to communicate with an operating system would "descramble a scrambled work, decrypt an encrypted work, or otherwise []avoid, bypass, remove, deactivate, or impair a technological measure protecting access."[684] Creating a driver merely to enable a dongle to work with an operating system may not implicate the prohibition on circumvention at all.

But opponents beg the question raised by Montoro when they state that this issue is, in fact, an interoperability issue. This is not simply a matter of trying to run an application program on a system that is incompatible with that program. Montoro alleges that in some cases, a functioning dongle will cease communicating with the operating system due to changes in the operating system, the hardware, or incompatibilities between applications.[685] It is not surprising that the concern raised does not address the dongle itself, because as Montoro fully agrees that, in

---

[682] T Montoro, 5/8/09, at 40 quoting John Gillespie-Brown.

[683] R17 (SIIA) at 4. *See also* T Metalitz, 5/8/09, at 55-56 ("I think what Mr. Montoro's describing is interoperability problems and again I don't think that -- this is not new to this proceeding or perhaps this is made in a somewhat different context. I'm not sure there really is an expectation, which I think he indicated at the beginning of his presentation, that every piece of software will work forever on any operating system that comes along, even if the operating system on which it originally was designed, for which it was really designed becomes obsolete. I'm just not sure that that's a problem that falls within the scope of this proceeding.")

[684] 17 U.S.C. § 1201(a)(3)(A).

[685] C6 (Montoro) at 5-8.

this scenario, the dongle is working properly. The problem is that the dongle is no longer communicating with the program it is intended to protect, that is, it is no longer fulfilling its intended function. As a result, the user who should be able to lawfully access the software is no longer able to access the work due to the hardware and software communication incompatibility. The dongle, a technological measure that controls access to the software, is not permitting access to a work even though access has been authorized and the dongle is supposed to permit access.

However, Montoro fails to fully articulate the particular harm or the necessary remedial measures that need to be taken. To the extent that the entire problem is the absence of a device driver, the creation of a new device driver to enable the operation of the dongle would not appear to implicate the prohibition on circumvention. But the problem may be more complicated. Although Montoro states that what his company primarily does is "create a device driver" for the dongle, he also suggests that in addition to the functionality for the driver, he emulates the dongle, by creating a new program that provides the authenticating answer to the question that the application is asking.[686] To the extent that Montoro is emulating the dongle rather than enabling it, he may be defeating "unauthorized access" – the very function that the dongle is intended to prevent. If the emulation of the dongle replaces the dongle, the access restrictions that the dongle is supposed to impose (*i.e.*, individual use or site license of a specific number of users) might be eliminated. While there is no suggestion in the record that Montoro is enabling unauthorized access, neither he nor the opponents of the exemption discuss the consequences of such apparent emulation. The Register is left with a record that does not offer enough information to evaluate whether it is actually necessary to circumvent an access control in order to overcome the "incompatible operating system" problem. Furthermore, Montoro fails to explain the scope of the problem relating to dongles that cannot communicate with applications. He does not explain with any specificity the nature of the problems cited as examples or the remedial actions (or lack thereof) offered by the copyright owners or applications or operating systems. For example, Montoro mentions the problem of a dongle that cannot be installed in Windows Vista. However, he does not demonstrate or even assert that there are no reasonably available operating systems that can perform the task or that the problem cannot be corrected by a professional through other

[686] T Montoro, 5/8/09, at 78. The Register notes that to the extent that Mr. Montoro (or anyone else) may be "offer[ing] to the public, provid[ing], or other traffic[king] in … [a] service … that … is primarily designed … for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title," this rulemaking proceeding can offer him no immunity from liability for violation of Section 1201(a)(2), the prohibition on offering products or services that circumvent technological measures that control access to works.

means. As the Register noted in 2000 and 2003, "there is no unqualified right to access works on any particular machine or device of the user's choosing."[687]

Moreover, Montoro specifically states that when an update to Windows Vista caused many dongles to be unresponsive, it "took weeks before the issue was resolved." In this instance, Montoro has shown, albeit perhaps unintentionally, that the matter may have been rectified in the market without the need to resort to circumvention.[688]

Although Montoro has articulated a potentially relevant problem, he has failed to build a sufficient record to support an designation of a class that addresses software and operating system incompatibilities. A sufficient record would require more detail about the precise cause of the problems, the scope of the problem, and the noninfringing means available to resolve the problem. The record before the Register does not, at present, support expansion of the class in this regard.

The evidence presented in the record also does not support Montoro's request to expand the class in relation to obsolete hardware, specifically parallel ports on computers. While it appears to be the case that parallel ports may be in the process of becoming obsolescent, there is insufficient evidence in the record to support the conclusion that parallel ports are currently, or in the next three years, will be obsolete. Montoro does not even argue that parallel ports are presently obsolete, but only that many new computers do not provide a parallel port. In order to make a case for an expanded class of works in relation to obsolete hardware, Montoro would have to sufficiently demonstrate that the hardware is, or is likely to be, obsolete in the next three year period (either as a preinstalled item or as an optional configuration), that the unavailability of this obsolete hardware would adversely affect noninfringing uses, and that copyright owners are not meeting the legitimate needs of existing users. Montoro has failed to demonstrate the case for this expansion in the current record.

---

[687] 2000 Recommendation of the Register of Copyrights, 65 Fed. Reg. at 64,569; 2003 Recommendation of the Register of Copyrights at 143. Moreover, the Register made that observation in recommending the rejection of a proposal for an exemption based on the incompatibility of a particular operating system (Linux, preferred by the proponents of the exemption) with a particular access control (*i.e.*, CSS).

[688] Similarly, Lincoln Han's comment supporting Montoro's proposed exemption mentions an instance where he could not access a particular computer program due to hardware incompatibilities: "I had an IBM Thinkpad 600x notebook computer, which has a parallel port. However, due to the proprietary design of the BIOS, the parallel port and hence the dongle could not be recognized by the software. I was forced to use another desktop computer with a more standard BIOS just for this software." R26 (Han) at 1. Han tacitly admits that he was able to find an alternate way to access the software, thus resolving the issue without substantial hardship.

In sum, it is important to recognize that while the record may be deficient in the present circumstances, it may be the case that there will be sufficient evidence to support an expanded class of works if the request were to come before the Copyright Office in the next rulemaking in 2012. Three years hence, there may be clear and convincing proof that software incompatibilities have indeed rendered some dongles obsolete and that computers with parallel ports are no longer manufactured or otherwise available in the marketplace. Until such time, the Register finds that the relief Montoro seeks is limited to the class of works stated below.

In the case of a malfunctioning or damaged dongle that is obsolete, there is a demonstrated substantial adverse effect on a noninfringing use, and the Register finds that the case has been made to designate an appropriately delineated class of works. As such, the Register recommends the following class of works, which is identical to the class designated in 2006:

> *Computer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete. A dongle shall be considered obsolete if it is no longer manufactured or if a replacement or repair is no longer reasonably available in the commercial marketplace.*

IV. OTHER CLASSES CONSIDERED, BUT NOT RECOMMENDED

A. Subscription based services that offer DRM-protected streaming video where the provider has only made available players for a limited number of platforms, effectively creating an access control that requires a specific operating system version and/or set of hardware to view purchased material; and

Motion pictures protected by anti-access measures, such that access to the motion picture content requires use of a certain platform.

Background. A recurring theme in all four rulemaking proceedings since 2000 has been the desire on the part of some participants in the proceedings to be able to gain access to protected digital works on platforms of their choosing, rather than on the platforms or platform options offered by content providers. In this proceeding, there were two proposals that sought exemptions allowing circumvention of technological protection measures in order to provide access to motion pictures on platforms other than those authorized by content providers or their licensees.

Comments. One proponent, Megan Carney, requested an exemption to allow circumvention of DRM-protected streaming videos offered by subscription based services, where the provider has made players available only for a limited number of platforms. This restriction of viewing options to a limited range of platforms, she argued, effectively constitutes an access control by requiring a specific operating system version and/or set of hardware to view purchased material. In particular, Carney seeks to use Netflix's "Watch Instantly" streaming video feature, which installs digital rights management and runs only on certain platforms of computer software and hardware.[689] "Watch Instantly" is included, at no charge, in Carney's monthly Netflix membership, but she is unable to use it because she does not own a compatible platform.[690] She seeks an exemption that would allow a user in her situation to create a separate program to circumvent the DRM on the streaming service system in order to view streaming video content made available by Netflix.[691]

Another proponent, Mark Rizik, requested an exemption to allow the circumvention of motion pictures on DVDs protected by the CSS access control system, which requires the use of a certain platform for access. Specifically, Rizik would like to view, on a computer running on the Linux system that does not have a CSS-licensed video player, DVDs which are only viewable on CSS-licensed players.[692] Rizik sought an exemption that would permit the creation of an unencrypted digital copy of the DVD by decrypting and extracting contents of DVDs for personal viewing purposes on Linux operating systems.[693]

---

[689] C2 (Carney) at 1. As part of a Netflix movie rental membership agreement, "Watch Instantly" allows a subscriber to instantly stream content to her own computer provided that the computer meets the technical specifications to install and run Microsoft's proprietary "Silverlight" application. Silverlight offers a cross-platform environment for Mac OS, Windows, and Linux operating systems. The number of times a subscriber can access this streaming video feature correlates with the subscriber's monthly membership category. If a subscriber has an account that provides for unlimited access, the subscriber may access the streaming content as many times as the subscriber wants. However, if the account is a fixed number membership account, the subscriber may only access a certain number of streaming videos set by the membership agreement using the "Watch Instantly" feature. For more information, *see* www.netflix.com/HowItWorks. (Last visited 5/7/10.)

[690] The reasons for her inability to access the technology are two-fold. While the "Watch Instantly" feature will work on Apple computers running the OS X or Windows operating systems, Carney apparently cannot install either because the Mac she is using is an older model that does not support either operating system. T Carney, 5/8/09, at 219.

[691] T Carney, 5/8/09, at 221.

[692] C3 (Rizik) at 1.

[693] *Id.* at 3.

The proponents of both classes of works sought exemptions permitting them to circumvent the access controls because, they contend, it is too expensive to acquire the hardware and software with the minimum requirements necessary to view motion pictures on the distribution mechanism of their choice. Carney was unable to access content provided by Netflix's "Watch Instantly" feature due to technical incompatibility issues between her computer (an Apple notebook with a Power PC Chip)[694] and Netflix's system requirements for the streaming video service (requiring an Intel Chip). She contended that it would cost hundreds to thousands of dollars to upgrade or purchase a new computer system that meets the technical requirements to utilize the "Watch Instantly" feature.[695] She further contended that this platform requirement is being used as an access control that prevents her from viewing the streaming video content included in her monthly subscription to Netflix.[696]

Similarly, Rizik stated that viewing DVDs on a Linux system is cost prohibitive because of the licensing fee that DVD CCA charges developers to include a DVD player in each copy of Linux.[697] Linux developers freely distribute the Linux operating system at no cost per download, and thus, he asserted, they lack the revenue or resources to cover the necessary costs.[698] Moreover, Rizik claimed that there is a lack of incentive for Linux developers to create a proprietary DVD player for Linux because the limited number of Linux users does not constitute a commercially viable market.[699] Finally, he contended that it is too expensive to purchase a copy of the Windows operating system and a larger hard drive to create a dual-boot system (using Windows and Linux side by side), or to purchase a separate TV and DVD player.[700]

Both of the proponents also contended that these software and/or hardware platform requirements are primarily used as anti-competitive tools in the marketplace. Carney stated that Netflix's Vice President of Corporate Communication has suggested that "the reason non-Intel based Macs are unable to take advantage of Netflix's 'Watch Instantly' feature is because Apple

---

694 T Carney, 5/8/09, at 235-36.

695 *Id.* at 211.

696 C2 (Carney) at 2.

697 C3 (Rizik) at 2.

698 *Id.*

699 *Id*. at 3.

700 *Id*. at 8 & 10.

refuses to license its DRM to Netflix."[701] She speculated that the inability to use the Netflix "Watch Instantly" feature on non-Intel-based Macs is because Apple, which offers its own movie rental services, prefers to limit platform options in order to prevent competition[702]

Rizik suggested that the CSS licensing scheme for DVDs is also used as an anti-competitive tool. He explained that Linux users are ideologically at odds with Windows because the "spirit of Linux" is opposed to a closed-source operating system, like Windows, which "obscures and limits functionality because its makers 'know better' than its users what they need."[703] He also critiqued the Register's 2006 suggestion that Linux users create dual-boot Windows/Linux systems as "particularly abrasive and unfair… to require Linux users to 'pay fealty' to Microsoft by purchasing a product, in order to gain access to motion pictures that intrinsically have nothing to do with the Windows platform."[704] Finally, Rizik pointed out that small operating systems like Linux will only have a "fair shake at the competition" if the DVD player is "legally decoupled" from the DVD content.[705]

Both proponents argued that there are no reasonable, non-infringing alternatives to circumvention for those wishing to engage in the activity affected by these platform requirements. Carney asserted that there is no other way she will be able to access the purchased streaming video content that is offered as part of her monthly membership in Netflix without circumventing the system requirements of the "Watch Instantly" feature.[706] She elaborated that the free streaming video site "Hulu" does not have as wide of a selection compared to Netflix,[707] and that she is limited to 18 DVDs a month if she uses her Netflix subscription solely to receive DVDs by mail.[708] Furthermore, she stated that if a person who is able to use the Netflix "Watch Instantly"

---

[701] C2 (Carney) at 2.

[702] *Id.*

[703] C3 (Rizik) at 9.

[704] *Id.*

[705] *Id.*

[706] C2 (Carney) at 2.

[707] *Id.*

[708] *Id.* This statement is not clearly supported by the options available on Netflix. The service provides free access to the "Watch Instantly" feature for any of the "unlimited" plans it provides for a monthly charge. There are a variety of unlimited plans which range from 2 DVDs at-a-time up to 8 DVDs at-a-time. With the higher priced option, assuming that it takes five days to receive replacement DVDs, it would appear that one could receive up to

service could use it instead of a cable television subscription, it could result in cost savings for the consumer.[709]

Likewise, Rizik claimed that there is no other suitable alternative to circumvention for viewing purchased motion pictures on DVDs on a Linux-based computer. As stated above, he rejected the alternative method of using a TV and DVD player to watch purchased material because, he said, it is more efficient as a matter of economics, living space, and portability to watch copied content from DVDs.[710] Furthermore, while he conceded that a few options for Linux DVD players do exist, he argued that these systems are tied to the Linux systems Linspire and TurboLinux, which are "obscure and unpopular compared to other Linux distributions such as Ubuntu and Debian."[711] He further emphasized that he is not seeking a free DVD player for Linux systems, but rather argued that Linux should be able to offer its users the "second-best" option of converting DVDs to video files in order to be able to view purchased material on Linux systems.[712]

The MPAA opposed the requested exemptions, characterizing the proponents' complaints as relating to "dissatisfaction with the platforms chosen for distribution of movies and other audiovisual content or the commercial terms on which they are offered, rather than to the ability to engage in noninfringing uses" and arguing that "Section 1201(a)(1)(C) was not intended to provide relief to customers who are unhappy with the commercial terms on which copyright owners make their works available or the platforms on which they choose to distribute their works."[713] MPAA also observed that owners of motion pictures and television programming are taking actions to meet the demands of consumers and to offer their content with options that permit people to view movies and TV shows when and how they want.[714]

---

48 DVDs within a month. There is no evidence that Netflix imposes a monthly limit on the number of DVDs that can be received under a plan. The Netflix plan options state: "Exchange DVDs as often as you want." Any limit appears to be a practical one caused by mail handling and delivery time.

709 *Id.*

710 C3 (Rizik) at 10.

711 *Id.* at 7.

712 *Id.* at 11.

713 R45 (MPAA) at 6.

714 *Id.*

Time Warner also opposed the requests, asserting that technological protection measures are actually used to facilitate the delivery of motion pictures and other works in new and innovative ways, while appropriately managing the rights to those works.[715] Time Warner stated that by licensing its content to a variety of outlets, it aims to "ensure that even if a work is not available on one platform, consumers will be able to access such content in other ways."[716] It noted, however, that "[a]llowing for circumvention of TPMs employed by services would ultimately hamper our goal to provide access to content on as broad a range of platforms as possible."[717]

Joint Creators opposed the requests, noting that in past rulemakings, the Register has recognized that tethering works to particular platforms provides copyright owners with some assurances that those works will not be easily placed on peer-to-peer file-sharing networks and that this is likely to encourage some copyright holders to make their works available in digital formats. It observed that the movies and television programs that the proponents desire to watch are available in a variety of formats.[718] It also asserted that Carney had failed to establish that any of the services to which she was referring actually use operating systems as access controls.[719] The Joint Creators made similar observations relating to Rizik's proposal, noting that Linux-based DVD players already exist and that there are also many other alternatives for accessing motion pictures on DVDs or by other means.[720]

The Assistant Secretary of Commerce for Communications and Information has advised the Register that he believes that the record does not support granting the requested exemptions.[721]

---

715 R48 (Time Warner) at 3-7.

716 *Id.* at 8.

717 *Id.*

718 R46 (Joint Creators) at 23.

719 *Id.*

720 *Id*. at 25-26.

721 NTIA Letter of November 4, 2009, at 13.

Discussion. Similar exemptions to those proposed by Carney and Rizik have been requested in the past three rulemakings.[722] Although the streaming video proposal presents a new factual situation, the Register concludes that the legal arguments are fundamentally similar to the Linux proposals advanced in the previous three rulemaking proceedings, as well as to the Linux proposal made in the current rulemaking. Likewise, arguments for the streaming video and Linux exemptions fail for fundamentally the same reasons as the earlier Linux proposals, and neither proposal warrants an exemption to the prohibition on circumvention.

As the Register noted in her recommendation in the 2006 rulemaking, "[i]n previous rulemakings, exemptions have been denied … because although a user might have been prevented from engaging in a noninfringing use of a work using a particular device, the user could engage in the same noninfringing use of the work using a different device."[723] Neither Carney nor Rizik have made a case for a departure from this principle. Nor have either of the proponents shown that one cannot engage in their desired use of copyrighted works, gaining access to and viewing motion pictures, albeit by means other than their preferred means of access, and opponents of the proposed exemptions have demonstrated that such alternative means exist and are readily available.

1. *Effect of Technological Measures*

As a threshold matter, it is unclear from the record regarding the streaming video situation what is actually prohibiting Carney from being able to access the Netflix "Watch Instantly" feature and, in particular, whether the technological issue is centered around an access control.[724] Although it appears that Carney does not have access to the feature for viewing motion pictures, this is not necessarily because an access control is preventing access. By analogy, failing to have access to FM radio programming that results from owning only an AM radio does result in a lack of access, but the cause for that lack of access is unrelated to the prohibition on circumvention. In

---

[722] *See* 2000 Recommendation of Register of Copyrights, 65 Fed. Reg. at 64,567-64,569; 2003 Recommendation of Register of Copyrights at 142-146; and 2006 Recommendation of Register of Copyrights at 72-74.

[723] *See* 2006 Recommendation of Register of Copyrights at 60 (citing and quoting 2000 Recommendation of the Register of Copyrights at 64,569 ("there is no unqualified right to access works on any particular machine or device of the user's choosing. There are also commercially available options for owners of DVD ROM drives and legitimate DVD discs. Given the market alternatives, an exemption to benefit individuals who wish to play their DVDs on computers using the Linux operating system does not appear to be warranted.").

[724] T Carney, 5/8/09, at 234-39.

Ms. Carney's case, she does have online access to Netflix's website, but does not have the software and hardware necessary to view the on-demand motion pictures. Unlike the straightforward radio analogy, the "Watch Instantly" service includes digital rights management that must be installed into the operating system in order to obtain access to this content. What is unclear is whether this digital rights management has anything to do with the lack of access, or whether the denial of access is simply software and hardware incompatibility. In a sense, the problem may involve both issues. Because Ms. Carney does not have hardware or software that is compatible with the chosen digital rights management system, there are no alternative DRM systems currently available on Netflix to provide Ms. Carney with access. And, because her operating system is incompatible, it seems likely that even if there is DRM that may block her access to the motion pictures she wishes to view, the circumvention of that DRM would be futile because the operating system's incompatibility would still prevent her from viewing the motion pictures.

Regarding DVD circumvention, there is a record established in this rulemaking proceeding that CSS qualifies as a technological measure that protects access. However, authorized decryption of CSS is available on many operating systems on the market which enable access to the works contained on CSS-protected DVDs. Because the Linux OS is generally distributed for free, but a license to decrypt CSS requires the payment of a fee, there appears to be a philosophical incompatibility between Linux and proprietary fee-based software to a greater extent than there is a technological incompatibility. This view is supported by the fact that CSS-compatible DVD players are in fact available for Linux systems.

2. *Alternatives to Circumvention*

Many alternatives exist for both Carney and Rizik. There are streaming video alternatives and other online content download sites and vendors that are able to service individuals who have non-Intel chip computers.[725] Furthermore, alternative methods to access content through online distribution and on-demand access have continued to flourish since the previous rulemaking in 2006. Consumers may access online movie stores and/or vendors to rent or purchase electronic

[725] A consumer may watch streaming video on network sites, like www.abc.com, (Last visited 5/7/10.) www.cbs.com (Last visited 5/7/10.), and www.nbc.com (Last visited 5/7/10.), or even purchase electronic sell-through or video-on-demand downloads from vendors like the iTunes Store or through www.amazon.com (Last visited 5/7/10.).

copies of video content through an increasing number of websites, game consoles,[726] and even set-top-boxes.[727] Streaming video content is also more readily being offered on websites offering broadcast network programming. As explained in the 2006 rulemaking, "if a user may access the content on a DVD in readily-available alternative ways or may purchase the works in alternative formats, the need for an exemption simply becomes a matter of convenience or preference."[728]

Even if such streaming video services are not available for persons using certain equipment or operating systems, other alternatives exist in the marketplace that offer access to the audiovisual content that such persons desire to watch. The statute directs the Librarian to consider the continued availability of copyrighted works for use. There are alternative formats on which these works may be viewed instead of streaming. Netflix's core business model is the subscription rental of DVDs; the "Watch Instantly" service is, at least at this point, a free add-on to Netflix's unlimited DVD rental service and not a service offered independently to the public. Thus, the issue is not whether access to a particular motion picture exists, but whether it exists in the format in which it is desired. The fact is that access does exist for Carney and those who are similarly situated. If Carney desires to obtain that access by means of Netflix's "Watch Instantly" feature, she may need to make a modest investment in a new computer or a new operating system. Otherwise, she can still rent DVDs of the movies she wishes to watch (either from Netflix or elsewhere) or take advantage of other video streaming or download services.

Carney's argument, taken to its logical conclusion, is essentially a claim that either all works should be available in every format by means that are compatible with every device or that all works that are made available to some users must be made available to all users. Neither argument is sustainable.

Netflix appears to be offering its "Watch Instantly" service in order to insure continued subscriber retention. As noted above, it offers this service to customers who can fulfill the requirements for free. Moreover, the service is not limited to computers. Subscribers can purchase a set-top device in order to make this free service available on television sets.

---

[726] *See* Sony Playstation and PSP, http://www.us.playstation.com/News/PressReleases/480 (Last visited 5/7/10.) .

[727] *See* Blockbuster's Video On Demand set-top-box, at http://www.blockbuster.com/outlet/electronics/onDemand?cid=ondemandFromHome (Last visited 5/7/10.); *see also* http://www.vudu.com/ (Last visited 5/7/10.).

[728] *See* 2006 Recommendation of Register of Copyrights at 74.

In short, there is undisputed evidence that many alternatives exist for access to the works in question.

With respect to Rizik's proposal, Linux users also have more alternatives to circumvention than Rizik suggests. Contrary to the argument that there is a lack of DVD players on popular Linux systems, DVD CCA points out that Dell, a major computer manufacturer and vendor, currently offers three PCs that come configured with the Ubuntu 8.04 Linux operating system with DVD Playback.[729] Moreover, DVD CCA observes that "CSS has been licensed royalty-free on reasonable and non-discriminatory terms to a variety of manufacturers." Moreover, Linux users still have the option to view their purchased material utilizing a television and a DVD player, a dedicated DVD player (such as a portable DVD player with its own screen for viewing DVD), or the aforementioned alternatives. The plethora of alternative options available to view video content precludes the need to recommend an exemption to enable a subset of Linux users the option to circumvent access controls in order to view purchased DVDs that are known to be inaccessible without a licensed player.[730]

3. *Cost-Effectiveness and Convenience*

In each of the three preceding rulemakings the Register, relying on the legislative history of Section 1201, has emphasized that "'mere inconveniences … do not rise to the level of a substantial adverse impact' on noninfringing uses – a necessary showing in order to justify exempting a class of works from the prohibition on circumvention.[731] In each case, the Register has concluded that complaints about the inability to view DVDs on computers running the Linux operating system relate, ultimately, at best to such mere inconveniences.[732]

---

[729] R37 (DVD CCA) at 14, n.1.

[730] *See* http://www.netflix.com/NetflixReadyDevicesList?lnkce=nrd-l&trkid=425738&lnkctr=nrd-l-n (Last visited 5/7/10.) (containing a list of available devices to connect to a television, one of which costs less than $79.00).

[731] *See* 2000 Recommendation of Register of Copyrights, 65 Fed. Reg. at 64,558, 64,562, 64,569; 2003 Recommendation of Register of Copyrights, at 11, 17, 18, 108, 113-15, 119, 123, 130, 143-145, 157, 170, 171; and 2006 Recommendation of Register of Copyrights at 22, 71-72, 74.

[732] *See* 2000 Recommendation of Register of Copyrights, 65 Fed. Reg. at 64,569; 2003 Recommendation of Register of Copyrights at 143-145; and 2006 Recommendation of Register of Copyrights at 74.

Carney suggests that the streaming video feature of Netflix may give consumers a cost saving benefit by substituting for a monthly cable subscription,[733] but it is not the purpose of this rulemaking to provide consumers with the most cost-effective manner to obtain commercial video content. If the consumer wants to obtain content, there are many reasonably-priced alternatives that may fulfill the consumers' wants and needs. Regarding Linux users, seeing that the cost of standalone DVD players has decreased since the previous rulemaking,[734] purchasing a DVD player is not an unreasonable, cost-prohibitive alternative and circumvention of CSS cannot be justified due to an alleged absence of inexpensive means of access to the desired works. Though a complete absence of reasonably priced alternatives might tend to support an exemption, that is not the record in this proceeding.

Moreover, as noted above, mere consumer inconvenience is not sufficient to support an exemption. The statute does not provide the Register with the responsibility of enabling the most convenient method of consuming video content. For example, while Carney may desire a platform "that is most useful for home entertainment purposes in general,"[735] the fact that such a platform does not, in her view, yet exist in the marketplace does not compel the recommendation of an exemption in order to facilitate the creation of such a platform.. Although the choices in ways to view video content may not be offered in all consumers' preferred manner, consumers have a variety of options at their disposal.

With respect to the Linux proposal, the fact that a consumer may not be able to play a particular work on the Linux platform of the consumer's choice is not sufficient to justify an exemption when there are other platforms and alternatives available to view purchased material.

The proponents have advanced requests aimed to satisfy their convenience and preferences as to how they would like to access media and have failed to demonstrate a need for remedial action. Accordingly, the Register cannot recommend either exemption in light of the alternatives and options that exist in the marketplace today.

B. Lawfully purchased sound recordings, audiovisual works, and software programs distributed commercially in digital format by online music and

---

[733] C2 (Carney) at 2.

[734] DVD CCA's comments provide evidence the cost of standard DVD players has decreased since the previous rulemaking and are now available for purchase over the Internet for $50.00. R37 (DVD CCA) at 15, n.2.

[735] C2 (Carney) at 2.

media stores and protected by technological measures that depend on the continued availability of authenticating servers, when such authenticating servers cease functioning because the store fails or for other reasons; and

Lawfully purchased sound recordings, audiovisual works, and software programs distributed commercially in digital format by online music and media stores and protected by technological measures that depend on the continued availability of authenticating servers, prior to the failure of the servers for technologists and researchers studying and documenting how the authenticating servers that effectuate the technological measures function.

Background. Many technological measures regulate user access to copyrighted works via connections to remote online authenticating servers. In contrast to access controls that are physically bundled with a copy of the work and maintain the same restrictions over their useful life, access controls linked to authenticating servers allow rights-holders to remotely operate technological measures that control access to their works.[736] In the typical case, an authenticating server is used to determine whether or not a user seeking access on a particular device to a work that he or she has purchased or licensed is in fact authorized to do so. Sometimes this authentication occurs only when: (1) the work is added to a new device; (2) a new operating system is installed on a device; or (3) in the event of a system crash.[737] In other instances authentication occurs more frequently.[738] In any event, access control via an authentication server always requires that the server be operational; if the server is shut down, the authentication process cannot take place.

Christopher Soghoian of the Berkman Center for Internet & Society at Harvard University has proposed two classes of works pursuant to Section 1201(a)(1)(A) to allow the circumvention of "technological measures that depend on the continued availability of authenticating servers" (or "DRM servers") for the following two uses: (1) by consumers, for access to and ordinary enjoyment of purchased works, and (2) by technologists and researchers, documenting the function of the technological measures. The Register does not recommend approving either of

---

[736] *See* R46 (Joint Creators) at 58.

[737] *See, e.g.* Walmart memo quoted at http://www.boingboing.net/2008/09/26/walmart-shutting-dow.html, (Last visited 5/10/10.) and cited in C10A & 10B (Soghoian) at 7 (describing the access limitations on purchased access-controlled music files after authenticating server ceases operation).

[738] *See, e.g.*, Google Video Store (beta) at 5, available at http://www.google.com/press/guides/video_overview.pdf, (Last visited 5/10/10: Click on "Quick View" to access the document) cited in C10A & 10B (Soghoian) at 2.

these classes, primarily because there is no evidence that the ban on circumvention has produced any adverse effects so far, and there is only speculation that it is likely to cause any adverse effects within the next three years. In the discussion that follows, each proposed class will be discussed in turn.

1. *Circumvention for access and ordinary use of works*

Comments. Soghoian's proposal relating to DRM servers that control access to "lawfully purchased sound recordings, audiovisual works, and software programs" was based upon several recent instances where "online music and media stores" tether their commercial distribution of digital works to DRM servers that ceased operation. Inclusion in the class would be conditioned upon the particular authentication server ceasing to function; circumvention of operational DRM servers was not contemplated. Soghoian argued that "when the DRM servers malfunction or are shut down by their operators, consumers lose the rights to engage in the legitimate, non-infringing usage of content that they lawfully purchased and reasonably expected to continue using."[739] However, there is no evidence that such a loss of rights has actually occurred thus far.[740]

Soghoian first cited to examples of stores offering the purchase and/or rental of digital motion pictures (Circuit City's Digital Video Express and Google Video Store), both of which used DRM servers and both of which shut down their servers when they decided to discontinue their services.[741] Upon the shut down of the servers, the Circuit City and Google stores offered full refunds to purchasers.[742]

Next, Soghoian offered the example of three digital sound recording stores that initially shut down their DRM servers without offering remedies to customers, only to reverse course after consumer complaints. One of these, Yahoo Music, after an initial announcement that it was ceasing operations and that its DRM servers would be shut down, later offered full refunds to its

---

[739] C10A & 10B (Soghoian) at 2.

[740] *See, e.g.*, T Soghoian, 5/6/09, at 78 ("MR CARSON: Okay. So, so far no one has been adversely affected? MR SOGHOIAN: So far, no one has been adversely affected.").

[741] C10A & 10B (Soghoian) at 4-5.

[742] *Id.* at 5.

customers.[743] Another, Microsoft's MSN Music Store, ceased operations in 2006 when Microsoft established a new music store – Zune Marketplace – but kept its DRM servers running in order to provide authentication for consumers who had purchased DRM-protected tracks. In 2008, MSN announced that it would be shutting down the server, and then announced that it would keep the server operational through at least the end of 2011.[744] The third digital music store example is that of Walmart which, as part of its move towards making all of its downloads available DRM-free, announced the cessation of its authentication server operations.[745] Yet, like MSN, Walmart changed course and ultimately decided to keep its DRM servers operational indefinitely.[746]

Soghoian also offered three examples of digital media stores who currently sell or have sold copies protected by DRM servers, copies he argued are "vulnerable to similar loss of usage in the event of a shutdown, breakage or obsolescence of the stores' authenticating servers": (1) Apple's iTunes Store, which offers motion pictures and sound recordings; (2) Microsoft's Zune Marketplace, which offers sound recordings; and (3) Napster, which now sells exclusively DRM-free music, but that had until May 2008 sold sound recordings tethered to DRM servers.[747]

Soghoian argued that, given the record he presents of digital media stores shutting down

---

[743] *Id.* at 6, n. 16 citing Antone Gonsalves, *Yahoo to Reimburse Customers Of DRM-Protected Music*, Information Week, http://www.informationweek.com/news/personal_tech/music/showArticle.jhtml?articleID=209601121. (Last visited 5/10/10.)

[744] *Id.* at 6, n. 12 citing Eliot Van Buskirk, *Microsoft Backtracks on MSN Music DRM Abandonment*, Wired.com, http://www.wired.com/listening_post/2008/06/microsoft-backt/. (Last visited 5/10/10.)

[745] *Id.* at 7, n. 19 citing BoingBoing.com, *WalMart shutting down DRM server, nuking your music collection -- only people who pay for music risk losing it to DRM shenanigans*, http://www.boingboing.net/2008/09/26/walmart-shutting-dow.html. (Last visited 5/10/10.)

[746] *Id.*, citing BoingBoing.com, *WalMart now says they'll keep the DRM servers on forever*, http://www.boingboing.net/2008/10/10/walmart-now-says-the.html. (Last visited 5/10/10.) Soghoian's assertion in his July 10, 2009, letter to the Copyright Office that Walmart will shut down its DRM servers on October 9, 2009, is incorrect. Soghoian's source for this claim [Mark Hefflinger, *Walmart to End Support for DRM-Wrapped Songs in October*, Digital Media Wire, (June 1, 2009) http://www.dmwmedia.com/news/2009/06/01/walmart-end-support-drm-wrapped-songs-october. (Last visited 5/10/10.)] bases its report upon a Hypebot post [http://www.hypebot.com/hypebot/2009/06/walmart-shutting-down-drm-download-servers.html (Last visited 5/10/10.)] that in turn bases its report on a Walmart memo of September 26, *2008*. This 2008 announcement was, as explained above, later withdrawn.

[747] C10A & 10B (Soghoian) at 7-9. Soghoian also mentioned software (one video game and one operating system), access to which is controlled by DRM servers. *Id.*, at 9-10. However, this category of works is not "distributed . . . by online music and media stores," and thus doesn't fit into his proposed class. Soghoian also failed to demonstrate any situation when a DRM server controlling software access has even been threatened with a shutdown.

their DRM servers, and given the increased migration of customers from physical CDs to downloads, "it is likely that in [the next three years] at least one DRM-media store and/or its authenticating servers will shut down."[748] Such a likelihood, he maintained, will adversely affect the noninfringing use of the protected works by those who purchased them. He proposed that exempting circumvention of DRM server technology after a server has stopped functioning is a reasonable remedy for these adverse effects under three of the four Section 1201(a)(1)(C) factors.

Factor One

Soghoian argued that the first factor, the availability for use of copyrighted works, supports the designation of his proposed class because once a DRM server is disabled, consumers who have purchased works that require authentication through the server will find that they are denied "the lawful ability, for which they have paid, to access and use purchased content."[749] Such use, Soghoian asserted, is plainly noninfringing because it does not involve the exercise of any of the Section 106 exclusive rights because it consists solely of accessing and privately performing copies of purchased works.[750] Additionally, Soghoian dismissed the option of burning CDs from downloaded works as an alternative to circumventing the access controls as "inadequate," challenging the quality of such reproductions, and pointing out that such a "burning" option is not available for downloaded motion pictures.[751]

Factor Two

Regarding the second factor of "the availability for use of works for nonprofit archival, preservation, and educational purposes," Soghoian presented hypothetical scenarios of libraries and colleges purchasing DRM-protected works that, after the DRM servers have been shut down, cannot be used with new operating systems or on other devices, thus becoming functionally inaccessible.[752]

---

748 *Id.* at 12.

749 *Id.* at 11.

750 *Id.* at 12.

751 *Id.* at 16-17.

752 *Id.* at 12-13.

Factor Three

Soghoian did not raise any arguments with regard to the third statutory factor in his exemption request.

Factor Four

With regard to the fourth factor, "the effect of circumvention of technological measures on the market for or value of copyrighted works," Soghoian asserted that, because his proposal would only allow circumvention in order to access works already purchased, such circumvention would have no impact on the market for those works.[753]

In addition to arguing the merits of his proposal based upon the statutory factors, Soghoian asserted that exempting circumvention of server-based access controls on digital media files is consistent with classes of works designated by the Librarian in prior rulemaking proceedings. He maintained that the class designated in 2006 relating to hardware locks attached to a computer that interact with software to prevent unauthorized access to that software (also known as the dongle exemption)[754] supports his proposal because "DRM schemes are simply a software version of [dongles] that apply not only to software, but also to audio and video files."[755] Soghoian also found a relevant precedent in the 2006 class relating to obsolete computer programs and video games distributed in formats that require the original media or hardware as a condition of access.[756] He argued that, like computer programs that are considered obsolete because the necessary operating systems are no longer available to support their formats, digital download files become obsolete when they can no longer communicate with their DRM servers and thus cannot be accessed.[757]

Joint Creators, Time Warner, and the AACS-LA all submitted separate comments opposing an exemption for the circumvention of access controls linked to DRM servers.

---

753 *Id.* at 13.

754 *See* 2006 Recommendation of the Register of Copyrights at 33-36.

755 C10A & 10B (Soghoian) at 14.

756 *See* 2006 Recommendation of the Register of Copyrights at 24-33.

757 *See* C10A & 10B (Soghoian) at 14-15.

Joint Creators made four primary arguments against the exemption. First, they contended that access controls linked to DRM servers are exactly the "use-facilitating" kinds of access controls sought to be protected by Congress,[758] and that an exemption aimed at such controls would inhibit their implementation, and thus delay or prevent the introduction of new services.[759] Time Warner joined the Joint Creators in this argument, maintaining that authentication servers are prevalent in all digital distribution channels and that they "facilitate the incremental addition of rights."[760] These benefits, Time Warner stated, outweigh the "unsubstantiated concerns" raised by Soghoian.[761]

Second, Joint Creators asserted that there has been no evidence of adverse effects upon noninfringing uses from the prohibition on circumventing DRM server-linked access controls, and that no likelihood of such effects exists either. Joint Creators emphasized the responses by proprietors of digital media stores to customer complaints, and stated that, either through refunds or through stores keeping DRM servers operating, "the scenario of . . . customers being stranded really has not occurred."[762]

Third, Joint Creators argued that the terms of service of a digital download store "will virtually always provide that the stores in question may discontinue service when necessary," meaning that customers who purchase DRM-protected works have in fact only purchased the ability to access the works for as long as the DRM server is operational.[763]

Fourth, according to Joint Creators, sufficient alternatives to circumvention exist such that circumvention is not necessary and thus, an exemption should not issue. Joint Creators pointed to the options of burning copies of purchased works onto blank CDs,[764] and of purchasing the works in other unprotected formats (such as physical CDs).[765] They also argued that, even after a DRM

---

758 *See* House Manager's Report at 6.

759 *See* R46 (Joint Creators) at 58.

760 T Aistars, 5/6/09, at 34.

761 R48 (Time Warner) at 14.

762 T Metalitz, 5/6/09, at 23.

763 R46 (Joint Creators) at 60.

764 *Id.* at 61.

765 T Metalitz, 5/6/09, at 28-29.

server ceases operation, those works already authenticated on a customer's device or devices will continue to be accessible despite lack of contact with the server, and that the specter of a complete, unanticipated loss of access to purchased works is thus a very unlikely prospect.[766]

The Joint Creators also challenged Soghoian's comparison of circumventing authentication servers with classes from previous rulemakings. They argued that the grounds for circumventing access controls in the cases of dongles and obsolete computer programs and video games are easily distinguishable from those Soghoian presented in support of his proposal.[767] They maintained that a more apt comparison is to earlier, rejected proposals relating to circumvention of access controls in order to use copyrighted works on particular platforms.[768]

The Assistant Secretary of Commerce for Communications and Information has advised the Register that he believes that the record does not support granting the requested exemption.[769]

Discussion. The Register must decline to recommend the proposed class for the simple reason that the proponent has not sustained his burden of demonstrating that the prohibition on circumvention of access controls either has produced, or is likely to produce, adverse effects on noninfringing uses of this class of works. As the NOI announcing the present rulemaking stated, "actual instances of verifiable problems occurring in the marketplace are generally necessary in order to prove actual harm."[770] No such instances have been shown. If, in the absence of any current adverse effect, an exemption is to be based solely upon anticipated harm, "the evidence of likelihood of future adverse impact during that time period [must be] highly specific, strong and persuasive."[771] Evidence of such a compelling nature is lacking in this instance.

In evaluating a proposed class, the Register must first determine whether the technology at issue is in fact "a technological measure that effectively controls access to a work protected under

---

766 R46 (Joint Creators) at 62; T Metalitz, 5/6/09, at 27.

767 R46 (Joint Creators) at 63.

768 *Id.*

769 NTIA Letter at 13.

770 *See Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies*, 73 Fed. Reg. at 58,075 (Oct. 6, 2008).

771 House Manager's Report at 6.

[title 17]."[772] Technological measures employed on digital downloads that operate through remote authentication servers are intended to control access to copyrighted works when in operation, and thus meet the statutory definition. In addition, such measures also control access even when disabled. Soghoian has demonstrated that a disabled server, by failing to authenticate legitimate users, in fact still effectively controls access to copyrighted works – at least to some degree. Thus, technological measures employed on digital downloads that are intended to operate through remote DRM servers, but can no longer do so because the servers have been disabled, qualify as the kind of access controls for this rulemaking to properly address.

The fundamental question in evaluating this proposed class is whether the adverse effects complained of by the proponent, "DRM-based stores that cease to operate or abandon their authenticating server system cause their customers to lose full, and often any, access to, and thus use of, their lawfully purchased works,"[773] are real, verifiable and reasonably likely to recur. There are several persuasive reasons in the record to answer this question in the negative.

Regarding the three categories of copyrighted works that Soghoian identifies in his proposed exemption, he presents no information that one of them, software in this instance, is even being sold by online retailers using authentication servers. Thus, the Register's review of adverse effects must be restricted to sound recordings and audiovisual works. Works in the latter category, according to Soghoian's comments, were sold by two entities, Circuit City and Google, who, upon deciding to withdraw from the market, fully refunded their customers' purchase costs.[774] In his testimony, Soghoian stated that he was willing to narrow his exemption to permit circumvention only "in the event that the service does not provide any remedy for consumers."[775] He further stated that "the refund is a totally appropriate and satisfactory remedy."[776] Since the record of DRM-protected audiovisual works shows only that there were two defunct services that

---

[772] 17 U.S.C. § 1201(a)(1)(A).

[773] C10A & 10B (Soghoian) at 11.

[774] *Id.* at 4-5.

[775] T Soghoian, 5/6/09, at 58.

[776] *Id.* at 77.

provided acceptable remedies, there is no reason for the Register to consider this category of works in her determination.[777]

Regarding sound recordings, of the three retailers who stopped selling DRM-protected works, Yahoo Music has provided full refunds.[778] The two others, MSN Music and Walmart, were faced with consumer backlash after announcing that they were going to shut down their authentication servers, and thus announced that they would keep the servers operational, in MSN's case through 2011, and in Walmart's case, indefinitely.[779] The record demonstrates that, thus far, there have been no adverse effects on the noninfringing use of DRM-protected sound recording downloads since purchasers retain identical access and use abilities. Soghoian points out in his request that consumer outcry has "so far prevented customers from losing complete access to their lawfully purchased works."[780] This point reinforces the Register's conclusion that it has not been demonstrated that customers have lost any access.

Soghoian's case in support of his proposed class focused more on future harm, arguing that "there is no reason to believe that other companies or services that fail or are shut down in the future will provide similar corrective steps."[781] He based this conclusion upon the belief that companies smaller than Microsoft and Walmart will not have the resources to provide refunds or keep authentication servers operating.[782] He also suggested that given the state of the economy, more companies will be jettisoning their DRM-protected music businesses,[783] and that in doing so, they may decide simply to deactivate their authentication servers without advance warning.[784] This appears to be pure conjecture. Soghoian presented no evidence supporting his claim that if another online retailer decides to disable its authentication server, it will leave affected consumers without a remedy. To the contrary, the record shows that, even though their Terms of Service

---

[777] iTunes also sells DRM-protected audiovisual works, but because none of its activities were cited as evidence of past harm or likelihood of future harm, the Register does not consider them as a category of works the noninfringing use of which is at risk.

[778] C10A & 10B (Soghoian) at 6.

[779] *Id.* at 5-7.

[780] *Id.* at 2.

[781] *Id.*

[782] *Id.* at 11.

[783] T Soghoian, 5/6/09, at 10.

[784] *Id.* at 54-55.

clearly allow them to disable their authentication servers,[785] two companies (MSN Music and Walmart) are instead keeping them operational. Thus, the prediction that within the next three years consumers will be prevented from accessing and using DRM-protected works due to the cessation of operations by an authentication server falls into the hypothetical zone.

Because the record provides no evidence for the allegation that the prohibition on circumventing disabled authentication servers has caused, is causing, or will cause adverse effects on noninfringing uses of copyrighted works, it is unnecessary for the Register to speculate upon whether an exemption would be appropriate if the opposite were true. However, it is worth noting that, in the case of every sound recording download service cited by Soghoian, disabling the authentication server does not deprive the user of all access to the purchased works. As Soghoian himself notes, "while [loss of access] will not necessarily happen immediately after a particular store is discontinued, it does take place once the DRM authentication servers are shut down and a user decides to take any action with respect to the works that requires a connection [to] the servers."[786] In other words, a DRM server that has been shut down still leaves the user with at least one, if not more, accessible copies of the protected works, although that access might cease depending upon other actions by the user, such as when a new operating system is installed. In contrast, the 2006 exemptions regarding "original only" access controls and malfunctioning dongles that Soghoian references concern DRM technologies that, absent circumvention, completely prevent the noninfringing use of the works they control.[787]

It is also unnecessary for the Register to address whether the uses that Soghoian alleges have been adversely affected are in fact noninfringing uses. Nor is Soghoian's analysis of the factors in Section 1201(a)(1)(C)(i)-(iv) relevant in light of his failure to make a satisfactory threshold showing that the alleged harm has occurred or is likely to occur. For the reasons elucidated above, the Register recommends rejection of this proposed class.

2. *Circumvention for technologists and researchers to document how authentication servers function*

Comments. Soghoian's second proposal would exempt circumvention of the same DRM

---

[785] *See, e.g.*, R46 (Joint Creators) at 60.

[786] C10A & 10B (Soghoian) at 11.

[787] *See* 2006 Recommendation of the Register of Copyrights at 24-33 ("original only" access controls), 33-36 (dongles).

servers controlling access to the same categories of works as his first proposal, discussed above. However, instead of being for the direct benefit of consumers seeking to circumvent defunct access controls, it would aid "technologists and researchers studying and documenting how the authenticating servers that effectuate the technological measures function."[788] Such study and documentation, the proposal states, would take place "prior to the failure of the servers."[789]

This class is intended to support Soghoian's first proposed class[790] by providing consumers with documentation about how DRM servers function, so that they can actually exercise the exemption. In Soghoian's words, "it is far less likely that even if people have the ability, the lawful ability to circumvent the DRM after the service fails, if they are not able to gather the information necessary ahead of time, there is not going to be much they can do."[791] Gathering information required to circumvent DRM protections linked to authentication servers, Soghoian asserted, requires research into messages being sent "back and forth between the customer's computer and the central DRM authentication server," as well as observing "the computer instructions that are executed as a song, movie, or piece of software is decrypted and run."[792] According to Soghoian, attempting to study such interactions when the server is inoperative will be difficult, if not impossible.[793]

Soghoian's legal argument in support of this class rests upon a comparison with the 2006 "rootkit" class. There, the Librarian designated a class of works relating to "technological protection measures that control access to lawfully purchased [sound recordings and associated audiovisual works on CD] and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities."[794] Soghoian's proposal focuses on the purpose of the "rootkit" class, contending that because his

---

[788] C10A & 10B (Soghoian) at 1.

[789] *Id.*

[790] *See* C10A & 10B (Soghoian) at 19 ("the purpose of the researcher exemption, which is to effectuate the general user exemption when circumvention is needed, …").

[791] T Soghoian, 5/6/09, at 19.

[792] C10A & 10B (Soghoian) at 18.

[793] *Id.* Along the same lines, Soghoian also argued that even a research exemption for the window of time between the announcement that an online retailer's DRM servers will be shut down and the actual shut down date is insufficient because future DRM server shutdowns may come without warning. *Id.* at 20.

[794] 2006 Recommendation of the Register of Copyrights at 53-54.

proposed class for researchers is also intended solely for good faith testing, investigation, and correction, (with the additional purposes of reverse engineering and documenting), it too meets the requirements for designation as a class of works in this rulemaking proceeding.[795] He does point out however, that "the cases of failed DRM and copy protection systems do not easily fit into the category of 'security flaw or vulnerability.'"[796]

As with Soghoian's first proposed class, Joint Creators, Time Warner, and the AACS LA all submitted comments opposing his proposal relating to circumvention of DRM servers for the purposes of studying and documenting their functions.

Joint Creators argued that the research proposal is unjustified: "because there is no need for an exemption for consumers, there is similarly no need for an exemption aimed at research activities."[797] They also contended that his request is merely a thinly veiled attempt at achieving an exemption from the Section 1201(a)(2) prohibition on providing circumvention tools and services.[798] Finally, Joint Creators stated that the comparison to the 2006 "rootkit" class is inapposite because Soghoian's proposal does not address "security flaws and vulnerabilities."[799]

In addition to these objections, Time Warner presented testimony that designation of Soghoian's "researcher" class could put much electronic content at risk. Time Warner argued that its authentication server systems worked to expand the range of content it offered to consumers as well as the range of uses.[800] Designating a class that permitted researchers to circumvent DRM servers controlling access to works purchased from online retailers would, Time Warner warned, result in the disruption of other DRM server functions because "the hack is the hack" and it applies to the technology, not to the particular work or category of works being protected.[801]

---

795 C10A & 10B at 19.

796 *Id.*

797 R46 (Joint Creators) at 64.

798 *Id. See also* Post-Hearing Response of Joint Creators to Copyright Office Questions relating to Authentication Servers of July 10, 2009.

799 R46 (Joint Creators) at 64.

800 T Aistars, 5/6/09, at 32-37.

801 *Id.* at 36.

The Assistant Secretary of Commerce for Communications and Information has advised the Register that he believes that the record does not support designation of the proposed class.[802]

Discussion. Soghoian's proposal for the benefit of researchers ultimately rests upon the same speculative argument as his proposal for the benefit of users. Since the record makes clear that the purpose of the "researcher" class is to facilitate the ability to circumvent under the umbrella of the "user" class, then, perforce, the arguments supporting the researcher class fail on the same basis as those supporting the user class. This failure to demonstrate an adverse effect on noninfringing uses obviates the need for the Register to discuss the arguments regarding the other merits and disadvantages propounded regarding the researcher class. And, as with the user class discussion, the Register declines to evaluate whether or not the researcher class would pass muster assuming that adverse effects had been demonstrated. The Register also declines to speculate upon the fate of the researcher class assuming that the user class was recommended. Accordingly, the Register recommends the rejection of this proposed class.

C. Software and information recorded, produced, stored, manipulated or delivered by the software, that a forensic investigator seeks to copy, activate, or reverse engineer in order to obtain evidence in a court proceeding.

Background and comments. Commenter Glenn Pannenborg proposed a class of works for the benefit of forensic investigators seeking evidence in court proceedings. Forensic investigators are experts in examining evidence, typically hired by a party to a court proceeding.[803] According to Pannenborg, forensic examiners practicing in the fields of financial or information technology may be faced with evidence "that is recorded, produced, stored, manipulated or delivered by software covered under 17 U.S.C. 1201," or evidence that may be "the software itself, as in a patent or licensing dispute."[804] He asserted that in order to obtain access to such evidence, a forensic investigator may have to circumvent a technological protection measure in violation of Section 1201(a)(1)(A).[805]

---

[802] NTIA Letter of November 4, 2009, at 13.

[803] C7 (Pannenborg) at 1-2.

[804] *Id.* at 2.

[805] *Id.* "[C]opy, activate, or reverse engineer" are the activities listed by the proponent, which the Register understands, given the context of the proposal, to include circumvention.

Pannenborg set forth a number of arguments relating to forensic investigators' need to be able to engage in circumvention, maintaining that "[i]ncomplete or inaccessible evidence impacts the rights of litigants and criminal defendants to due process. Likewise restrictions that limit acquisition of evidence hinder the ability of law enforcement and civil regulators to conduct investigations and prosecutions necessary for public safety."[806] Pannenborg maintained that methods of gaining access to encrypted evidence other than circumvention are inadequate. For example, he noted that the statutory exemptions for government activities (Section 1201(e)), encryption research (Section 1201(g)), and security testing (Section 1201(j)) do not apply to forensic investigation.[807] Also, he stated that seeking a court order to compel the production of encrypted information is unlikely to be effective if the software manufacturer is beyond the reach of the court, lacks the requisite technological knowledge, or refuses to fully comply with an order.[808]

Joint Creators opposed Pannenborg's proposal because, in their view, he has not shown that copyright owners of a work at issue in a court proceeding would refuse to authorize circumvention for forensic analysis.[809] Furthermore, they argued that there is no evidence that recalcitrant copyright owners, whether litigants or third parties, would not be subject to court orders authorizing circumvention.[810] Finally, the Joint Creators suggested that the statutory exemptions for government activities and reverse engineering could apply to circumvention for forensic analysis, a factor that mitigates the need for the Librarian to exercise his authority under Section 1201(a)(1)(C) and (D).[811]

NTIA comments. The Assistant Secretary of Commerce for Communications and Information has advised the Register that he believes that the record does not support granting Pannenborg's request.[812]

---

806 *Id.*

807 *Id.* at 3.

808 *Id.*

809 *See* R46 (Joint Creators) at 44-45.

810 *See id.* at 45.

811 *See id.* at 45-46.

812 NTIA Letter of November 4, 2009, at 13.

Discussion. The Register finds that the proponent in this case has not met the statutory burden of proof. In the first place, Pannenborg fails to intelligibly describe the nature of authorship of the proposed class of works, proposing initially that the class should consist of "computer software," and then stating that it is both software and "information" protected by the software.[813] In addition, the proposal's references to "information"[814] and "data"[815] raise the question of whether what is being sought by a forensic investigator is in any way a copyrighted work protected by title 17.[816]

More significantly, Pannenborg presents no compelling evidence, and provides no concrete examples, that noninfringing uses of works in the proposed class have been or will be affected by the circumvention ban. Indeed, he provides little information about the works to which he has apparently been denied access. Panneborg refers to two forensic investigations he has conducted, but the information he provides is sketchy and is insufficient to support the conclusion that the prohibition on circumvention has created problems in this area. In each case, counsel "made informal objections" that "the request lacked relevance because the installation media allowed only one installation and was unusable without circumvention of the digital protection."[817] However, it is difficult to discern how a relevance objection could be sustained on such grounds, and the precise nature and context of the "informal objection" are also unclear, providing no reasonable basis upon which to evaluate whether Section 1201's prohibition on circumvention in fact adversely affected the proponent's ability to engage in a noninfringing use.[818] If the proponent had provided more information concerning these examples, an evaluation of whether and the extent to which the prohibition on circumvention caused such an adverse effect might have been possible.

---

[813] C7 (Pannenborg) at 2.

[814] *Id*.

[815] *Id.* at 3.

[816] The statute is clear that the subject matter of this rulemaking proceeding in that exemptions is confined to "noninfringing uses under this title of a *particular class of copyrighted works*." 17 U.S.C. § 1201(a)(1)(C) (emphasis added). Mere information or data, without the application of "some minimal degree of creativity," *Feist Publ'ns v. Rural Telephone Service Co.*, 499 U.S. 340, 435 (1991), is not copyrightable and thus not eligible to be, or to be included in, a "class of copyrighted works."

[817] C7 (Pannenborg) at 3.

[818] For purposes of this analysis, the Register assumes that the proposed use was noninfringing, but the proponent has not actually attempted to make the case that the use was noninfringing.

Regarding the Joint Creators' argument that Pannenborg has not demonstrated an unwillingness on the part of copyright holders to authorize access control circumvention in the context of court proceedings, it appears to the Register that it is fair to interpret the "informal objections" described by Pannenborg as at least two examples of just such unwillingness, or, at least, reluctance. These examples by themselves, of course, cannot support Pannenborg's proposed exemption, particularly since he presents no evidence of himself or anyone else requesting a court order compelling the copyright owners to authorize circumvention, not to mention evidence of a court refusing to issue such an order or of a copyright owner refusing to comply.[819] The Joint Creators argue that, "as a matter of discovery, motions practice, or otherwise, the court would generally have the authority to order the owner of copyright in the data which is the subject of the forensic investigation to authorize circumvention of the access control in question."[820] Whether or not this is in fact the case, Pannenborg has provided no evidence one way or the other, much less any evidence of a court order failing to achieve the intended result due to the copyright owner being beyond the court's jurisdiction, lacking technological knowledge, or simply refusing to comply.[821]

Finally, regarding the question of whether Panneborg's proposal is pre-empted because one of Section 1201's statutory exemptions already applies,[822] the Register finds that none of the statutory exemptions offer sufficient protection for the circumvention of access controls for the

---

[819] The question of whether a litigant has requested authorization to circumvent, either from a copyright owner or the court itself, is addressed here only in the narrow context of a court proceeding in which a need arises to circumvent an access control in order to gain access to potential evidence. The Register is by no means suggesting a general rule that permission to circumvent must first be sought and denied in order for a user to be able to demonstrate an adverse effect on a noninfringing use.

[820] R46 (Joint Creators) at 45. Pannenborg argues that, in some cases, a software manufacturer might be beyond the jurisdiction of the court in which the litigation is pending and may choose not to comply with a court order. He also suggests other situations in which the software manufacturer may choose not to, or may not be able to, comply. But such speculation appears to be contrary to established procedures for obtaining discovery in civil litigation. It is typical for state judicial procedures to permit the issuance of subpoenas to obtain discovery, including the production of documents and things, in connection with litigation pending in other states. *See, e.g*, Calif. C.C.P. §§ 2029.100 *et seq*. (eff. Jan. 1, 2010); Md. Code, Courts and Judicial Proceedings, §§ 9-401 *et seq.* (2009); Va. Code. Ann. §§ 8.01-410 *et seq*.(2009). A federal court may also issue a subpoena for production of documents and things in connection with litigation pending in a federal court in another state. *See* Fed.R.Civ.Pr. 45(a)(2). The Register will not assume, especially in the absence of any evidence, that a software manufacturer (who is likely to be the copyright owner) would refuse or be unable to comply with a properly issued subpoena or a court order to either provide an unencrypted copy or to authorize decryption of an encrypted copy..

[821] *See* C7 (Pannenborg) at 3.

[822] *See, e.g.*, 2003 Recommendation of the Register of Copyrights at 181 ("Where a statutory scheme exists for particular activity, persons must utilize such statutory exemptions to accomplish their goals or provide evidence why the statutory exemption is unavailable to accomplish a noninfringing use . . .")

purposes of forensic analysis. Ultimately, however, given the failure of Pannenborg to show that Section 1201's access control circumvention ban is having or will have any effect upon the noninfringing use of works in his proposed class, the question of whether a statutory exemption may be available is moot. The Register, therefore, declines to recommend that the Librarian designate this proposed class of works.

D. Audiovisual works delivered by digital television ("DTV") transmission intended for free, over-the-air reception by anyone, which are marked with a "broadcast flag" indicator that prevents, restricts, or inhibits the ability of recipients to access the work at a time of the recipient's choosing and subsequent to the time of transmission, or using a machine owned by the recipient but which is not the same machine that originally acquired the transmission.

Background. In 2003, the FCC adopted regulations mandating a broadcast flag for digital broadcast television programming. The broadcast flag can be described as a digital code embedded in a DTV broadcasting stream, which prevents digital television reception equipment from redistributing broadcast content. The broadcast flag affects receiver devices only after a broadcast transmission is complete. The goal behind the broadcast flag requirement was to prevent the unauthorized redistribution of digital broadcast television content over the Internet. However, the FCC's regulations were overturned by the United States Court of Appeals for the District of Columbia Circuit in 2005.[823] Nevertheless, in the 2006 rulemaking, a number of commenters sought relief targeting broadcast flags for television and radio broadcasts, noting that such restrictions could possibly interfere with the personal recording of digital broadcast content for time-shifting and format-shifting purposes.[824] The Register rejected those requests stating that there was no broadcast flag mandate in effect for either television or radio at that time. The Register concluded that a class could not be designated based upon non-existent regulations.[825]

Comments. Matt Perkins proposed the following class of works:[826]

---

[823] *American Library Association v. FCC*, 406 F.3d 689, 693 (D.C. Cir. 2005)(FCC found to have lacked the statutory authority to implement a broadcast flag regime.)

[824] *See* 2006 Recommendation of the Register of Copyrights at 83.

[825] *Id.* at 84.

[826] C9A (Perkins) at 1.

> Audiovisual works delivered by digital television ("DTV") transmission intended for free, over-the-air reception by anyone, which are marked with a "broadcast flag" indicator that prevents, restricts, or inhibits the ability of recipients to access the work at a time of the recipient's choosing and subsequent to the time of transmission, or using a machine owned by the recipient but which is not the same machine that originally acquired the transmission.

Perkins believed that broadcasters and copyright owners will experiment with copy protection measures to restrict the recording of broadcast television content soon after the completion of the DTV transition in June 2009.[827] He asserted that consumers will experience frustration if their television recording privileges are in any way restricted.

The National Association of Broadcasters ("NAB") argued that Perkins has failed to provide evidence either that actual harm currently exists or that it is likely to occur in the ensuing 3-year period.[828] Specifically, it argued that the request must be rejected because there are no devices to which it would apply.[829] It concluded that the suppositions in support of the request are pure speculation and a class cannot be designated in this rulemaking any more than it could in 2006 when the Register found a similar proposal to be premature.[830]

NAB stated that even if there were a broadcast flag to which an exemption might apply, the proposed exemption should be rejected for several reasons. NAB asserted that since the flag would affect redistribution, it would not be an access control technological protection measure for purposes of Section 1201(a), and therefore it would not be subject to action in this rulemaking proceeding.[831] NAB also asserted that the proposal is devoid of any explanation or justification as to what noninfringing activity the prohibition on circumvention of the broadcast flag is preventing.[832] NAB concluded that Perkins' proposal is fatally flawed because it fails to

---

[827] Congress initially established February 17, 2009, as the date for the completion of the transition from analog to digital broadcast television. *See* Pub. L. No. 109-171, Section 3002(a), 120 Stat. 4 (2006). In early 2009, however, Congress passed the DTV Delay Act, extending the date for the completion of the nationwide DTV transition from February 17, 2009, to June 12, 2009. All full-power television broadcast stations now transmit only in a digital format.

[828] R40 (NAB) at 2. MPAA, Joint Creators, and Time Warner agree with NAB and all assert that the proposal is premature and nothing has changed since 2006 to alter that conclusion.

[829] *Id*. at 2.

[830] *Id.*

[831] *Id.* at 3.

[832] *Id*. at 4 -5.

demonstrate that noninfringing activities are being prevented by the prohibition on circumvention.

NAB also stated that Perkins made no case at all, much less a *prima facie* case, demonstrating why the plethora of sources providing access to most of the audiovisual works that will be transmitted over DTV are "insufficient substitutes for accomplishing [his] noninfringing use."[833] In support of this statement, NAB explained that the Internet and mobile wireless devices are becoming increasingly popular modes of disseminating movies and television shows. It added that consumers can view videos on subscription sites, through pay-per video downloads, and via commercial-supported streaming video, as well. NAB reiterated that works transmitted over DTV are not protected by access control technological protection measures, but asserted that, even if they were, the explosion in the fast and efficient availability of such works on DVDs, the Internet, and other digital networks eviscerates any claimed need for the relief proposed here.[834] The Assistant Secretary of Commerce for Communications and Information has advised the Register that he believes the record does not support designating the proposed class.[835]

Discussion. Perkins has failed to make his case. He has generally stated that a broadcast flag would interfere with the recording of digital television programming for personal use. However, he has not met his burden of proof in showing a need for any action. There is no broadcast flag mandate for digital television broadcasts in effect and it is highly speculative as to whether broadcasters and copyright owners will implement measures to restrict consumer recording privileges in the new DTV era.

The record does not indicate that there currently exist any devices that include broadcast flags. NAB asserts that no such devices exist, and the proponent of the class does not contradict this assertion, instead stating only his prediction that copyright owners will deploy the broadcast flag.[836] Furthermore, the proponent's theory in support of designating the class lacks any explanation or justification as to what non-infringing use would be prevented by the prohibition on circumvention with respect to the broadcast flag and fails to provide evidence that actual harm

---

833 *Id.* at 6.

834 *Id.* at 9.

835 *See* NTIA Letter of November 4, 2009, at 13.

836 R40 (NAB) quoting C9A (Perkins) at 1 ("It must be expected that, following the complete shut-off of standard analog TV signals in 2009, broadcasters and copyright owners will do more to experiment with these copy restrictions.")

exists or that it is "likely" to occur in the ensuing three year period. NAB also appears to be correct in asserting that the proposal exemption should be rejected because it affects redistribution and is not focused toward an access control technology measure for purposes of Section 1201.

Three years ago, in reviewing a similar request, the Register observed,

> The proponents offer no evidence to suggest that such systems will be established, nor is such evidence readily available – it is a matter of conjecture and opinion. Moreover, even if an audio or television broadcast flag were to be established or re-established, the precise substance of the requirement is likewise unknown at this time. Nonetheless, the comments assert that such a system will adversely affect their ability to make noninfringing uses. That is speculation. No evidence has been presented that a "broadcast flag" is currently being deployed and the case has not been made that a "broadcast flag" is likely to be deployed in the next three years (or whether it would constitute an access control). The proposed exemption is simply premature at best.[837]

The same observation is true with respect to the current proposal. For the reasons stated above, the Register recommends that the proposal be rejected.

E. Audiovisual works embedded in a physical medium (such as Blu-ray discs) which are marked for "down-conversion" or "down-resolutioning" (such as by the presence of an Image Constraint Token "ICT") when the work is to be conveyed through any of a playback machine's existing audio or visual output connectors, and therefore restricts the literal quantity of the embedded work available to the user (measured by visual resolution, temporal resolution, and color fidelity).

Background. This class was also proposed by Matt Perkins.[838] Here, Perkins focused his exemption request on the Blu-ray Disc.[839] He states that the Blu-ray disc's data structure allows a

---

[837] *See* 2006 Recommendation of the Register of Copyrights at 84.

[838] C9B (Perkins) at 2.

[839] Blu-ray, also known as Blu-ray Disc, is the name of a next-generation optical disc format jointly developed by the Blu-ray Disc Association, a group of consumer electronics, personal computer, and media manufacturers. The format was developed to enable recording, rewriting and playback of high-definition video, as well as storing large amounts of data. The format offers more than five times the storage capacity of traditional DVDs and can hold up to 25GB on a single-layer disc and 50GB on a dual-layer disc. *See* http://www.blu-

disc publisher to assign an image constraint token ("ICT") to an audiovisual work. He further explained that a licensed Blu-ray disc player responds to that token by "down-rezzing" the electronic video signal when conveyed over an "untrusted" analog connection (*i.e.*, a trio of RCA cables). He asserted that no such constraints occur when the signal is conveyed over the preferred, "trusted" digital pathway (High-Definition Multimedia Interface ["HDMI"] incorporating High-bandwidth Digital Content Protection or ["HDCP"]).

Perkins admitted that there is little evidence that ICTs are currently embedded in available Blu-ray discs. He nevertheless asserted that the possible inclusion of an image constraint token will cause user frustration because program content will not be seen in the promised high definition format.

Perkins argued that ICT denies access to discarded video details until a condition is satisfied (HDMI connectivity), and therefore that ICT qualifies as a 1201 access control measure. Perkins suggested that the Register should carefully consider measurements of fidelity, such as visual, temporal, and auditory resolution, not only to inform assumptions on what does and does not qualify as a 1201 access control, but also in judging the substitutability of one format for another in her balancing assessments.[840]

Comments. AACS LA[841] filed comments in opposition to Perkins' request. It argued that his proposal fails to satisfy the burden of proof required in this proceeding. It asserted that, as stated in the NOI, a proposal to designate a class "must be based on a showing that the prohibition has or is likely to have a substantial adverse effect on noninfringing uses of a particular class of works." It argued that Perkins has failed to make such a showing here, as he has provided no evidence or description of any actual harm or any adverse effect on noninfringing uses nor any evidence that the ICT has ever actually been used. Rather, it stated that Perkins simply mentions the possibility that an increase in ICT use at some point in the future would "cause user frustration."[842] AACS LA concluded that the proposal, based purely on hypotheticals, should be denied.

---

ray.com/info. (Last visited 5/7/10.)

[840] Melody Reineke was the only party to file comments in support of Perkins' request. *See* R18 (Reineke) at 2.

[841] AACS LA ("Advanced Access Content System Licensing Administrator") is a cross-industry effort founded by members from key industry sectors including studios, consumer electronics firms, and information technology companies. AACS LA explains that AACS is "an effective technological protection measure" covered by the anti-circumvention provisions of the DMCA, including the "access control" anticircumvention provisions of Section 1201(a). AACS LA states that it licenses AACS for use to protect against unauthorized access to or use of prerecorded video content using the Blu-ray Disc format. R35 (AACS LA) at 1-3.

[842] *Id.* at 8.

AACS-LA also asserted that the proposal is unwarranted because the potential problem described by Perkins is a rapidly disappearing legacy issue related to early iterations of high definition television sets. It stated that almost every high definition television currently manufactured contains the HDMI connections necessary to allow a user to view Blu-ray content in its highest resolution. Further, to the extent there are some users affected by the existence of an ICT, AACS-LA stated that this by no means renders even those users unable to access the work. It explained that this circumstance only means that the consumer cannot view the content in the highest resolution possible, but still could be able to view the content in a resolution higher than that displayed by a DVD. AACS-LA asserted that this does not constitute a substantial adverse effect on noninfringing uses of a particular class of works. Accordingly, it urged that the proposal should be denied.[843] The Assistant Secretary of Commerce for Communications and Information has advised the Register that he believes the record does not support the proposed class of works.[844]

Discussion. Perkins' proposed class request cannot withstand scrutiny. He has failed to meet his burden of proof demonstrating that designation of the proposed class is warranted with regard to the willful downconversion of high definition programming recorded on Blu-ray discs. He has not shown that the prohibition on circumvention has or is likely to have a substantial adverse effect on a clearly identifiable noninfringing use. Similarly, he has not demonstrated the existence of actual harm, or the likelihood of future harm that would be rectified by designating the proposed class. Specifically, he has not provided evidence that ICTs are currently being used on Blu-ray discs to restrict users from accessing the highest resolution format offered by Blu-ray discs. Further, AACS-LA correctly asserts that the proposal is unnecessary because the potential problem described by Perkins is a rapidly disappearing legacy issue related to early generation high definition televisions. Perkins request appears to be a cure in search of a disease. For the foregoing reasons, the Register recommends that the proposed class of works be rejected.

F. Literary works distributed in ebook format when all existing ebook editions of the work (including digital text editions made available by authorized entities) contain access controls that prevent the enabling either of the book's read-aloud function or of screen readers that render the text into a specialized format.

Background. Electronic books ("ebooks") are books that are distributed electronically and downloaded by users to their personal computers or portable electronic devices. On personal computers, the dominant formats for ebooks have been the Adobe's ".PDF" format and the Microsoft Reader's ".LIT" format. Personal electronic devices coupled with ebook reader applications, such as the Palm Reader, Amazon's Kindle, or Apple's iPhone or iPod Touch, have

---

[843] *Id.* at 7-9.

[844] *See* NTIA Letter of November 4, 2009, at 13.

begun expanding the ebook market. Although the public's acceptance of ebooks has until recently been sluggish, the development of these portable electronic devices capable of delivering and conveniently rendering electronic books has spurred demand in the marketplace. For the first time since access to ebooks has been raised in this rulemaking, ebooks now represent a vibrantly developing market.

The benefits of ebooks were immediately apparent to the blind and visually impaired. Ebooks present significant advantages to this community of users. When a book is in electronic form, it offers the potential for accessibility that is otherwise not available from the print version of a book. An ebook is capable of allowing a user to modify the size of the print, to activate a "read-aloud" function, or to interact with the work by means of separate screen reader software and hardware. The modification of print size can allow users with visual impairments to access an ebook without the need for corrective lenses or external magnification. The "read-aloud" function can render written text to synthesized speech, enabling the user to listen to a copy of a work by having the computer or device voice the text that appears on the screen. A screen reader program can also enable read-aloud functionality, but offers additional benefits to the blind and visually impaired. For instance, screen reader software can be coupled with hardware to enable rendering written text into Braille, or it can facilitate navigation through an ebook that would not be available with simple read-aloud options on a computer or portable device.

In 2006, the Librarian designated a class consisting of "Literary works distributed in ebook format when all existing ebook editions of the work (including digital text editions made available by authorized entities) contain access controls that prevent the enabling either of the book's read-aloud function or of screen readers that render the text into a specialized format."[845] The American Foundation for the Blind ("AFB"), which was the principal proponent of similar classes in 2003 and 2006,[846] has proposed that the Librarian "continue the current exemption to ensure that people who are blind or visually impaired are not excluded from the digital revolution in education, information and entertainment."[847]

AFB contended that because ebooks offer access to the blind and visually impaired, who would not otherwise have access to such works in text form, the DMCA should not be used as an obstacle to this unique opportunity for accessibility. It asserted that although some ebooks do offer the access that it seeks, not all ebooks enable read-aloud or screen reader functionality.

---

[845] This class was almost identical to a class designated in 2003: "Literary works distributed in ebook format when all existing ebook editions of the work (including digital text editions made available by authorized entities) contain access controls that prevent the enabling of the ebook's read-aloud function and that prevent the enabling of screen readers to render the text into a specialized format."

[846] *See* http://www.copyright.gov/1201/2006/comments/discipio_afb.pdf (Last visited 5/10/10.) and http://www.copyright.gov/1201/2003/comments/026.pdf. (Last visited 5/10/10.)

[847] C1 (AFB) at 2-3.

Given the advantages of access for this community and the likelihood that most underlying uses of the works that enable accessibility are noninfringing uses, AFB sought a "renewal" of the class designated by the Librarian in 2006.[848] It claimed that there have not been any significant changes in the market to eliminate inaccessibility that is caused by technological measures that control access and use of ebooks.[849]

Comments. In support of its proposal, AFB offered an examination of five ebooks, two tested in the PDF format and three of which were in the Microsoft LIT format.[850] AFB stated that of the five books tested, only one—or twenty percent of the sample—was accessible.[851] In order to make its case for an exemption, the AFB had to demonstrate that the prohibition on circumvention has adversely affected, or is likely to adversely affect, users' ability to make noninfringing uses of a particular class of works. There is no dispute that making an ebook accessible to the blind is a noninfringing use. Therefore, the main question before the Register is whether the prohibition on circumvention of technological measures that protect access have adversely affected persons in their ability to make noninfringing uses of a particular class of works, namely ebooks that are not available in an accessible format.

Because the determination whether to recommend designation of this proposed class turns on the factual case made by proponents of the class, and because those facts were presented succinctly, the case made in the initial comment is presented here verbatim:

> Title: *The Sign of the Fish*
> Author: Joan Klusmeyer
>
> This historical fiction novel written by one of the most prolific writers of e-books available on the Internet, opened in Acrobat, but content was not accessible. The screen reader voiced an extended string of question marks. Choosing the "accessibility quick check" on the "document" menu provided feedback, voiced by the screen reader. We were told that the "document's security settings prevented access by screen readers." This check did not indicate that this document is structured, so even if a screen reader could access the content, the user might be required to modify settings related to reading order preferences. The document cannot be saved as a text file.
>
> Title: *Brian's Hunt*
> Author: Gary Paulsen

---

[848] The class designated in 2006 was identical to the class proposed by AFB in this proceeding.

[849] C1 (AFB) at 6-7.

[850] *Id.* at 7-8.

[851] *Id*. at 8-10. In this discussion, "accessible" is used as shorthand for "available in an ebook edition that permits use of screen readers and the read-aloud function."

> This popular children's book was not accessible in the Microsoft Lit format. The work proved even less accessible than either of the Adobe PDF books as no messages were spoken with a screen reader. In fact, the Microsoft Reader software did not function fully with the screen reader, *i.e*. no menus were spoken or accessible using the keyboard. The Microsoft text-to-speech component did not improve the accessibility. As shown in the screen shot, only when a sighted assistant used a mouse to click on the book did a message indicate that the content was not accessible with text-to-speech.
>
> Title: *The Bridges of Madison County*
> Author: Robert James Waller
>
> This New York Times Best Seller was not accessible in the Microsoft Lit format. Our experience with this novel was virtually the same as the other Microsoft Reader digital books. The screen reader provided no feedback, and "tweaking" yielded no help to us when we tried to access the content independently. Sighted help was required to display the message in the screen shot.
>
> Title: *The Einstein Theory of Relativity*
> Author: H.A. Lorentz
>
> This physics book is a public domain book in the Microsoft Reader Lit format. The book is inaccessible – this is true whether or not Microsoft's text-to-speech product is installed. Sighted help was required to display the message shown in the screen shot.
>
> Title: *The Complete Works of Edgar Alan Poe Volume 1*
> Authors: Edgar Alan Poe
>
> This book, created using Adobe PDF, was the only one of the five that was accessible. The book opened easily in Acrobat version 8.1.2. We were permitted to choose options for processing and presenting the book in an accessible fashion. Although using the "accessibility quick check" indicated that the document was not tagged to provide structure, we were encouraged to try different reading order preferences, as necessary, in order to improve the reading experience. This 267-page book seemed to be accessible after a quick skim through some pages using Adobe's "infer reading order" option.[852]

In short, the proponents surveyed five ebook titles and found that three (*Brian's Hunt, The Bridges of Madison County,* and *The Einstein Theory of Relativity,* were not accessible in editions published in the Microsoft LIT format, one (*The Sign of the Fish)* was not accessible in an edition published in the Adobe PDF format, and one (*Einstein's Theory of Relativity*) was accessible in

---

[852] C1 (AFB) at 8-10.

the Adobe PDF format. Thus, four out of the five titles sampled were available in formats that were not accessible.

Proponents of the class presented no other factual information relating to whether (and the extent to which) the prohibition on circumvention actually has had an adverse effect on the ability of blind and visually impaired persons to engage in the noninfringing use of reading ebooks by using screen readers and the read-aloud function offered in many ebooks.[853]

The Joint Creators, while stating that they "do not oppose renewal of the exemption related to literary works in ebook format if the Register and the Librarian conclude that the proponent meets its burden of persuasion during this proceeding," questioned whether the prohibition on circumvention of access controls "is to blame for the discrepancy between access for the fully sighted and access for the visually impaired." They also questioned whether the proponents had provided sufficient facts to support designation of the class.[854]

The Assistant Secretary of Commerce for Communications and Information has advised the Register that he believes that an exemption based on this proposals should be renewed. NTIA did not state that the record supports granting the requested exemption; in fact, it observed that "the case made here is again weak. The proponents do not present the level of evidence envisioned by the requirements established in this proceeding." Nevertheless, NTIA concluded that "[d]espite the limited level of information provided by the exemption's proponent, NTIA is persuaded that harm to these uses and users is likely to exist."[855] Although NTIA was encouraged that the market is providing greater access of ebooks to the blind, the Assistant Secretary stated

---

[853] At the hearing on the proposed class, AFB's witness alluded to issues relating to Amazon's Kindle ebook reader, and to reports that "many owners of copyright through contract have essentially said to Amazon we want to exercise the option to restrict that text-to-speech option, to essentially be able to turn it off." T Richert, 5/8/09, at 8-9. However, he acknowledged that he had no information whether that function had been turned off; he simply expected that it would happen. *Id.* at 10. At no point did AFB or anyone else submit or seek to submit any information as to whether the text-to-speech option had ever actually been disabled in books sold for use with the Kindle, nor did anyone ever suggest whether or how such disabling would affect the analysis whether the prohibition on circumvention was having an adverse effect on the ability of blind and visually impaired persons to obtain access to books published in ebook form. For example, there was no information or suggestion that there were any books that: (1) have been published on the Kindle with the text-to-speech function disabled, and (2) are not otherwise available in an accessible ebook format. Nor was there any information or discussion as to how the existing and proposed class could be applied to ebooks distributed for use a stand-alone device such as the Kindle, rather than on personal computers, and whether or how such a stand-alone device could accommodate separate screen reader software. Thus, there is insufficient evidence in the record to support a conclusion that there are restrictions on ebooks distributed for use on the Kindle that have adversely affected the ability of users of ebooks to engage in noninfringing uses, or to determine how a class might be fashioned if such an adverse effect were shown to exist.

[854] R46 (Joint Creators) at 22.

[855] NTIA Letter of November 4, 2009, at 12.

that he believed that "even a limited number of literary works without access to the visually impaired is too many."

Discussion. Since 2003, when the issue of accessibility to ebooks was first raised by AFB and others, the Register has been supportive of the need to ensure that access controls are not used to prevent people who are blind and visually impaired from gaining meaningful access to books distributed in electronic formats. When AFB proposed that the Librarian designate a class of works that would permit circumvention of access controls on ebooks when those access controls had the effect of disabling screen readers or the read-aloud function, the proposal drew vigourous opposition from book publishers and other copyright owners. Opponents of that proposal challenged the ability of the Librarian to designate the proposed class because the issue, in their view, had nothing to do with whether users of the ebooks were denied *access* to the contents of the books. Rather, they argued, the issue related to "accessibility," a different issue governed by other provisions of the law. The Register rejected this objection, describing it as a "red herring" and noting that "To say that a blind person technically has 'access' to a work that he cannot perceive does not assist in resolving whether to recommend an exemption." She observed that "it is far from apparent that a blind person does have 'access' to an work in an ebook format that can be perceived only by viewing it on the ebook's screen."[856]

The Register concluded in 2003 that "the evidence that has been submitted by both proponents and opponents of the exemption establishes that a significant number of ebook titles are currently offered to the public for which accessibility to the blind and visually impaired has been disabled."[857] She noted that AFB had offered statistics from ebooks.com indicating that the percentage of ebook titles with the read-aloud function enabled was only 62% of the titles in Adobe "Ebook" format, 28% of the titles in Microsoft Reader format and 0% of the titles in Mobipocket and Palm format.[858] Moreover, the Association of American Publishers (AAP), the primary opponent of the proposal, had admitted that a publisher with 1650 ebook titles available applied a default setting of "read-aloud off" to those ebooks.[859] The same submission by AAP indicated that another "major publisher ... indicated that its current default setting is 'read aloud off' for e-books in the Adobe Reader format."[860]

---

[856] 2003 Recommendation of the Register of Copyrights at 68.

[857] *Id.* at 76.

[858] *Id.* at 75-76 n. 128.

[859] *Id.* at 76 n. 129. See also *id.* at 80 n. 138.

[860] Post-Hearing Response of Association of American Publishers to Copyright Office Questions Relating to Exemption for literary works/eBooks for persons with disabilities of June 20, 2003, at 2, in Docket No. RM 2002-4 (available at http://www.copyright.gov/1201/2003/post-hearing/post08.pdf).

Based on this record, the Register found that the proponents had made the case for designation of a class of works that would not be subject to the prohibition on circumvention of access controls.[861]

In the 2006 rulemaking proceeding, the Register again recommended that the Librarian designate a class of works to ensure that blind and visually impaired persons could have access to books published in the form of ebooks, but she observed that the case made by the proponents in that particular proceeding was tenuous and urged the proponents, in any future proceedings, to present a stronger case similar in nature to the case they had presented in 2003. She described the case presented in support of the proposal as follows:

> To make that case, AFB reported on its examination of five book titles. In the particular formats AFB tested, AFB reported that there was only one title that was accessible to screen readers. However, as the Joint Reply Commenters pointed out, AFB did not test all of the ebook formats in which the sampled book titles were available. For instance, AFB tested *The Imitation of Christ*, by Thomas A. Kemp is, in the Microsoft Reader LIT Format and found that work to be inaccessible whether or not Microsoft's text-to-speech product was installed. However, the Joint Reply Commenters pointed out that the same title appeared to be available in the Adobe format with the read-aloud function enabled. Still, for two of the five titles considered (40%), neither AFB nor the Joint Reply Commenters could find a format accessible to the visually impaired.
>
> In selecting a tiny sample of only five titles, and in conducting only a limited examination of the options available even for those five titles, AFB has made, at best, a minimal showing to demonstrate the existence of a continuing problem and the need to renew the proposed exemption. If AFB or others propose renewal of this exemption three years from now, they would be well advised to review a larger, more representative sample of titles and ascertain the availability and accessibility of those titles in all ebook formats.[862]

---

[861] 2003 Recommendation of the Register of Copyrights at 72. The Register's recommendation regarding the scope of the class is discussed below.

[862] 2006 Recommendation of the Register at 39 (footnotes omitted). The Register contrasted the case made in 2006 with the case that had been made three years earlier:

> In contrast to the showing made in this proceeding, three years ago AFB not only presented the results of its examination of a small number of ebooks, but also presented statistics relating to the overall percentage of ebooks in which the read-aloud function was enabled. *See* 2003 Recommendation of the Register of Copyrights at 76-77 n. 128.
>
> AFB suggested that due to budgetary limitations, it was not possible to test very many ebooks. T Dinsmore, 3/29/06, at 72. But AFB's 2003 submission of statistics reveals that there appear to be other ways to obtain the information without having to purchase a large number of ebooks. Moreover, sources such as ebooks.com, an online seller of ebooks, provide information for each title as to whether that title is available with the read-aloud feature enabled. *Id.* at 39 n. 111.

The Register also described the case for designating the class as "borderline."[863] However, in light of the lack of opposition to the proposal, the fact that publishers had admitted that there were ebooks in the marketplace that were not enabled for screen readers or the read-aloud function, and the strong benefits in making works accessible for use by the visually impaired, the Register recommended that the Librarian redesignate the class.

The Register's comments on the nature of the case presented in 2006 were not gratuitous or hostile. Having been persuaded in 2003 that there were strong legal and policy justifications for an exemption that would address the unwarranted (and probably unintended) obstacles that access controls on ebooks created for blind and visually impaired persons who simply wished to use existing tools that would permit them to get access to the contents of those ebooks, the Register was concerned that proponents had presented what appeared to be a perfunctory case for redesignation of the class. While the Register was willing to generously conclude that "the proponents have met their burden, if only barely,"[864] her comments on the deficiencies in the proponents' case and her contrasting of that case with the significantly stronger case presented in 2003 were intended to serve as a friendly reminder that even a sympathetic regulator cannot act unless an adequate record has been made to justify regulatory action. The intended message, which (as discussed below) apparently was not received by the proponents of the class, was that while the Register was willing to give the proponents the benefit of the doubt in that particular proceeding, they should be prepared in future proceedings to present a case that truly met their burden of proving facts that would justify the relief they sought.

Before discussing the inadequacies of the case presented by the proponents in the current proceeding, it is pertinent to review the scope of the classes that were designated in the 2003 and 2006 proceedings. In 2003, AFB proposed a class consisting simply of "literary works."[865] Library associations that supported of the AFB proposal proposed a narrower class of "Literary works, including eBooks, which are protected by technological measures that fail to permit access, via a "screen reader" or similar text-to-speech or text-to-braille device, by an otherwise authorized person with a visual or print disability."[866] The library associations' proposal was more narrowly tailored to the specific problem that AFB was proposing to solve by seeking relief in the proceeding. While agreeing that the library associations' proposal was closer to the mark, the Register refined it by limiting it to "literary works distributed in ebook format," and only "when all existing ebook editions of the work (including digital text editions made available by

---

863 *Id.* at 40.

864 *See 2006 Final Rule*, 71 Fed. Reg. at 68,475.

865 *See* 2003 Recommendation of the Register of Copyrights at 72.

866 *See id.*

authorized entities) contain access controls that prevent the enabling of the ebook's read-aloud function and that prevent the enabling of screen readers to render the text into a "specialized format" since the issues presented related only to ebooks. Moreover, she further refined the class by noting that "it would not apply to a work if, at the time of circumvention, an ebook version is on the market for which either the read-aloud function or screen readers are enabled."[867] The Register justified this limitation by noting:

> If an accessible ebook edition of a work is available in the marketplace or a digital text is available through a § 121 authorized entity, then the exemption does not apply. As the exempted class is framed, affected users are likely to consider circumvention only as a last resort and only where the work is unavailable for the intended noninfringing use. The exemption also serves to encourage publishers to make accessible versions available: when such a version is available, the publisher need not worry that users may lawfully circumvent access controls applied to the work. Thus, the recommended exemption gives the publisher ultimate control over whether any user can ever take advantage of the exemption with respect to that publisher's work.[868]

The Librarian accepted the Register's recommendation.

In 2006, AFB again proposed that the Librarian "continue the current exemption to ensure that blind and visually impaired people are not excluded from the digital revolution in education, information and entertainment."[869] As noted above, the Register described the case presented in support of the proposal as follows:

> To make that case, AFB reported on its examination of five book titles. In the particular formats AFB tested, AFB reported that there was only one title that was accessible to screen readers. However, as the Joint Reply Commenters pointed out, AFB did not test all of the ebook formats in which the sampled book titles were available. For instance, AFB tested *The Imitation of Christ*, by Thomas A. Kemp is, in the Microsoft Reader LIT Format and found that work to be inaccessible whether or not Microsoft's text-to-speech product was installed. However, the Joint Reply Commenters pointed out that the same title appeared to be available in the Adobe format with the read-aloud function enabled. Still, for two of the

---

[867] *See id.* at 64, 72-74.

[868] *Id.* at 75. This reasoning was consistent with a principle that has guided the Register's recommendations since the first Section 1201 rulemaking in 2000: If a class of works is available in both a "protected" format (*i.e.*, a format protected by access controls) and an "unprotected" format, there will ordinarily be no justification for designating that class of works in this rulemaking. See 2000 Recommendation of the Register of Copyrights, 65 Fed. Reg. at 64,568.

[869] Comments of the American Foundation for the Blind, Docket No. RM 2005-11, at 2.

> five titles considered (40%), neither AFB nor the Joint Reply Commenters could find a format accessible to the visually impaired.
>
> In selecting a tiny sample of only five titles, and in conducting only a limited examination of the options available even for those five titles, AFB has made, at best, a minimal showing to demonstrate the existence of a continuing problem and the need to renew the proposed exemption. If AFB or others propose renewal of this exemption three years from now, they would be well advised to review a larger, more representative sample of titles and ascertain the availability and accessibility of those titles in all ebook formats.[870]

The Register also described the case for designating the class as "borderline."[871] However, in light of the lack of opposition to the proposal, the fact that publishers had admitted that there were ebooks in the marketplace that were not enabled for screen readers or the read-aloud function, and the strong benefits in making works accessible for use by the visually impaired, the Register recommended that the Librarian designate the class, but with a minor modification: because the record established that the read-aloud function was insufficient to meet all the needs of blind and visually impaired readers and that screen readers provided greater and more useful access, the Register accepted the suggestion that the class include ebooks "when all existing ebook editions of the work … contain access controls that prevent the enabling *either* of the book's read-aloud function *or* of screen readers that render the text into a specialized format."[872]

Unfortunately, the record presented in support of redesignating the class in the current rulemaking is even weaker than the minimal, borderline showing made three years ago.

In reviewing the evidence presented in support of designating the proposed class, the first issue that is readily apparent is that two of the five works examined by AFB are in the public

---

[870] 2006 Recommendation of the Register at 39 (footnotes omitted). The Register contrasted the case made in 2006 with the case that had been made three years earlier:

> In contrast to the showing made in this proceeding, three years ago AFB not only presented the results of its examination of a small number of ebooks, but also presented statistics relating to the overall percentage of ebooks in which the read-aloud function was enabled. *See* 2003 Recommendation of the Register of Copyrights at 76-77 n. 128.
>
> AFB suggested that due to budgetary limitations, it was not possible to test very many ebooks. T Dinsmore, 3/29/06, at 72. But AFB's 2003 submission of statistics reveals that there appear to be other ways to obtain the information without having to purchase a large number of ebooks. Moreover, sources such as ebooks.com, an online seller of ebooks, provide information for each title as to whether that title is available with the read-aloud feature enabled. *Id.* at 39 n. 111.

[871] *Id.* at 40.

[872] *Id*. at 41-42 (emphasis added). The Librarian accepted the Register's recommendation.

domain.[873] Works in the public domain are not affected by the prohibition on circumvention. Section 1201(a)(1), in part, states: "No person shall circumvent a technological measure that effectively controls access to a work protected under this title."[874] A work in the public domain is not a work "protected under this title." Therefore, Section 1201 does not prohibit circumvention of a technological protection measure when it simply controls access to a public domain work; in such a case, it is lawful to circumvent the technological protection measure and there is no need for an exemption. Thus, the two works in the public domain included in the tiny sample – forty percent of the entire sample -- are irrelevant to the case for an exemption. Even though one of these two public domain works was found to be inaccessible, the prohibition on circumvention cannot be said to be adversely affecting uses of that work given that the prohibition does not apply to public domain works.

Two of the other ebooks cited in support of designating the class -- *Brian's Hunt,* by Gary Paulsen, and *The Bridges of Madison County,* by Robert James Waller – are alleged to be inaccessible in Microsoft LIT format. However, assuming that to be the case, it is not sufficient to justify redesignation of a class consisting of "literary works distributed in ebook format when *all* existing ebook editions of the work (including digital text editions made available by authorized entities) contain access controls that prevent the enabling either of the book's read-aloud function or of screen readers that render the text into a specialized format." (Emphasis added). If *Brian's Hunt* and *The Bridges of Madison County* are available in other editions that provide read-aloud and screen reader accessibility, then they are not examples of works justifying redesignation of the class. As the legislative history of section 1201 states, in assessing the impact of the prohibition

on the ability

to make noninfringing uses, the Librarian "should take into consideration the availability of works in the particular class in other formats that are not subject to technological protections."[875]

The only witness to testify in support of designation of this class, Mark Richert, acknowledged this, stating that "if it's exactly the same work and it's available in one electronic format versus another, I wouldn't see that this exemption would apply."[876] However, he admitted

---

[873] *The Complete Works of Edgar Alan Poe Volume 1,* by Edgar Alan Poe and *The Einstein Theory of Relativity,* by H.A. Lorenz. AFB itself states that the book by Lorenz is in the public domain. C1(AFB) at 9, 15. AFB does not provide information as to the specific edition of *The Complete Works of Edgar Alan Poe Volume I,* but it is apparent that any works by Edgar Allan Poe, who died in 1849, are in the public domain. In any event, AFB reported that *The Complete Works of Edgar Alan Poe Volume I* is accessible.

[874] 17 U.S.C. § 1201(a)(1)(A).

[875] House Manager's Report, at 7.

[876] T Richert, 5/8/09, at 15. He also stated that "It's a question of whether this particular book is available in an accessible format." *Id.* Mr. Richert is AFB's Director of Public Policy. *Id.* at 5.

that in examining the five ebooks in the sample offered in support of designating the class, the proponents did not check to see whether any of the inaccessible books was available in another ebook format.[877]

In failing to even check to see whether *Brian's Hunt* or *The Bridges of Madison County* are available in an accessible format, the proponents failed to meet their burden of proof with respect to those two titles. Evidence that a particular title, when published in *one* of the existing ebook formats is not accessible, does not demonstrate that "*all existing ebook editions* of the work … contain access controls that prevent the enabling either of the book's read-aloud function or of screen readers that render the text into a specialized format" (emphasis added).

The final book offered as an example of inaccessibility was *The Sign of the Fish*, by Joan Klusmeyer. The proponents of the class stated that the book "opened in Acrobat, but content was not accessible." Nothing was said about whether the book was also available in other formats (and, if so, whether those formats were accessible). Again, the proponents presented insufficient evidence to evaluate whether yet another of the limited number of titles in their sample was inaccessible in all ebook formats.

Although the Register could recommend against designation of the proposed class based simply upon the proponents' failure to provide sufficient evidence to evaluate whether any of the three non-public domain books cited by the proponents are inaccessible in all ebook formats, the Register's staff conducted some additional research to determine whether the case could be made that any or all of those three books that were identified by AFB are inaccessible in all formats.[878]

With respect to *Brian's Hunt* and *The Bridges of Madison County*, a quick review of the market revealed that both of these works are available as digital texts through Bookshare.org, which qualifies as an "authorized entity" under Section 121 of the Copyright Act.[879] Section 121

---

[877] *Id*. at 13-14.

[878] If that research had uncovered sufficient evidence to warrant designating the class, the Register would have had to decide whether she could rely upon evidence that was outside the record in order to designate a class. As will be seen, it was not necessary to make such a decision as the Register's staff did not find sufficient evidence to warrant designation of the class.

[879] Bookshare.org is an arm of a California not-for-profit organization known as the Benetech Group that allows persons and organizations qualified under Section 121 to download digital text and contribute scanned versions of books and certain printed material to the program. Those digital versions are made available to blind and disabled persons. *See* 2003 Recommendation of the Register of Copyrights at 74. As of April 2010, Bookshare.org was reported to have over 70,000 titles available on its service, including digital books, textbooks, teacher-recommended reading, periodicals, and assistive technology tools. *See* http://www.bookshare.org/. (Last visited 5/10/10.) The digital books provided by Bookshare.org are compatible with screen readers. *See* http://www.bookshare.org/_/gettingStarted/readBooks; http://www.bookshare.org/readingTools. (Last visited 5/10/10.)

permits authorized entities to reproduce and distribute copies or phonorecords of nondramatic literary works in specialized formats exclusively for use of the blind or other persons with disabilities.[880] "Specialized formats" include "braille, audio, or digital text which is exclusively for use by blind or other persons with disabilities."[881] An "authorized entity" is a nonprofit organization or a governmental agency that has a primary mission to provide specialized services relating to training, education, or adaptive reading or information access needs of blind or other persons with disabilities.[882] As noted above, in light of the showing only that the Microsoft LIT editions of the two books are inaccessible, the Register cannot conclude that *Brian's Hunt* and *The Bridges of Madison County* are inaccessible in her evaluation of the case for designating the proposed class. That conclusion is bolstered by the further quick research that reveals that both books are available in accessible formats.

The case with respect to *The Sign of the Fish*, by Joan Klusmeyer, is somewhat more equivocal. In its comments, AFB included a description of its testing of this ebook[883] and a screenshot of the cover in the Adobe Reader format,[884] but did not provide any information about where this ebook may be obtained. A search of the worldwide web revealed some information about the author and a location where the book might be downloaded in PDF format. A description of the author at eBookMall introduces Ms. Klusmeyer as "one of the most prolific authors of eBooks on the Internet."[885] The page lists many of Ms. Klusmeyer's titles, including *The Sign of the Fish*, but clicking on the link takes one to a page that states: "Sign of the Fish; Joan Klusmeyer of Rock Creek Publications; This page has been moved or the product is no longer available."[886] However, considerable further searching led to the book itself, on the same website.[887] The copy of the book available on the website, available for free in PDF format, does not appear to be accessible. No other copies of *Sign of the Fish* have been located. It appears that the book is available only (and barely) on the Internet.[888] Therefore, it appears that this single title

---

[880] 17 U.S.C. § 121(a).

[881] 17 U.S.C. § 121(d)(4)(A).

[882] 17 U.S.C. § 121(d)(1).

[883] C1 (AFB) at 8.

[884] *Id.* at 12.

[885] *See* http://www.ebookmall.com/authors/rockcreekpublications/. (Last visited 5/10/10.)

[886] *See* http://www.ebookmall.com/ebook/28976-ebook.htm. (Last visited 5/10/10.)

[887] *See* http://www.ebookmall.com/authors/rockcreekpublications/Sign-ofthe-Fish-JK32.pdf. (Last visited 5/10/10.)

[888] A search of the Library of Congress catalog and of OCLC's Worldcat catalog turned up no records relating to this book.

is not available in any edition that permits the enabling of the ebook read-aloud function or of screen readers.

Thus, after the inadequate case made by the proponents is supplemented by additional research regarding the three non-public domain titles relied upon by the proponents, the state of the evidence with respect to inaccessibility of ebooks boils down to a single example: *Sign of the Fish.* The Register cannot conclude that the prohibition on circumvention has had an adverse effect on the noninfringing use of reading ebooks with screen readers or the read-aloud function when the record reveals the case is built upon a single obscure book.

In 2006, the Register concluded that when a survey of only five titles found two titles that were inaccessible, that was "at best, a minimal showing" and she *advised* that in the future, proponents should "review a larger, more representative sample of titles."[889] Yet in the current proceeding, proponents returned with another sample of five titles, and only one non-public domain title turned out to be inaccessible. Proponents barely made their case three years ago. The case presented in this proceeding is, at best, half as strong. This simply does not rise to the level of "distinct, verifiable and measurable impacts" that Congress required in order to justify designation of a class; rather, it amounts to the kind of *de minimis* showing that does not justify relief in this proceeding. Even the Assistant Secretary of Commerce for Communications and Information, who recommends against rejection of the proposed class because such rejection "may have an uncertain effect on the progress made in the marketplace to make these works available to the visually impaired," acknowledges that the record is "weak."[890] In fact, NTIA observes that "[t]he proponents do not present the level of evidence envisioned by the requirements established in this proceeding."[891]

The Register agrees with that evaluation of the evidence. As the Notice of Inquiry in this proceeding stated, "The identification of isolated or anecdotal problems will be generally insufficient to warrant an exemption."[892] At best, the case in support of designating the proposed ebook class is anecdotal, based upon a single title.

As noted above, three years ago the proponents of the existing ebook class submitted a sample of five titles, two of which turned out to be inaccessible. The Register characterized that showing as "minimal" and "borderline," and advised that in future rulemakings proponents would be "well advised to review a larger, more representative

---

889 2006 Recommendation of the Register of Copyrights at 39.

890 NTIA Letter of November 4, 2009, at 13 n . 87.

891 *Id.* at 12 n. 83.

892 NOI, 73 Fed. Reg. at 58,075.

sample of titles and ascertain the availability and accessibility of those titles in all ebook formats."

In the current proceeding, proponents again came forward with a sample of five titles, only one of which turned out to be inaccessible.[893] The proponents' unwillingness or inability to survey a more substantial number of book titles and to determine whether the titles they presented were accessible in any format is inexplicable. As a result, although (as her past recommendations have demonstrated) the Register would be favorably disposed to recommend designation of the class if sufficient facts were placed in the record, she has no choice but to recommend that the Librarian decline to designate this proposed class.

The Register does not come to this conclusion lightly, but notes that there are additional bases in the record for denial of AFB's proposed exemption. AFB's Mark Richert was directly asked at the hearings whether he had any knowledge whether the exemption that issued in 2006 has ever been used by anyone. Apart from vague references to knowledge by "the general community" that "particularly smart, capable individuals who've been able to find their way around these barriers," Richert was unable to identify any actual cases in which someone has taken advantage of the existing exemption.[894] This was consistent with the statements made in testimony in 2003.[895] While it may be difficult to ascertain the ways in which an exemption to the prohibition remedies a verifiable problem, some evidence of the benefit of an existing exemption would be probative for a request to issue the exemption in a subsequent three-year period, and the lack of evidence that an existing exemption has been used suggests that there is no need for such an exemption.[896] Some evidence of this nature has been provided to bolster more specific evidence in other contexts.[897] The AFB's failure to inquire and report on the benefits or deficiencies of the existing exemption serves only to diminish the already inadequate evidentiary support for the need for an exemption.

---

[893] As noted above, the Register does not count *The Einstein Theory of Relativity*, because, as a work in the public domain, it is irrelevant.

[894] T Richert, 5/8/09, at 27-28.

[895] T Richert, 3/29/06, at 62-65.

[896] *See* 2006 Recommendation of the Register of Copyright*s* at 39-40 ("One could well conclude that the fact that a class of works has enjoyed an exemption for the past three years but nobody appears to have taken advantage of that exemption is proof that the prohibition on circumvention is unlikely to have any adverse effect on the ability of users of that class of works to make noninfringing uses during the next three years.")

[897] *See, e.g.*, C4E (Decherney) at 4 (For the past three years, media professors have benefitted greatly from the anticircumvention exemption, and we now hope to extend this exemption to allow students to enhance their learning experience in the field of media and film studies.)

Another prominent issue raised in AFB's comments and testimony relates to insufficient information, at the time of sale, about the accessibility of ebooks. The provision of clear information about digital rights management information is a concern being addressed in others areas of the federal government, and is within the jurisdiction of other federal agencies.[898] These concerns may even be more compelling in relation to the blind and visually impaired. However, an exemption to the prohibition on circumvention would have absolutely no effect on the labeling of works or product return policies.[899] In order for an exemption to be warranted, the prohibition on circumvention must be the proximate cause of the adverse effect identified. While inadequate labeling for persons with disabilities is an undisputed concern, it is causally unrelated to the prohibition on circumvention.

The Register fully supports universal accessibility to ebooks for the blind and visually impaired.[900] However, the rulemaking established by Congress requires proponents to demonstrate, *de novo*, in each rulemaking proceeding, that an exemption for any particular class of works is warranted for the ensuing three-year period. The Register is sympathetic to the needs of the blind and visually impaired, and agrees that as a matter of policy, access to e-books for the visually impaired should be encouraged and, when there is evidence that the prohibition on circumvention is having an adverse impact on that goal, an exemption is warranted. The Register has not hesitated to recommend such exemptions when the record has supported such a recommendation. However, unless the burden of presenting a *prima facie* case for an exemption is met, the statutory standard established for this rulemaking does not permit the Register to recommend an exemption. To justify an exemption for a class of works simply because there are strong policy arguments in favor of the exemption, and despite the lack of a factual foundation, would establish a basis for a perpetual exemption unless, in a particular rulemaking, no proponent came forward in support of the proposed exemption. Exemptions in this rulemaking were intended to be limited exceptions to the default prohibition on circumvention and to be grounded in the record of the rulemaking proceeding and based on existing marketplace conditions.[901]

---

[898] *See, e.g.*, the Federal Trade Commission's inquiry, comments, and town hall meeting on digital rights management concerns: http://www.ftc.gov/opa/2008/12/drm.shtm. (Last visited 5/10/10.)

[899] *See* "related issues" in C1 (AFB) at 10.

[900] Indeed, in testimony before Congress a few months ago, the Register stated:

> "Likewise, the promise to offer millions of titles through libraries in formats accessible by persons who are blind and print disabled is not only responsible and laudable, but should be the baseline practice for those who venture into digital publishing."

Competition and Commerce in Digital Books: Hearing before the H. Comm. on the Judiciary, 111th Cong. 67 (2009)(statement of Marybeth Peters, Register of Copyrights).

[901] *See* Commerce Committee Report at 36 ("This mechanism would *monitor developments in the marketplace* for copyrighted materials, and allow the enforceability of the prohibition against the act of

Establishing a perpetual exception to the prohibition, or any purely policy-based exception not based on a factual record, is and should be a legislative act within the domain of Congress.

For all of the reasons set forth above, the Register finds no factual basis for designating this proposed class of works for the ensuing three-year period. While the Register's recommendations in previous rulemakings made clear that the Register understands and accepts the legal and policy reasons for such an exemption, under the constraints established by Congress in this rulemaking proceeding, the Register cannot recommend designation of the class in the absence of a factual record that supports the need for the exemption. No such showing has been made in this proceeding.

---

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.") (Emphasis added).